VANJA KORAĆ

INFRASTRUKTURA SA JAVNIM KLJUČEVIMA U FUNKCIJI ZAŠTITE INFORMACIONOG TOKA I ELEKTRONSKOG POSLOVANJA

ARHEOLOGIJA I
PRIRODNE NAUKE

POSEBNA IZDANJA

Center for New Technology
Archaeological Institute Belgrade

ARCHAEOLOGY AND SCIENCE

SPECIAL EDITION
5

Belgrade 2010

Centar za nove tehnologije
Arheološki institut Beograd

ARHEOLOGIJA I PRIRODNE NAUKE

POSEBNA IZDANJA
5

Beograd 2010.

Published by:
Center for New Technology Viminacium
Archaeological Institute Belgrade

Izdavači:
Centar za nove tehnologije Viminacium
Arheološki institut Beograd

For the publishers:
Miomir Korać
Slaviša Perić

Za izdavače:
Miomir Korać
Slaviša Perić

Editor:
Miomir Korać

Urednik:
Miomir Korać

Book design:
Nemanja Milićević

Dizajn knjige:
Nemanja Milićević

Print:
DigitalArt Company Beograd

Štampa:
DigitalArt Company Beograd

Printed in:
500 copies

Tiraž:
500 primeraka

ISSN 1820-6492
ISBN 978-86-87271-21-0

Vanja Korać

INFRASTRUKTURA SA JAVNIM KLJUČEVIMA U FUNKCIJI ZAŠTITE INFORMACIONOG TOKA I ELEKTRONSKOG POSLOVANJA

Beograd
2010

SADRŽAJ

Sažetak

U ovom radu je razmatran problem izgradnje infrastrukture javnih ključeva (PKI) u organizaciji. U radu su analizirane osnovne bezbednosne karakteristike savremenih računarskih mreža baziranih na Internet tehnologijama i dat je prikaz tehnika i kriptografskih protokola kojima se navedeni bezbednosni problemi rešavaju. Opisane su tehnike zaštite na aplikativnom, transportnom i mrežnom nivou ISO/OSI modela koje se baziraju na primeni infrastrukture sistema sa javnim ključevima. PKI rešava mnoge probleme u oblasti sigurnosnih računarskih komunikacija, i sprovodi bezbednosnu politiku organizacije. Rad je baziran na predlogu izvodljivog pristup izgradnje na bazi Microsoft PKI rešenja. Navedeni pristup snižava troškove i kompleksnost izgradnje PKI i čini je dostupnom širem krugu organizacija.

Abstract

In this paper, an implementation of public key infrastructure (PKI) in an organisation is considered. Here we analyse basic security caracteristic of modern computer communication network based on Internet technology and one overview of cryptographic protocols by which these security problems could be solved is given. In this work security techniques on application, transport and network layer ISO/OSI model which are based on PKI implementation are described. PKI enables solving problems in the area of secure computer communications and enforces an organization's security policies. This thesis suggests a feasible approach for creating PKI based on Microsoft PKI implementation. Given approach lowers the cost and level of building complexity of PKI and puts them within the reach of an organisation.

UVOD

Savremene računarske mreže se uglavnom baziraju na Internet tehnologijama i protokolima koji su podložni mogućim napadima koji narušavaju bezbednost podataka i identitet subjekata. Ključni problem leži u činjenici da podaci egzistiraju u elektronskom obliku koji nije neposredno vidljiv i zbog toga postaju izloženi novim vrstama napada, a osnovni razlozi, za to, leže u samim osnovnim karakteristikama arhitekture računarske mreže Internet/Intranet tipa:

- TCP/IP protokoli nisu projektovani da zadovolje zahteve za zaštitom informacija,
- Internet je mreža sa komutacijom paketa, u kojoj se jednostavno pristupa informacijama koje se prenose i moguće je ubacivanje poruka nepoznatog porekla i sadržaja.

U cilju rešavanja navedenih problema, uporedo sa razvojem računarskih mreža, razvijaju se i specijalizovani softverski i hardverski sistemi zaštite. Danas, u svetu postoji veliki broj proizvođača tehnološki kvalitetnih proizvoda za različite nivoe zaštite savremenih mreža. U ovim proizvodima su ugrađeni javni standardni kriptografski algoritmi. Iako pomenuti proizvodi predstavljaju veoma kvalitetna rešenja sa stanovišta tehnologije realizacije, oni se ne preporučuju za primenu u TCP/IP računarskim mrežama sa bezbednosno osetljivim podacima. Osnovni razlog je nepostojanje potpune sigurnosti u kriptografski kvalitet ovih rešenja, tj. ona se ne mogu verifikovati na nivou izvornog koda.

Najkvalitetnija kriptografska rešenja, koja se primenjuju u savremenim računarskim mrežama, baziraju se na primeni simetričnih kriptografskih sistema za zaštitu tajnosti (po mogućstvu uz korišćenje sopstvenih simetričnih algoritama višeg kriptografskog kvaliteta), asimetričnih kriptografskih sistema baziranih na tehnologiji digitalnog potpisa, digitalnih sertifikata i hardverskih modula (kriptografski koprocesori i smart kartice). Ovakvi sistemi zaštite su projektovani da se uspešno odbrane od potencijalnih opasnosti i napada u cilju ugrožavanja bezbednosno osetljivih resursa informacionih sistema[19].

Kriptografski algoritmi koji se primenjuju u sistemima zaštite Internet/Intranet računarskih mreža dele se u dve velike grupe:

- Simetrični kriptografski algoritmi;
- Asimetrični kriptografski algoritmi;

Podela je izvedena na osnovu posedovanja informacija neophodnih za šifrovanje i dešifrovanje. Primenom simetričnih kriptografskih algoritama se, kao i u tradicionalnim sistemima zaštite, ostvaruje funkcija zaštite tajnosti u savremenim informacionim sistemima.

Sa druge strane, infrastruktura sistema sa javnim ključevima (engl. Public Key Infrastructure PKI) omogućuje ambijent za pouzdanu primenu elekronskog poslovanja i ona se najčešće bazira na kombinovanoj primeni asimetričnih i simetričnih šifarskih sistema. PKI infrastruktura se sastoji od više komponenata, aplikacija i dokumenata koji definišu način realizacije četiri osnovne kriptografske funkcije u elektronskom poslovanju:

- Zaštita tajnosti – realizuje se simetričnim kriptografskim sistemima;
- Autentičnost – realizuje se asimetričnim šifarskim sistemima;
- Integritet podataka – realizuje se asimetričnim šifarskim sistemima;
- Neporecivost transakcija – realizuje se asimetričnim šifarskim sistemima.

Predmet ovog rada je da ispita mogućnosti i predloži rešenje za PKI u organizaciji. Ovo rešenje mora pre svega biti izvodljivo, odnosno dovoljno jednostavno i prihvatljivo, uzimajući u obzir ograničene hardverske, softverske, finansijske i ljudske resurse dostupne organizaciji. Rad će se sastojati od tri glavna dela. Prvi deo je posvećen neophodnim teoretskim osnovama, drugi deo je posvećen PKI sistemima. U trećem delu će biti izložen plan izgradnje infrastrukture javnih ključeva na bazi MS PKI tj. Microsoft Certificate services sistema za izdavanje digitalnih sertifikata internim korisnicima tj. zaposlenima u organizaciji.

U prvom delu će biti izložene teoretske osnove na kojim se zasniva infrastruktura javnih ključeva. Ukratko će biti navedena uloga i namena kriptografije kroz istoriju do danas. Biće predstavljene osnove simetrične kriptografije sa značajnim algoritmima. Asimetrična kriptografija, kao temelj infrastrukture javnih ključeva, biće takođe opisana. Digitalni potpis, kao nadogradnja asimetrične kriptografije i protokol koji omogućava infrastrukturu javnih ključeva, biće detaljno obrađeni. U drugom delu sve osnovne komponenete infrastrukture javnih ključeva i principi rada biće izloženi do nivoa detalja potrebnog za sagledavanje pitanja vezanih za izgradnju ovakve infrastrukture. Treći deo je posvećen MS PKI implementaciji. Osnovne komponente predloženog sistema su:

19. Transmission Control Protocol/Internet Protocol. Protokol za kontrolu prenosa/Internet protokol.

- Microsoft Stand-alone Root CA koji je podignut za potrebe PKI sistema Organizacije kao vrh u PKI hijerarhiji (Top Level CA – Root CA Organizacija);
- Microsoft Enterprise Subordinate CA koji je integrisan sa Aktivnim direktorijumom kao CA izdavalac (issuing CA) sertifikata korisnicima;
- Smart kartice za zaposlene (uz čitač smart kartica) na kojima se izdaju sertifikati za Windows logon, zaštićeno slanje S/MIME email poruka (korporativni zaštićeni mail) i SSL klijentsku autentikaciju;
- E-mail klijenata (MS Outlook i MS Outlook Express) u kojima se koriste pomenute kartice za digitalno potpisivanje i šifrovanje, kao i Internet browser program ili odgovarajuća aplikacija za SSL zaštićen pristup web aplikacijama i web servisima;

Pošto je CA (engl. Certificaion Authority - Sertifikaciono telo) osnova PKI, prvi korak u izgradnji PKI, nakon definisanih potreba, je utvrđivanje kakva CA je potrebna da bi se zadovoljile definisane potrebe i koliko nivoa CA je potrebno za dovoljnu bezbednost u organizaciji. Predložena je dvonivoiska CA. Prvi nivo je Root standalone (offline) CA, a drugi nivo je Microsoft Enterprise Subordinate CA. Biće razmotreni svi aspekti uspostavljanja takve MS PKI hijerhije i biće predložena potrebna konfiguracija. Na osnovu definisane konfiguracije, će se razmotriti konfiguracija digitalnih sertifikata. Biće detaljno razmotren format sertifikata, sigurnosne opcije kriptografski algoritimi, templejti, dužine ključeva i period trajnosti sertifikata i odgovarajućih ključeva.

U radu će takođe biti razmotreno i pitanje upravljanja sertifikatima metode dobijanja, obnavljanja i opoziva sertifikata. Biće predloženo sigurno i praktično izvodljivo rešenje. Kroz pomenuta razmatranja će biti definisani svi elementi PKI sa međusobnim interakcijama. Na osnovu ovih definicija biće moguće pristupiti izgradnji konkretnog sistema kroz korake koji će biti opisani u radu. Ova infrastruktura će dati svim korisnicima u organizaciji digitalni identitet. Digitalni sertifikati, u okviru predloženog internog Microsoft PKI okruženja date organizacije, bi se izdavali na smart karticama. Na ovaj način zaposlenima u organizaciji bi bila omogućena:

- Jaka autentikacija;
- Zaštićena interna elektronska pošta putem S/MIME standarda e-mail zaštite;
- Zaštita pristupa i zaštićena SSL komunikacija u okviru posebnih aplikacija date orgranizacije.

Na ovaj način će se u organizaciji omogućiti sigurna komunikacija i upotreba računarskog sistema zasnovane na osnovnim postulatima sigurnosti:

- Autentikacija strane koja je poslala digitalno potpisanu poruku;
- Poverljivost digitalno potpisanih podataka;
- Integritet podataka;
- Neporecivost sadržaja digitalno potpisane poruke.

OSNOVNI POJMOVI IZ KRIPTOGRAFIJE

Kriptografija je nauka koja se bavi metodama očuvanja tajnosti informacija i pruža rešenje ovog problema. Kriptografija zbog svoje specifičnosti i uloge koju je imala kroz istoriju sve više postaje vrlo zanimljiva i široj publici – netehničkoj. Kriptografija je imala bitan uticaj na ishode mnogih vojnih sukoba još od vremena starih Egipćana, Rimljana, uključujući i oba svetska rata. Knjige Simona Singa "The Codebook" [2] i Davida Khan-a "The Codebreakers" [3] daju vrlo dobar netehnički prikaz kriptografije kroz istoriju.

Upotreba kriptografije je osetljiva stvar , pa je iz tog razloga bila vezana isključivo za vojsku i diplomatske krugove sve do pojave savremenih elektronskih komunikacija 60-tih godina. Iako kriptografska literatura nije objavljivana zbog vojnih i nacionalnih tajni postoje i određeni izuzeci. To su dva istorijska članka koji su postavili neke od temelja savremene kriptografije. Prvi je William Friedman-ov "The Index of Coincidence and Its Applications in Cryptography", objavljen 1920. godine [4]. Drugi članak je Claude Shannon-ov "The Communication Theory of Secrecy Systems," objavljen 1949. godine [5]. U stvari oba članka su dela nastala aktivnim učestvovanjem samih autora u ktiptografskoj oblasti tokom prvog tj. drugog svetskog rata. Nedostupnost literature iz kriptografske oblasti nije značilo da se ona nije razvijala, već da je dostupna samo određenim krugovima ljudi unutar vojnih i obaveštajnih službi. Sa ozbiljnijim porastom elektronskih komunikacija, u poslovnom svetu sredinom 60-tih godina prošlog veka, pojavila se potreba i za zaštitom podataka velikih kompanija. Time su se stekli preduslovi za prodor kriptografije van obaveštajnih i vojnih krugova.

Lider u privatnom sektoru, koji je primenio rezultate kriptografskog rada početkom 70-tih godina prošlog veka, je bio IBM. Ekipa naučnika koju je predvodio Horst Feistel, razvila je simetrični blok šifarski sistem pod imenom Lucifer [6]. Na osnovu ovog šifarskog sistema razvijen je još jedan simetričan šifarski sistem pod imenom DES - Data Encryption Standard , 23. novembra 1976. godine [7]. On je usvojen kao američki standard za šifrovanje podataka. DES je postao de-facto standard u poslovnom svetu i najpoznatiji kriptografski mehanizam u istoriji.

Tek, 2001. godine, NIST (National Institute of Standards and Technology), organizacija u SAD, je objavila novi standard za simetrične kriptografske algoritme AES (Advanced Encryption Standard), koji je zamenio prethodni standard DES [8]. Na međunarodnom otvorenom takmičenju za najbolji algoritam, za novi američki standard, proglašen je Rijndael. Rijndael predstavlja blok šifarski algoritam koji podržava promenljivu dužinu bloka informacije (128, 192 i 256 bita), kao i promenljivu dužinu ključa (128, 192 i 256 bita). Ovaj algoritam je delo dvojice belgijskih matematičara Joan Daemen i Vincent Rijmen. Rijndael algoritam je, u odnosu na konkurentske algoritme (MARS, RC6, Serpent, Twofish), bio brži i zahtevao je manje operativne memorije u procesu šifrovanja i dešifrovanja poruka. Rijndael algoritam, sa 128-bitnom dužinom ključa, je brži za oko 2.5 puta u odnosu na 3-DES algoritam. Zvanični naziv ovog standarda je AES. Danas se može reći da je AES preuzeo ulogu DES-a.

Paralelno sa ekipom iz IBM-a, dva naučnika su 1976. godine objavili jedan izuzetno važan članak "New Directions in Cryptography" [9]. U njemu se govori o jednom sasvim novom konceptu kriptografije. Ovaj metod, za razliku od dotadašnjih metoda sa jednim ključem, koristi metod šifrovanja poruke sa jednim ključem, a dešifrovanje se obavlja sa drugim ključem. Takođe, bio je rešen problem razmene ključeva na siguran način za klasičnu, simetričnu, kriptografiju. Whitfield Diffie and Martin Hellman 1976. godine, su predstavili koncept asimetrične kriptografije [9], a nezavisno Ralph Merkle 1978. godine[47], ali nisu imali odgovor na to kako da ga i relizuju. Međutim, ova nova ideja je pokrenula istraživanja u pravcu realizacije. Nakon dve godine Rivest, Shamir i Adleman su pronašli metod praktične realizacije asimetrične kriptografije [10]. U članku "A method for Obtaining digital signatures and Public-Key Cryptosystems " se spominje i metoda kreiranja digitalnog potpisa. Na ovim idejama, u kombinaciji sa napretkom u klasičnoj kriptografiji, zasnovana je i infrastruktura javnih ključeva. Elektronske komunikacije su se proširile i među običnim ljudima. Ljudi su počeli koristiti elektronsku poštu za privatne komunikacije, ali pošto su elektronske komunikacije, u svom izvornom obliku, nesigurnije od standardnih poštanskih komunikacija (elektronska poruka može biti pročitana ili čak i promenjena na svom putu od pošiljaoca do primaoca, a da je to teško ili gotovo nemoguće otkriti), javlja se potreba za njenom zaštitom.

Potpunim nadziranjem od strane vlade ili druge moćne organizacije građanska privatnost bi prestala da postoji. Iz tog razloga se morao naći kompromis između dovoljne bezbednosti i građanske privatnosti. Pojavila se potreba za kriptografijom za širu javnost. Metode su postojale, ali je tehnologija uglavnom bila previše komplikovana, a često i zaštićena patentima. Phil Zimmermann je napravio proizvod koji je na jednostavan način omogućavao šifrovanje i digitalno potpisivanje poruka elektronske pošte. Ovaj program se zove PGP, Pretty Good

Privacy. Zimmermann je nameravao komercijalizovati PGP, ali pošto je izgledalo da će američka vlada zabraniti upotrebu kriptografije za najširu jav-

nost, on je program 1991. godine preko Usenet bulletin board-a, predao svetu na besplatno korišćenje [2]. Ovim gestom praktična kriptografija je postala dostupna svima. Danas postoje mnogi proizvodi koji omogućavaju jednostavnu upotrebu kriptografije za lične potrebe za osiguranje elektronskih komunikacija, ali ih ipak veoma mali procenat ljudi koristi.

NAMENA KRIPTOGRAFIJE

Posle isticanja najvažnijih događaja u istoriji kriptografije istakli bismo i njenu namenu. Definicije koji, se najčešće navode u literaturi vezane za kriptografiju, zasnovane na njenoj nameni, ističu da kriptografija predstavlja istraživanje matematičkih tehnika vezanih za aspekte sigurnosti informacija kao što su poverljivost, integritet podataka, autentikacija i poreklo podataka [11]. Ova definicija obuhvata tri od četiri funkcije ili cilja kriptografije. Ove četiri funkcije su: poverljivost (confidentiality), integritet podataka (data integrity), autentikacija (authentication) i neporicanje (non-repudiation).

1. Poverljivost predstavlja obezbeđivanje da sadržaj informacija nije dostupan nikom drugom do onom kome su informacije namenjene. Ovo je najstarija namena kriptografije. Ponekad se za ovu namenu koriste termini privatnost ili tajnost.

2. Integritet podataka znači osiguravanje nepromenljivosti podataka. Da bi se osigurao integritet, potrebno je obezbediti otkrivanje bilo kakve promene podataka. Pod promenama podataka se podrazumevaju radnje kao što su dodavanje, uklanjanje ili zamena. Uobičajeno je da se detektuju promene podataka od strane neovlašćenih lica.

3. Autentikacija je vezana za razmenu informacija. Namena autentikacije je identifikacija subjekata u procesu razmene informacija kao i sama informacija. Elementi autentičnosti informacije su njeno poreklo, vreme nastajanja i vreme slanja. Ponekad se autentikacija deli na dve klase: autentikacija entiteta i autentikacija porekla podataka.

4. Neporicanje onemogućava negiranje prethodno učinjenih dela od strane bilo kog učesnika u njima. Sa aspekta razmene informacija, ovo znači da ni jedna strana u toj razmeni ne može poreći svoje učešće u razmeni i sadržaj razmenjenih informacija.

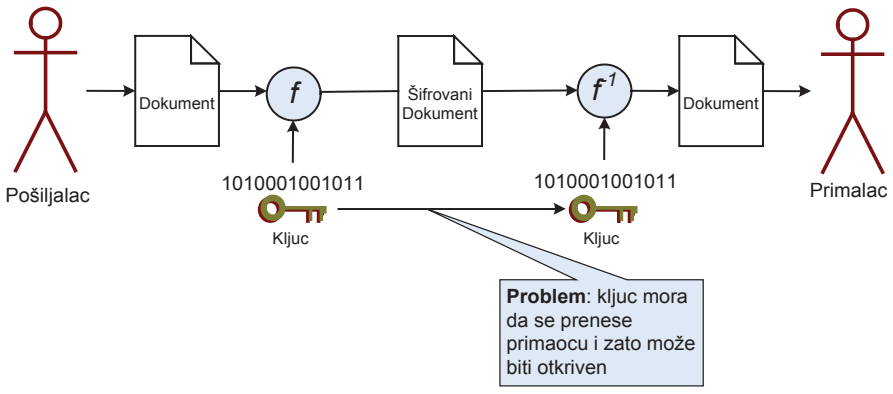
Kriptografija treba da omogući da subjekti, učesnici u sigurnoj komunikaciji, znaju, da su podaci koje razmenjuju dostupni samo njima, da su nepromenjeni tokom prenosa, da se može ustanoviti identitet druge strane i da se ova komunikacija i njen sadržaj ne mogu poreći. Kriptografija treba da spreči i otkrije bilo kakvu vrstu varanja ili nedobronamernog ponašanja u ovoj sferi.

Postoje različite metode kojima se ostvaruju neke ili sve od ove četiri osnovne funkcije kriptografije. Namena kriptografije nije vezana za tipove kriptografije, simetričnu ili asimetričnu. Infrastruktura javnih ključeva, o kojoj je reč u ovom radu, predstavlja sistem koji pruža sve četiri usluge zaštite.

SIMETRIČNA KRIPTOGRAFIJA

Simetrična kriptografija često se još naziva i konvencionalnom kriptografijom jer koristi istu osnovnu ideju kao i kriptografija iz najstarijih vremena, još iz doba „Cezarovih šifri“ [5][6][7].

Za šifrovanje i dešifrovanje, kod simetrične kriptografije, koritsti se isti ključ (slika 2.2.1). Razlika između šifrovanja i dešifrovanja podataka je u tome što se dešifrovanje podataka obavlja



Slika 2.2.1. Proces šifrofanja i dešifrovanja

postupkom šifrovanja, ali obrnutim redosledom. Algoritmi iz ove grupe se takođe nazivaju i algoritmi sa tajnim ključem, jer je tajnost ključa koji se koristi i za šifrovanje i za dešifrovanje, esencijalna za bezbednost poruka u sistemu. Simetrični kriptografski algoritmi obavljaju dve operacije, supstituciju i transpoziciju. Prvi šifratori su obavljali samo jednu od ovih operacija i to samo jednom. Savremeni šifarski sistemi kombinuju ove dve operacije ponavljajući ih više puta. S obzirom da zaštita informacija težišnu primenu ima u poslovima vezanim za državne strukture (vojska, policija i diplomatija), ovi sistemi su bili isključivo tajni sistemi, namenski definisani i realizovani od strane nadležnih državnih institucija. Sa porastom intenziteta i primene elektronskih oblika komunikacija, javila se potreba za definisanjem javnih simetričnih kriptografskih algoritama, pa je u poslednjih desetak godina definisano više javnih simetričnih kriptografskih algoritama za primenu u aplikacijama u kojima za to postoji potreba.

Prvu dokumentovanu upotrebu sistema supstitucije u vojne svrhe primenio je Julije Cezar [2]. Ovaj rimski vladar i vojskovođa je koristio više substitucionih šifratora, od kojih je najpoznatiji onaj u kome je svako slovo alfabeta bilo zamenjeno slovom koje se nalazilo tri mesta dalje u alfabetu. Ova zamena je predstavljala šifrovanje. Za dešifrovanje je bilo potrebno znati da je vršena ovakva vrsta substitucije (algoritam) i da je pomeranje bilo za tri mesta (ključ). Primer:

Otvoreni tekst :	VENIVIDIVICI
Šifrat :	YHQLYLGLYLFL

Transpozicija je permutacija simbola u poruci. Transpozicija je korišćena u prvom vojnom kriptografskom uređaju spartanskom skital (engl. scytale), u petom veku pre nove ere [2]. To je bio drveni štap sl.2.2.2 oko kojeg se namotavala traka od pergamenta, pa se na nju nanosila poruka. Nakon upisivanja poruke, traka bi se odmotala, a na njoj bi ostali izmešani znakovi koje je mogao da pročita samo onaj ko je imao štap iste debljine.

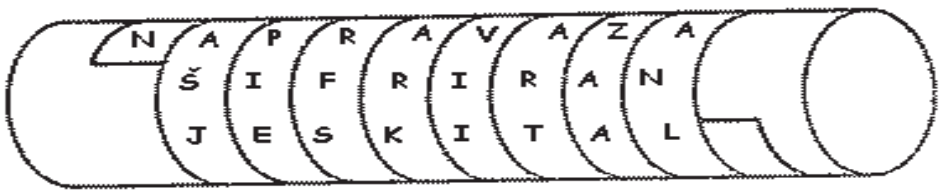
Za dešifrovanje je bilo potrebno znati način na koji je izvršena transpozicija (algoritam) i veličinu ključa. Primer:

Otvoreni tekst :	VENIVIDIVICI
Proces transpozicija:	VENI
	VIDI
	VICI
Šifrat glasi :	VVVEIINDCIII

Substitucija i transpozicija, se mogu obavljati na razne načine, a ne samo na ove pomenute. Bitno je da postoji algoritam i ključ koji su poznati učesnicima u sigurnoj komunikaciji. Teoretsko značenje ove dve operacije je dao Shannon. On je ukazao na to da su ove dve operacije zapravo vezane za tehnike prikrivanja redundantnosti u izvornom tekstu koja se koristi u kriptoanalizi [5].

Simetrični algoritmi se uglavnom koriste u aplikacijama vezanim za sisteme poslovnih i finansijskih komunikacija. Imajući u vidu eksplozivni razvoj poslovnih i finansijskih sistema, u poslednje vreme, javni simetrični kriptografski algoritmi su postali dominantni u pogledu korišćenja. Međutim, nijedan od njih nije usvojen kao generalni standard već pomenuti sistemi uglavnom koriste odgovarajuće liste mogućih kriptografskih algoritama. Na taj način, kao parametar komunikacije, bira se i identifikator simetričnog šifarskog algoritma koji će se koristiti pri datoj transakciji.

Iako je po masovnosti komercijalna upotreba simetričnih kriptografskih algoritama daleko prevazišla upotrebu u tajnom sektoru (vezanom za državne strukture), glavni teorijski rezultati se i dalje dešavaju u oblasti tajne kriptologije i tajnih sistema. Većina država ima specijalizovane or-



Slika 2.2.2. Drveni štap skital

ganizacije koje se bave dizajniranjem i analizom raznih vrsta šifarskih sistema (npr. NSA u SAD). Stepeni dostignuća u toj oblasti najčešće nisu javno poznati i nalaze se u sferi pretpostavki.

Postoje dve osnovne vrste simetričnih šifarskih sistema:

- blok šifarski sistemi,
- sekvencijalni šifarski sistemi (stream cipher).

Sekvencijalni šifarski sistemi koriste samo supstituciju, a blok šifarski sistemi koriste i supstituciju i permutaciju [12]. Blok šifarski sistemi procesiraju blokove nešifrovanog signala - otvorenog teksta (OT) i šifrovanog signala – šifrata (ST), obično u blokovima čija je veličina 64 bita ili više. Sekvencijalni šifarski sistemi procesiraju nizove bita, bajtova ili reči (16 ili 32 bita) OT i ST. Ako se u toku procesa šifrovanja jedne poruke, nekim blok šifarskim sistemom više puta pojavljuje isti blok otvorenog teksta, (OT) rezultat će biti uvek isti blok šifrata (ST), što nije slučaj kod sekvencijalnih šifarskih sistema. Kod sekvencijalnih šifarskih sistema, verovatnoća da isti niz bita, bajtova ili reči OT pri svakom pojavljivanju u jednoj poruci, proizvodi isti šifrat, teži nuli. Blok šifarski sistemi se veoma mnogo koriste u sistemima poslovnih i finansijskih transakcija, ali su njihove bezbednosne osobine dosta slabije od sekvencijalnih šifarskih sistema. I pored toga definisan je veliki broj javnih algoritama baziranih na blok šifarskim sistemima, kao što su DES, 3-DES, RC2, IDEA, i mnogi drugi koji su našli veoma široku primenu u savremenim informacionim sistemima.

Kako je već rečeno, za proces šifrovanja i dešifrovanja u simetričnoj kriptografiji, potrebno je znati algoritam i ključ. U prošlosti su se algoritmi držali u tajnosti, ali je praksa pokazala da prikrivanje algoritma ne doprinosi sigurnosti.

Sigurnost dobrog sistema zasnovana je na dužini i sigurnosti ključa, a ne na tajnosti algoritma. Svi savremeni kriptografski algoritmi su javno dostupni. Na ovaj način ih je moguće u potpunosti testirati na sve vrste napada, odnosno kriptoanalize. Razlog, iz kog je DES zamenjen AES-om kao novim standardom, je prvenstveno dužina ključa od 56 bita. Ovaj ključ je, sa današnjim nivoom razvoja računara i računarskih mreža, postao podložan napadima ispitivanjem svih njegovih kombinacija (engl. brute force analysis). Javno razbijanje šifre zaštićeno DES-om je bilo 1997. godine. Electronic Frontier Foundation je 1998. godine za manje od $250.000 izgradila računar specijalne namene za pronalaženje DES ključa, koji je za manje od tri dana uspeo otkriti ključ [15].

Sa današnjim dužinama ključa, od 128 bita i više, broj kombinacija je isuviše veliki da bi kratkoročna sigurnost algoritama bila ugrožena. Potrebno je naći siguran način distribucije ključeva, od jedne do druge strane u komunikaciji, pre nego što sigurna komunikacija može početi. Pošto je sigurnost svih šifrovanih informacija zasnovana na sigurnosti ključa, otkrivanjem ključa otkrivaju se i sve informacije šifrovane tim ključem. Sigurna razmena ključeva, pogotovo na velike daljine, može predstavljati vrlo ozbiljan problem.

Ako je potrebno, a uglavnom jeste, za svaki par subjekata u sistemu koji žele sigurno komunicirati imati poseban ključ, broj ključeva veoma brzo raste sa rastom broja korisnika sistema. Za n korisnika potrebno je imati n(n - 1)/2 ključeva. Generisanje ovolikog broja ključeva i upravljanje njima postaje vrlo nepraktično za veliki broj korisnika kakav je danas uobičajen u sistemima komunikacije. Broj mogućih ključeva je toliko velik da je praktično nemoguće u zamislivom vremenu i uz svu raspoloživu računarsku snagu ispitati sve moguće kombinacije primenom grube sile. O izboru odgovarajuće dužine ključa biće diskutovano u narednom poglavlju.

Prednosti simetrične kriptografije leže u činjenici da su simetrični kriptografski postupci vrlo brzi. Tajni simetrični ključ ima dvostruku ulogu. Sa njim se vrši proces kriptovanja i dešifrovanje poruke i sme biti poznat samo stranama koje žele bezbedno da komuniciraju. Iz ovog zahteva proizilazi najveći nedostatak simetričnih kriptosistema. Postavlja se pitanje na koji način će dve strane razmeniti tajni ključ, ako nisu u mogućnosti fizički se sastati i dogovoriti. Razmena tajnog ključa nesigurnim mrežnim kanalom nije moguća, jer će svako ko presretne mrežnu komunikaciju znati ključ i biti u mogućnosti razumeti ili promeniti sve kasnije poruke koje se šalju mrežom. Simetrična kriptografija ne može dati odgovor na ovo pitanje. Za rešavanje problema razmene tajnih ključeva koriste se postupci asimetrične kriptografije.

ASIMETRIČNA KRIPTOGRAFIJA

Razvoj savremenih elektronskih komunikacija, a pogotovo računara i računarskih mreža, učinili su problem distribucije ključeva simetrične kripto-

grafije još većim. Računarske mreže omogućavaju brzu razmenu podataka, ali u svojim počecima nisu pravljene da budu veoma sigurne. Da bi upotreba računarskih mreža bila sigurnija, bilo je potrebno organizovati distribuciju ključeva na neki drugi način. Kako je u istorijskom pregledu rečeno, 1976. godine su Diffie i Hellman predložili sasvim novi koncept u kriptografiji - asimetrična kriptografija [9]. Umesto jednog istog ključa, za šifrovanje i dešifrovanje, predloženo je postojanje para ključeva: javnog i privatnog. Javni ključ je dostupan svima i to je ključ koji se koristi za šifrovanje podataka. Odgovarajući privatni ključ je tajni i samo taj ključ omogućava dešifrovanje podataka šifrovanih javnim ključem. Na ovaj način se rešava problem distribucije ključeva i njihovog broja. Svaki subjekt koji želi sigurnu komunikaciju može objaviti svoj javni ključ i svako ko mu želi poslati šifrovanu poruku koristi taj ključ za šifrovanje. Pošto jedino ovaj subjekt ima privatni ključ koji može dešifrovati podatke, obezbeđena je poverljivost podataka. Nema potrebe za posebnim sigurnosnim kanalima za distribuciju ključeva i generisanje ključeva pri svakoj komunikacji. Videti sliku 2.3.1:

Slika 2.3.1. Primer algoritma sa asimetričnim ključevima

Ideja asimetrične kriptografije rešava problem distribucije ključeva, ali Diffie i Hellman nisu predložili konkretan način realizacije. Da bi ovakav sistem radio, neophodno je obezbediti da se na osnovu znanja javnog ključa ne može izračunati privatni ključ. Ova dva ključa moraju biti matematički povezana, tako da će uvek biti teoretski moguće izračunati jedan iz drugog, ali ovo treba učiniti računski neisplativim. Odnosno, resursi potrebni za izračunavanje privatnog ključa iz javnog ključa treba da budu nesrazmerno veći od vrednosti informacija koje se šifruju. Sa druge strane, potrebno je obezbediti jednostavno i brzo šifrovanje i dešifrovanje. Za ovo je potrebna takozvana "jednosmerna funkcija sa tajnim prolazom" (trap-door one-way function). Funkcija je jednosmerna jer je lako izračunati u jednom pravcu (šifrovanje), a nesrazmerno teže u drugom (dešifrovanje). "Tajni prolaz" znači da je funkciju lako izračunati i u težem pravcu, ako se poseduje tajna informacija (privatni ključ).

Prvu ovakvu transformaciju su obavili Rivest, Shamir i Adleman, u prethodno pomenutom članku, 1978 [10]. Njihove originalne metode šifrovanja i dešifrovanja slede u nastavku:

Poruku koja se šifruje potrebno je predstaviti kao celi broj između 1 i n-1.

Zapravo poruku je potrebno razbiti u blokove koji se mogu predstaviti na ovaj način. Ovo predstavljanje niza karaktera preko celog broja nije predmet algoritma, već standardna transformacija. Broj n će biti u nastavku precizno definisan.

Šifrovanje poruke se obavlja dizanjem poruke, odnosno broja M kojim je ona predstavljena, na e-ti stepen po modulu n. Rezultat, ostatak deljenja Me na n je šifrovana poruka, C. Dešifrovanje se obavlja dizanjem šifrovane poruke, odnosno broja kojim je ona predstavljena, na d-ti stepen po modulu n. Odnosno, ostatak deljenja Cd na n je originalna poruka M. Matematički zapisano:

$C \equiv E(M) \equiv Me \pmod n$; šifrovanje poruke M u C.

$M \equiv D(C) \equiv Cd \pmod n$; dešifrovanje C u originalnu poruku M.

Javni ključ, koji se koristi za šifrovanje, je par celih brojeva (e; n).

Privatni ključ, koji se koristi za dešifrovanje, je par celih brojeva (d; n).

Vrednosti za n, e i d se biraju na sledeći način:

- broj n je proizvod dva vrlo velika "slučajna" prosta broja:

$n = p * q$

Iako je n javno, faktori p i q ostaju tajni zbog velike težine rastavljanja broja na proste faktore. Na ovaj način je onemogućeno dobijanje d, drugog dela privatnog ključa, iz e, drugog dela javnog ključa.

- broj d se bira da bude veliki, slučajan celi broj koji nema zajedničkih faktora sa $(p - 1) * (q - 1)$, odnosno da d zadovoljava:

$NZD(d; (p - 1) * (q - 1)) = 1$

- broj e se računa iz p, q i d da bude "multi-

plikativna inverzija" d moduo
(p – 1) * (q – 1), što znači,
e * d ≡ 1 (mod (p – 1) * (q – 1))

Matematički dokaz ispravnosti metode je dat u navedenom radu [10]. Ovaj algoritam nazvan je RSA po inicijalima prezimena autora. RSA algoritam je realizovao koncept asimetrične kriptografije. Šifrovanje je bilo vrlo jednostavno, a dešifrovanje neuporedivo teže bez poznavanja privatnog ključa d. Za one koji znaju vrednost d, postupak dešifrovanja je jednostavan. Dešifrovanje bez poznavanja vrednosti d, postaje praktično nemoguće, ako su p i q, odnosno n dovoljno veliki. Rivest, Shamir i Adleman su predložili 100 cifrene p i q, odnosno 200 cifreni n. Veći n donosi veću sigurnost, ali usporava šifrovanje i dešifrovanje. Pitanje izbora velikih prostih brojeva p i q, pitanje izbora d, te pitanje računanja e, su obrađeni još u izvornom članku [10], a i mnogo puta kasnije. Ispostavilo se da nijedna od ovih operacija ne predstavlja ozbiljniji problem, te da je RSA vrlo praktičan i upotrebljiv algoritam šifrovanja i dešifrovanja. Sigurnost RSA algoritma je zasnovana na težini rastavljanja broja na proste faktore. Ovo se smatra jednim od teških problema za koje ne postoji brz i jednostavan algoritam, već samo poboljšanja u odnosu na pretraživanje svih mogućih kombinacija. Ovim problemom se matematičari bave preko 300 godina i smatra se da je prilično dobro izučen. Od 1978. godine kada je RSA predstavljen, nije bilo dovoljno značajnog napretka u ovoj oblasti koji bi ugrozio sigurnost RSA. Ne postoji nikakva garancija da se jednom, možda čak i u skoroj budućnosti, neće naći brza i jednostavna metoda za rastavljanje velikih brojeva na proste faktore, ali to razmatranje već izlazi iz okvira ovog rada.

Od 1978. godine objavljeno je više algoritama koji implementiraju ideju asimetrične kriptografije. Svi predloženi algoritmi nisu jednako sigurni ni praktični. U široj upotrebi se pored RSA koriste još i ElGamal algoritam [16], i kriptografski sistemi bazirani na eliptičkim krivama [17], [18]. Ovi, asimetrični kriptografski algoritmi, se uglavnom nazivaju algoritmi sa javnim ključem. Asimetrična kriptografija je rešila problem distribucije ključeva, ali i ona ima svoje nedostatke [12]:

- algoritimi sa javnim ključem su od 100 do 1000 puta sporiji od simetričnih algoritama;
- kriptosistemi sa javnim ključem su podložni jednoj vrsti kriptoanalize koja se naziva napad na izabrani izvorni tekst (chosen-plaintext attack).

U savremenoj praktičnoj upotrebi algoritmi sa javnim ključem, nisu zamenili simetrične algoritme, već se koriste za različite namene. Algoritmi sa javnim ključem se koriste najčešće za šifrovanje ključeva koji se koriste za šifrovanje podataka koji se razmenjuju simetričnim algoritmima. Primer ovoga su vrlo korišćeni, takozvani, hibridni kriptosistemi kod kojih se simetrični algoritam sa slučajnim sesijskim ključem koristi za šifrovanje poruka, a algoritam sa javnim ključem za šifrovanje tog slučajnog sesijskog ključa [50].

Izbor odgovarajućih dužina ključeva je od kritičnog značaja za implementaciju odgovarajuće sigurnosti. Veća dužina ključa znači i veću sigurnost, ali i duže vreme potrebno za kriptografske operacije. Sigurnost izabranog RSA algoritma, leži u pretpostavljenoj težini rastavljanja velikog broja na proste faktore. Napretkom u algoritmima i tehnologiji smanjuje se vreme potrebno za ove operacije, odnosno, sve veći brojevi se mogu rastaviti na proste faktore u sve kraćem vremenu. 2003 godine, najveći broj rastavljen na proste faktore je 576 bitni broj (174 decimalne cifre) [19]. Ovo je u decembru 2003 godine postigla grupa naučnika sa nekoliko nemačkih univerziteta [20]. Korišćeni algoritam bio je number field sieve algoritam (najbrži postojeći algoritam brojeva većih od 110). Računarsko vreme, mereno u MIPS (milion instrukcija u sekundi) godinama potrebno za rastavljanje brojeva različite dužine na proste faktore, po ovom algortimu, prema dostupnoj proceni [12], dato je u tabeli 2.3.1:

Jedna MIPS (milion instrukcija u sekundi) godina se definiše kao količina računanja koje se može proizvesti u toku godinu dana, na računaru, sposobnom da proizvede milion instrukcija u sekundi.

Savremeni Pentium 4 procesori, obavljaju oko 2000 miliona instrukcija u sekundi [21][22]. Ovo znači da bi 15 računara sa ovakvim procesorima, radeći neprekidno godinu dana, uspeli rastaviti broj dužine 512 bita na proste faktore. Na ovaj način bi se iz javnog RSA ključa moglo doći do privatnog ključa i u potpunosti eliminisati sve elemente sigurnosti sistema. Prema tome, može se reći da već danas 512-to bitni ključ nije dovoljno siguran. Ključevi od 768 i 1024 bita izgledaju bezbedni u sadašnjem trenutku. Izabrane veličine ključeva, treba da nude sigurnost i na duži vremenski rok. Vrlo je nezahvalno praviti dugoročne prognoze u ovoj oblasti. Ipak je neophodno doneti odluku o dužini ključeva zasnovanu na nekim prognozama. Menezes i Jurišić su upoređivali potrebna vremena za probijanje ECC i RSA šifri [44], a u članku iz 2001. godine [45], Lenstra i Verheul su dali preporuke za dužine ključeva koje bi trebalo koristiti kako bi se postigla zadovoljavajuća sigurnost. Data su i predviđanja o kretanju dužina

Broj bita	Potreban broj MIPS godina za rastavljanje
512	$3*10^4$
768	$2*10^8$
1024	$3*10^{11}$
1280	$1*10^{14}$
1536	$3*10^{16}$
2048	$3*10^{20}$

Tabela 2.3.1. Broj MIPS godina za rastavljanje brojeva na proste faktore

ključeva u budućnosti. U svojim preporukama su uzeli u obzir više varijabilnih parametara. Jedan od osnovnih parametara uzima u obzir razumnu pretpostavku da najbolji javno objavljeni rezultati o razbijanju pojedinih kriptosistema, ne predstavljaju garanciju da ne postoje i bolji (neobjavljeni) rezultati. Za parametar koji uzima ovu pretpostavku u obzir, uzeli su zadnju godinu u kojoj se smatra da je najpopularniji simetrični kriptosistem DES bio siguran. DES je kao standard prihvaćen 1976. godine. Dužina ključa je bila 56 bitova i smatralo se da je premala, a javno razbijanje šifre zaštićene DES-om desilo se 1997. godine. U proračunu podataka koristi se pretpostavka da je zadnja godina u kojoj je DES bio siguran bila 1982. godina. Važno je napomenuti da predviđanja ne uzimaju u obzir moguću konstrukciju kvantnih računara, koja bi sve kriptosisteme sa javnim ključem, koji su danas u upotrebi, učinila nesigurnim.

U tablici 2.3.2 nalaze se preporučene dužine ključa u bitovima, za simetrične kriptosisteme (DES, AES), za kriptosisteme zasnovane na faktorizaciji ili diskretnom logaritmu u konačnom polju (RSA, ElGamal) i kriptosisteme zasnovane na eliptičkim krivama i procena kompjuterskog vremena potrebnog za razbijanje šifre u MIPS-godinama [45]:

Pre konačne odluke o potrebnoj dužini ključeva potrebno je razmotriti i negativnu stranu dužih ključeva. Kriptografske operacije, kod asimetrične kriptografije, su računski intenzivne, na primer pri generisanju novog para ključeva koje se odvija prilikom kreiranja sertifikata i dodeljivanja javnog ključa subjektu. Kreiranje para ključeva kod izabranog RSA algoritma uključuje pronalaženje pogodnog para prostih brojeva, i izračunavanje javnog i privatnog ključa na osnovu ovih brojeva, kako je u teoretskim osnovama objašnjeno.

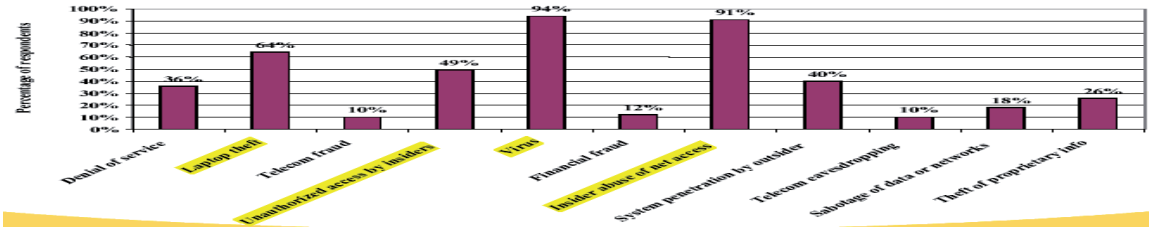
Godina	DES dužina ključa	RSA dužina ključa	ECC dužina ključa	MIPS godina
1990	63	622	117	$3.51*10^7$
2000	70	952	132	$7.13*10^9$
2010	78	1369	146	$1.45*10^{12}$
2020	86	1881	161	$2.94*10^{14}$
2030	93	2493	176	$5.98*10^{16}$
2040	101	3214	191	$1.22*10^{19}$

Tabela 2.3.2. Preporučene dužine ključeva i vreme potrebno za razbijanje šifri

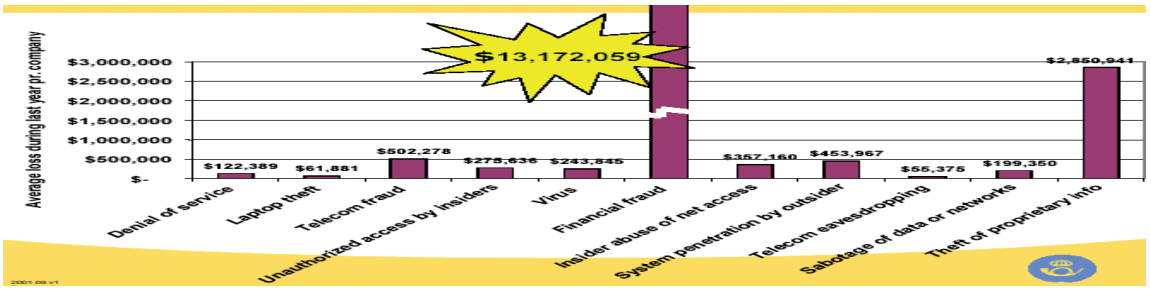
POTENCIJALNI NAPADI NA RAČUNARSKE MREŽE BAZIRANE NA INTERNETU I MOGUĆI NAČINI ODBRANE

Uporedo sa razvojem i implementacijom računarskih mreža Internet tipa, razvijaju se i različiti mehanizmi zaštite, specijalizovani za odbranu od pojedinih vrsta napada. U startu treba biti svestan da računarske mreže Internet tipa, pored toga što omogućavaju izuzetno povećanje efikasnosti rada i smanjenje troškova, predstavljaju kritičnu tačku bezbednosti date organizacije sa stanovišta bezbednosti informacija koje se u sistemu prenose. U svetu postoji veliki broj različitih pregleda i analiza opasnosti korišćenja računarskih mreža na bazi Internet tehnologija, izrađenih od strane relevantnih institucija. Jedna takva analiza, data u [26], ukazuje na tipove napada, u procentima prijavljenih napada slika 3.1, kao i prosečne gubitke prouzrokovane tim napadima u 2001. godini, slika 3.2. Druga analiza pokazuje gubitke u slučajevima primene magnetnih platnih kartica u Nemačkoj [27], slika 3.3.

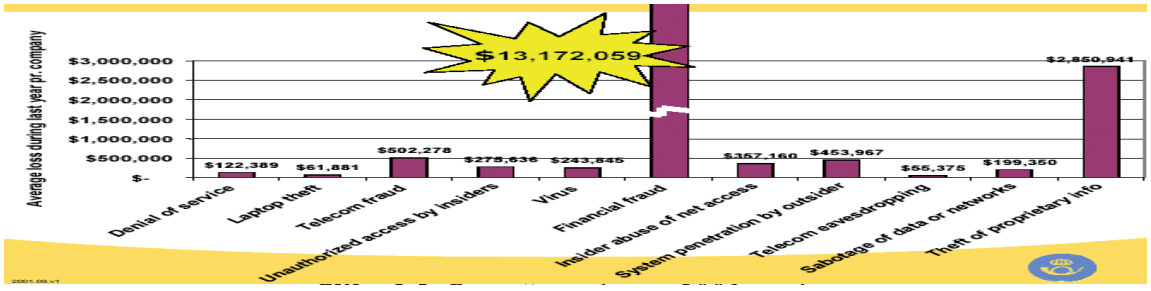
Prema jednom sličnom pregledu američkog instituta za zaštitu računara (Computer Security Institute - CSI 2000 Computer Crime and Security Survey) koji je obuhvatao velike korporacije, 70% razmatranih subjekata je prijavilo detektovane neautorizovane pristupe u svojim mrežama u prethodnoj godini. Takođe, prema istoj analizi, u prethodnih 5 godina, 66 razmatranih subjekata je prijavilo ukupan



Slika 3.1. Tipovi prijavljenih napada na računarske mreže u procentiama



Slika 3.2. Prosečni gubici u 2001. godini



Slika 3.3. Gubici u primeni magnetnih platnih kartica u Nemačkoj

gubitak proizveden krađom osetljivih korporacijskih informacija u iznosu od $66 708 000, a 54 razmatrana subjekta su prijavila ukupan gubitak proizveden finansijskom proneverom u iznosu od $53996000.

Ova analiza je takođe potvrdila sledeće trendove u korišćenju računarskih mreža Internet tipa u poslednje vreme:

- Razvoj sve šireg spektra mogućih napada;
- Napadi na korporacijske računarske mreže Internet tipa mogu biti eksterni i interni. Iako su prethodnih godina napadi na računarske mreže Internet tipa bili pretežno eksterni, novije analize pokazuju da mnogo veću štetu i finansijske gubitke nanosi širok spektar internih napada. Razlozi za to leže u samoj prirodi mreža Internet tipa u kojima interni učesnici nisu samo zaposleni u datoj korporaciji (za koje postoji određeni stepen poverenja), već i poslovni partneri, zaposleni u firmama podružnicama, kooperanti, dostavljači, itd., koji iz razloga jednostavnosti korišćenja i povećanja efikasnosti i produktivnosti rada imaju vrlo sličan, ako ne i isti, pristup korporacijskoj mreži kao i zaposleni u datoj korporaciji;
- U poslednje vreme su zabeleženi veoma veliki finansijski gubici prouzrokovani napadima na računarske mreže Internet tipa;
- Uočeno je da primena samo komercijalnih tehnologija zaštite informacija ne može predstavljati pouzdano rešenje odbrane od potencijalnih napada, već da se mora koncipirati i primeniti slojevita i sveobuhvatna politika zaštite koja će pored komercijalnih tehnologija zaštite obavezno uključiti i primenu kvalitetnijih, sopstveno realizovanih mehanizama zaštite, kao i mehanizama kontrole pristupa i organizacionih elemenata zaštite date računarske mreže Internet tipa;

Sa druge strane, SANS[19] Institut je obavio istraživanja koja su rezultovala u definisanju tri liste osnovnih grešaka koje omogućavaju različite vrste napada na mreže Internet tipa i pojedinačne radne stanice u mreži.

Prva lista se odnosi na krajnje korisnike i definiše sledećih pet najvećih bezbednosnih grešaka [43]:

- Otvaranje nezahtevanog e-mail priloga (attachment) dobijenog od nepoverljivog izvora;
- Propust da se instaliraju bezbednosni patch-evi standardnih Internet programskih paketa, kao i novih definicija (upgrade) antivirusnih programa;
- Instaliranje i download-ovanje screen saver-a i igara od nepoverljivih izvora;
- Nekreiranje i netestiranje back-up operacija;
- Korišćenje modema dok ste vezani u lokalnoj računarskoj mreži (LAN).

Druga lista se odnosi na korporacijske uprave (menadžment) i definiše sledećih sedam najvećih bezbednosnih grešaka koje utiču na slabosti korporacijske računarske mreže:

- Neobezbeđenje odgovarajućeg broja službenika koji treba da uspostave i održavaju sistem zaštite u okviru korporacije;
- Primena samo organizacionih vidova zaštite bez primene (i bez prihvatanja neophodnosti primene) mehanizama zaštite informacija;
- Rešavanje samo pojedinačnih bezbednosnih problema bez primene mera i stvaranja uslova za kreiranje kompletnog sistema zaštite koji bi osigurao rešenje najšireg spektra bezbednosnih problema;
- Korišćenje samo mrežnih barijera (firewall) u korporacijskoj računarskoj mreži;
- Neshvatanje koliko vrede intelektualno vlasništvo i poslovna reputacija firme;
- Primena kratkotrajnih rešenja pojedinačnih situacija što dovodi do brzog umnožavanja bezbednosnih problema;
- Pretvaranje da će se bezbednosni problemi rešiti sami od sebe ako se ignorišu.

Treća lista se odnosi na informatičke profesionalce i definiše sledećih deset najvećih bezbednosnih grešaka:

- Priključivanje računarskog sistema na Internet bez prethodne primene svih neophodnih bezbednosnih mera da se to učini;
- Priključivanje sistema na Internet sa default lozinkama;
- Propust da se sistem ažurira sa rešenjima nekih bezbednosnih problema;
- Korišćenje nekriptovanih protokola za

19. SANS (SysAdmin, Audit, Network, Security) Institute, http://www.sans.org

upravljanje sistemima, ruterima, firewallovima i PKI infrastrukturom;
- Davanje korisnicima lozinki preko telefona i njihovo menjanje bez prethodne autentikacije osobe koja zahteva izmenu;
- Propust pri održavanju i testiranju procedure back-up-a sistema;
- Korišćenje nepotrebnih Internet servisa;
- Primena mrežnih barijera sa pravilima koja ne osiguravaju bezbedno osetljivi dolazeći i odlazeći saobraćaj;
- Propust u implementaciji i ažuriranju softverskog paketa za detekciju virusa;
- Propust u edukaciji korisnika u odnosu na to šta je potrebno učiniti kada se uoči potencijalni bezbednosni problem.

Imajući u vidu prethodno rečeno, u nastavku su sumirani najčešći vidovi potencijalnih napada i moguće odbrane u okviru TCP/IP distribuiranih računarskih sistema.

Najčešći vidovi napada na računarske mreže Internet/Intranet tipa su:

- Prisluškivanje (Eavesdropping) – neovlašćeno pristupanje podacima u otvorenom obliku i lozinkama. Generalno većina elektronske komunikacije odvija se u formi čistog teksta (plaintext) nekriptovan format, koji omogućava napadaču koji je uspeo da provali u sistem da nadgleda i čita navedenu komunikaciju. Sposobnost prisluškivača da nadgleda mrežni saobraćaj predstavlja najveći problem sigurnosti sa kojim se administratori susreću u kompaniji. Bez jakih servisa zaštite koji se zasnivaju na kriptografiji, podaci su lako dostupni drugima dok putuju kroz mrežu;
- Lažno predstavljanje identiteta (Identity spoofing – IP address spoofing) – Većina mreža i Operativnih sistema koriste IP adrese za identifikaciju računara na mreži. U nekim slučajevima moguće je falsifikovanje IP adrese. Ova pojava je poznata pod nazivom Identity spoofing. Napadač može upotrebiti specijalne programe da napravi IP pakete koji se pojavljuju u mrežnom saobraćaju i to kroz registrovane adrese u okviru intraneta kompanije. Nakon ulaska na mrežu bez validne IP adrese, napadač može da modifikuje, preusmeri i obriše podatke. Napadač takođe može da organizuje i druge tipove napada koji će biti opisani u nastavku;
- Napad tipa ukidanja servisa (Denial of service attack) - Ovaj tip napada sprečava normalnu upotrebu računara odnosno mreže. Nakon uspešnog ulaska u mrežu napadač može da uradi bilo šta od navedenog:

- Da ometa osoblje koje održava informacioni sistem i na taj način ih spreči da momentalno detektuju napad. Ovo daje napadaču mogućnost da organizuje dodatne napade;

- Da šalje netačne podatke aplikativnim i mrežnim servisima i resursima sprečavajući njihovo normalno funkcionisanje;

- Da generiše ogromnu količinu saobraćaja sve dok celokupan sistem ne padne;

- Da blokira saobraćaj, što rezultuje nemogućnost pristupa mreži od strane ovlašćenih korisnika.

- Izmena poruka (Data modification) –Nakon što napadač pročita podatke, njegov sledeći logičan korak je najčešće modifikovanje istih. Napadač može da vrši izmenu podataka u paketu bez znanja pošiljaoca ili primaoca poruke;
- Pogađanje lozinke (Password based attack) – Neovlašćeni pristup podacima uz pomoć otkrivene lozinke. Kontrola ulaza pomoću passworda je najčešći oblik kontrole operativnih sistema i mreža. Ulaz u računar i mrežu definišu se kroz username i password. Starije verzije operativnih sistema nisu uvek dozvoljavale zaštitu identiteta dok je u toku proces autorizacije. To omogućuje napadaču da sazna username i password, a zatim ih iskoristi da bi provalio u mrežu. Kada napadač pogodi šifru on dobija ista prava kao i pravi korisnik. Ako korisnik ima administratorska prava, napadač može da napravi dodatni korisnički nalog koji može kasnije da koristi. Nakon ulaska na mrežu napadač može da uradi bilo šta od navedenog:

- Da prikupi liste registrovanih korisničkih naloga i njihovih imena kao i informacije sa mreže;

- Da modifikuje serverske i mrežne konfiguracije, uključujući kontrolu ulaza i tabelu za usmeravanje saobraćaja;

- Da modifikuje, preusmerava i briše podatke;

- Kriptoanaliza – otkrivanje tajnih ključeva (engl. Compromised key attack)– otkrivanje podataka u otvorenom obliku na bazi šifrata i otkrivenog tajnog ključa. Ključ je tajni broj za šifrovanje, dešifrovanje odnosno verifikaciju podataka. Iako je otkrivanje ključa težak resursno zahtevan proces za napadača, to je ipak moguće. U slučaju

njegovog otkrivanja ključ postaje kompromitovan. Napadač koristi ključ da bi ostvario pristup zaštićenoj komunikaciji, a pošiljalac i primalac nisu ni svesni napada. Sa kompromitovanim ključem napadač može da dešifruje šifrovane podatke. Napadač može takođe uz pomoć kompromitovanog ključa da napravi dodatne ključeve uz pomoć kojih bi mogao da stekne pristup drugoj obezbeđenoj komunikaciji;

- „Man in the middle“ napad – (engl. Man in the middle attack), Ovaj tip napada postoji kad se napadač nađe između dva korisnika koja komuniciraju i aktivno nadgleda kontroliše i uzima podatke bez znanja ovih korisnika. Na primer napadač može da učestvuje pri razmeni ključeva oba korisnika. Svaki korisnik na taj način šalje šifrovane podatke napadaču koji ih momentalno dešifruje. Kada računari komuniciraju na nižem nivou mrežnog sloja, računari nisu u mogućnosti da odrede sa kojim računarom razmenjuju podatke;
- Sniffer attack – sniffer je program ili uređaj koji može da čita nadgleda i pribavlja podatke i pakete sa mreže. Ako paketi nisu šifrovani sniffer obezbeđuje kompletan uvid u podatke koji se nalaze u okviru paketa. Čak i enkapsulirani paketi koji prolaze kroz tunel mogu da se otvore i čitaju ako nisu šifrovani. Pomoću sniffera napadač može da uradi sledeće:

- Da analizira mrežni saobraćaj i ima neovlašćeni pristup informacijama, što može da ima za posledicu prekid mrežnog saobraćaja;

- Da čita privatnu komunikaciju.

- Napad na nivo Aplikacija (engl. Application layer attack) - Ovaj tip napada pogađa aplikativne servere izazivajući greške u operativnom sistemu odnosno aplikacijama. Kao rezultat napada javlja se mogućnost napadača da preuzme kontrolu pristupa na sistem. Napadač koristi ovu situaciju tako što dobija kontrolu nad aplikacijama ili nad sistemom tako da može da uradi i bilo šta od navedenog:

- Da čita modifikuje i briše podatke ili Operativni sistem;

- Da instalira virus koji će zaraziti ostale korisničke računare na mreži;

-Da instalira sniffer program kako bi analizirao mrežni saobraćaj i dobio informacije koje mogu da prouzrokuju pad sistema kao i ometanje njegovih funkcija;

-Da onemogući ostale sigursnosne kontrole i obezbedi buduće napade.

- Napadi tipa Trojanskog konja – distribucija zlonamernih programa na radne stanice;
- Virusi – uništenje podataka.

Iako pomenuti napadi nisu specifični samo za TCP/IP računarske mreže, oni su tu najviše ispoljeni, jer se najveći broj računarskih mreža u svetu bazira na Internet tehnologijama.

Mogući načini odbrane od navedenih napada su sledeći [43]:

- Šifrovanje – zaštita tajnosti podataka i lozinki;
- Primena tehnologije digitalnog potpisa – provera autentičnosti, zaštita integriteta podataka i obezbeđenje neporecivosti za sadržaj poslate poruke;
- Procedura jake autentikacije – bezbedna međusobna autentikacija strana u komunikaciji;
- Korišćenje jakih ključeva i česta izmena ključeva – sprečavanje metoda kriptoanalize;
- Zaštita adresa servera – zaštita od napada tipa ukidanje servisa;
- Korišćenje digitalnih sertifikata kao jednoznačnih identifikacionih parametara subjekata u komunikaciji;
- Korišćenje smart kartica za generisanje digitalnog potpisa i bezbedno čuvanje ključeva i drugih kriptografskih parametara;
- Višeslojna antivirusna zaštita.

U cilju odbrane od navedenih potencijalnih napada na mrežu, najsvrsishodnije je primeniti kombinovane metode zaštite koje se sastoje od većine gore navedenih metoda.

VIŠESLOJNA ARHITEKTURA SISTEMA ZAŠTITE SAVREMENIH RAČUNARSKIH MREŽA

U cilju optimalne odbrane savremenih računarskih mreža od potencijalnih opasnosti i raznovrsnih napada kojima se ugrožavaju mrežni resursi, predlaže se arhitektura sistema zaštite koja se sastoji od tri nezavisna bezbednosna nivoa koji su namenjeni za

odbranu od različitih tipova napada [43]. Ovi nivoi su projektovani da minimizuju i ograniče moguću štetu tako što, eventualno ugrožavanje jednog nivoa, ne može kompromitovati ostale bezbednosne nivoe arhitekture sistema zaštite. Sistem zaštite savremenih računarskih mreža bi trebalo da se sastoji od sledeća tri nivoa:

- Zaštita "s kraja na kraj" (end-to-end security) ili zaštita na aplikativnom nivou se zasniva na primeni tehnologije digitalnog potpisa na bazi asimetričnih kriptografskih algoritama i zaštite tajnosti podataka primenom simetričnih kriptografskih algoritama. Primenom ovog nivoa zaštite globalno se obezbeđuje: provera autentičnosti korisnika servisa mreže kako u smislu komunikacije (end-user authentication) tako i u smislu kontrole pristupa mreži (access control), zaštitu integriteta podataka koji se prenose, zaštitu od eventualne mogućnosti naknadnog poricanja poslatih podataka i zaštitu tajnosti podataka;
- Zaštita na transportnom nivou predstavlja zaštitu tajnosti podataka primenom simetričnih kriptografskih algoritama i autentikacije čvorova komunikacionog segmenta mreže. Ovaj nivo štiti mrežu od internih i eksternih napada primenom kriptografskih tunela (zaštićenih sesija), između čvorišta komunikacionog segmenta mreže na bazi simetričnih kriptografskih sistema i primenom procedure "jake" autentikacije (strong authentication), između čvorišta mreže čime se obezbeđuje provera autentičnosti strana u komunikaciji. Dodatnom primenom asimetričnih kriptografskih sistema obezbeđuje se zaštita integriteta podataka koji se prenose kroz mrežu i nemogućnost poricanja emisije datih podataka;
- Zaštita na mrežnom IP nivou obezbeđuje kriptografsku i logičku zaštitu na nivou IP paketa koji se razmenjuju između mrežnih čvorova i štiti čitavu mrežu od eksternih napada korišćenjem:
- Zaštitnih mehanizama koje pruža standardna komunikaciona oprema;
- Zaštite primenom "firewall"-a i IP filtriranja;
- Zaštitnih mehanizama na mrežnom nivou koje pruža sam operativni sistem.

Kriptografska zaštita na aplikativnom nivou zasniva se na primeni asimetričnih i simetričnih kriptografskih sistema, čime se generalno realizuju sledeće funkcije:

- Provera autentičnosti subjekata u komunikaciji (asimetrični sistemi);
- Zaštita integriteta podataka koji se prenose kroz mrežu (asimetrični sistemi);
- Nemogućnost naknadnog poricanja subjekta za poslate podatke (asimetrični sistemi);
- Zaštita tajnosti na aplikativnom nivou bezbednosno kritičnih podataka (simetrični sistemi).

Na bazi ovih principa su razvijeni sistemi i protokoli zaštite koji su postali "de-facto" standardi u zaštiti Internet/Intranet mreža, među kojima su najpozantiji: S/MIME[20], Kerberos[21], Proxy serveri[22] na apli-

20. Secure Multipurpose Internet Mail Extensions. Takođe poznat kao Secure/MIME ili S/MIME. Opisan je u RFC dokumentima 2632-2643. Ovaj standard obezbeđuje proveru identiteta, kotrolu integriteta podataka, tajnost i nemogućnost poricanja. Definisano je više novih MIME zaglavlja, na primer zaglavlje za čuvanje digitalnih potpisa. Nema strogu hijerarhiju sertificiranja koja počinje od jedinstvenog vrha, već korisnici mogu da biraju između više pouzdanih polazišta. Sve dok se za sertifikat može povratno naći pouzdano polazište kome korisnik poklanja poverenje, sertifikat se smatra važećim.

21. Kerberos je Internet Engineering Task Force (IETF) standard. Predstavlja sistem obezbeđenja mreže prvobitno razvijen za projekat Athena na Tehnološkom institutu u Masačusetsu. On je distribuiran sistem sa proverom autentičnosti. Kada se korisnik prijavi, on proverava njegovu legitimnost. Kerberos štiti prenos pomoću posebnih ključeva tzv. Kartica (engl. tickets), kojima se šifruje prenos između Kerberosa i korisnika. Kerberos koristi metode šifrovanja sa privatnim ključem.

22. Proksi server je server čija je uloga u ostvarivanju komunikacije između klijenata unutar mreže i spoljne mreže. On ne predstavlja nužno zaštitnu barijeru (engl. firewall), ali se često koristi kao sastavni deo zaštitne barijere, čime se u dobroj meri može kontrolisati saobraćaj, npr. dozvoljava se da source adresa poslatih paketa može biti samo adresa Proxy-a, a da ostali koji idu van Proxy servera budu odbijeni. Takođe Proxy serveri sadrže i razne Auditing alate koji beleže sav saobraćaj, tako da ukoliko dođe do neke provale logovi mogu biti od velike pomoći.

kativnom nivou, SET[23], IPSec[24] (ISAKMP[25]) i drugi. Danas, najviše korišćen protokol zaštite na aplikativnom nivou je S/MIME (Secure Multipurpose Internet Mail Extension), protokol za standardizovano slanje elektronske pošte. S/MIME aplikacije se najčešće ugrađuju u softverske pakete za slanje poruka, kao što su: Microsoft Outlook, Netscape Communicator, Lotus Notes, Novell, itd. Njihova osnovna karakteristika je da obezbeđuju interoperabilnost rešenja od različitih proizvođača. Ovi sistemi se baziraju na primeni asimetričnih i simetričnih kriptografskih algoritama i digitalnih sertifikata, kao jednoznačnim parametrima identifikacije strana u komunikaciji.

Zaštita tajnosti, na transportnom nivou, se generalno ostvaruje primenom simetričnih šifarskih sistema za ostvarivanje kriptografskog tunela između računara u komunikaciji. Pre uspostave kriptografskog tunela, neophodno je realizovati proceduru bilateralne autentikacije koja se bazira na asimetričnim šifarskim sistemima. Iako se pomenuti mehanizmi mogu namenski razviti za bilo koju mrežu računara, ovi sistemi se uglavnom koriste za zaštitu na transportnom nivou između klijenata koji koriste standardne pakete za Internet pretraživanje (Internet Explorer, Netscape) i web servera. Najpoznatiji korišćeni protokoli su: SOCKS[26] (ranije korišćen), SSL[27], TLS[28] i WTLS[29]. Od ovih sistema se najviše koristi SSL (Secure Sockets Layer) protokol, koji u stvari, predstavlja i daleko najkorišćeniji protokol zaštite u Internet/Intranet računarskim mrežama. SSL protokol se sastoji iz dve faze. Prva faza je postupak autentikacije koji se bazira na asimetričnim kriptografskim sistemima i digitalnim sertifikatima servera (i klijenta opciono) i u kojoj se vrši provera autentičnosti strana u komunikaciji i razmena sesijskog ključa. Druga faza je ostvarivanje kriptografskog tunela koji se bazira na simetričnim kriptografskim sistemima i sesijskom ključu koji je prenesen u fazi autentikacije. WTLS (Wireless Transport Layer Security) je bežična varijanta SSL protokola i služi za zaštitu na transportnom nivou između WAP[30] mobilnih telefona i WAP servera na istim principima i isto u dve faze (autentikacija i kriptografski tunel), kao i SSL protokol. Što se tiče zaštite na aplikativnom nivou u okviru mobilne komunikacije, u finalnoj fazi razvoja se nalazi novi tip identifikacionih kartica pod nazivom WIM (WAP Identity Module) u kojima je implementirana funkcija digitalnog potpisivanja.

Zaštita na mrežnom nivou se ostvaruje šifrovanjem mrežnog linka između dva čvora mreže, bez obzira da li su oni direktno povezani ili su povezani odgovarajućim putanjama koje podrazumevaju veći broj čvorišnih servera. Ove metode najčešće predstavljaju osnovu za realizaciju virtuelnih privatnih mreža (VPN – Virtual Private Networks) na mrežnom nivou. Najpoznatiji protokoli koji se koriste u ovom slučaju su: IPSec (AH, ESP), paketsko filtriranje i protokoli tuneliranja na mrežnom nivou. IPSec (IP Security) se najšire koristi i često je već ugrađen u komunikacione i ruterske uređaje. IPSec se bazira na asimetričnim kriptografskim sistemima (uglavnom) za realizaciju autentikacije i simetričnim sistemima za šifrovanje IP paketa. Postoje različite varijante ovog protokola, a najbezbednije su one koje koriste šifrovanje čitavih IP paketa (zajedno sa hederom i IP adresama) obezbeđujući na taj način da se iz spoljnjeg sveta vidi samo adresa pojedinih IPSec servera (VPN gejtveja), ali ne i računara koji u stvari komuniciraju.

23. Secure Electronic Transaction. Tehnologija razvijena od strane Visa and Mastercard za bezbedna plaćanje putem Interneta.

24. Internet Protocol Security. Opisan je u dokumentima RFC 2401, 2402, 2406. Koristi se pri kreiranju VPN. Koristi IKE protokol za razmenu ključeva i autentikaciju.

25. Internet Security Association and Key Management Protocol. Predstavlja deo IPSec-a i služi za uspostavljanje ključeva. Opisan je u dokumentu RFC 2408.

26. The SOCKS Protocol je Internet protokol koji dopusta klijent server aplikaciji da transparentno koristi servise mrežnih barijera.

27. Secure Sockets Layers. Protokol razvijen 1995. godine od strane Netscape communications korporacije pod nazivom Sloj bezbednih utičnica. SSL pravi bezbednu vezu između dve utičnice što podrazumeva dogovaranje parametara između klijenta i servera, međusobnu proveru identiteta klijenta i servera, tajno komuniciranje, zaštitu integriteta podataka. Kad se uspostavi bezbedna veza , SSL uglavnom kompresuje i šifruje podatke. Kada se protokol HTTP koristi preko sistema SSL to se zove bezbedni HTTP (engl. Secure HTTP, HTTPS), iako se i dalje koristi standardni HTTP protokol.

28. Transport Layer Security. Predstavlja poslednju verziju SSL. TSL je u stvari poboljšana verzija SSL version 3.0, i preporučena je kao Internet standard. Opisan je u dokumentu RFC2246.

29. Wireless Transport Layer Security protocal (WTLS). Predstavlja bežičnu varijantu SSL protokola. WTLS se koristi za šifrovanje, dešifrovanje, autentikaciju i zaštitu integriteta podataka.

30. Wireless Application Protocol. Protokol za bežične aplikacije. Predstavlja skup protokola za pristupanje WEB-u, optimizovan za veze malog propusnog opsega i bežične uređaje sa sporim procesorima, malom količinom memorije i malim ekranima.

Dodatni mehanizmi zaštite na mrežnom nivou se mogu ostvariti primenom mrežnih barijera (firewall). Firewall-ovi mogu biti računari, ruteri, radne stanice ili njihove kombinacije koje imaju osnovnu funkciju da definišu kojim se informacijama i servisima interne mreže može pristupiti iz spoljnjeg sveta i kome je, iz interne mreže, dozvoljeno da koristi informacije i usluge spoljnjih segmenata mreže. Ove barijere se uobičajeno instaliraju na tačkama gde se spajaju bezbedno osetljive interne mreže i nebezbedne spoljnje mreže. U zavisnosti od potreba, firewall se sastoji od jedne ili više funkcionalnih komponenti iz sledećeg skupa: ruter paketskog filtriranja, gejtvej na aplikacionom nivou (Application Level Gateway – proksi) i gejtvej na transportnom nivou (Circuit Level Gateway). Postoje četiri važna primera mrežnih barijera: Packet Filtering Firewall, Dual-Homed Firewall (sadrži dve mrežne kartice), Screened Host Firewall (sastoji se od rutera paketskog filtriranja i gejtveja na aplikativnom nivou) i Screened Subnet Firewall (sastoji se od dva rutera paketskog filtriranja i gejtveja na aplikativnom nivou). Poslednja navedena mrežna barijera predstavlja firewall koji nudi najviši nivo zaštite jer uvodi i demilitarizovanu zonu (DMZ) između interne i eksterne mreže.

PKI SISTEMI

Infrastruktura sistema sa javnim ključevima (PKI – Public Key Infrastructure) omogućuje ambijent za pouzdanu primenu elekronskog poslovanja i ona se najčešće bazira na kombinovanoj primeni asimetričnih i simetričnih šifarskih sistema [48]. PKI infrastruktura se sastoji od više komponenata, aplikacija i dokumenata koji definišu način realizacije četiri osnovne kriptografske funkcije u elektronskom poslovanju:

- Zaštita tajnosti – realizuje se simetričnim kriptografskim sistemima;
- Autentičnost – realizuje se asimetričnim šifarskim sistemima;
- Integritet podataka – realizuje se asimetričnim šifarskim sistemima;
- Neporecivost transakcija – realizuje se asimetričnim šifarskim sistemima.

Dok se funkcije zaštite tajnosti i integriteta podataka mogu realizovati i primenom tradicionalnih simetričnih tehnika, funkcije autentičnosti i neporecivosti transakcija zahtevaju primenu asimetričnih kriptografskih sistema – u okviru uspostavljenog PKI sistema. Najbolje karakteristike pokazuju sistemi u kojima su realizovane sve pomenute četiri funkcije. PKI sistemi obezbeđuju pouzdan metod za realizaciju funkcija provere autentičnosti i neporicanja transakcija koji je baziran na precizno utvrđenoj politici rada. PKI sistemi su brzo postali ključna karika svih sistema elektronske trgovine i korporacijske bezbednosti i sigurno će dominirati u bezbednosnim sistemima budućnosti [48]. Osnovni funkcionalni zahtevi koje treba da ispuni određeni PKI sistem navedeni su u nastavku.

FUNKCIONALNI ZAHTEVI KOJE TREBA DA ISPUNI ODREĐENI PKI SISTEM

PODRŠKA RAZLIČITIM POLITIKAMA RADA PKI SISTEMA

PKI sistem mora omogućiti podršku za primenu različitih bezbednosnih politika krajnjeg korisnika. Ova funkcionalnost omogućuje adaptaciju sistema na promene zakonskih, poslovnih i drugih politika rada koje utiču na realizaciju PKI sistema. S obzirom da PKI sistemi predstavljaju infrastrukturu u kojoj su, pored tehničkih aspekata, veoma bitni i značajni legalni i proceduralno-organizacioni aspekti, mogućnost adaptacije sistema na promene politike funkcionisanja predstavlja jedan od ključnih zahteva [48].

BEZBEDNOST SISTEMA

S obzirom da, Sertifikaciono telo (Certification Authority – CA) predstavlja centralni deo PKI sistema sa najvažnijim ciljem da uspostavi jedinstvenu tačku poverenja u čitavom sistemu, osnovni zahtev koji se postavlja je najviša bezbednost samog CA. Naime, ako je CA kompromitovano (tj. ako je tajni ključ asimetričnog šifarskog sistema CA kompromitovan) bilo internim ili eksternim napadom, i čitav PKI sistem je kompromitovan. Iz tih razloga, CA i čitav PKI sistem je potrebno zaštititi na najvišem nivou.

SKALABILNOST

Komercijalno dostupni PKI sistemi su skalabilno dizajnirani tako da se kreću od malih konfiguracija, koje rade na jednom PC računaru, na kome su realizovane aplikacije CA registracionih tela (Registration Authority – RA) i neophodne baze podataka, do velikih instalacija sistema. U velikim instalacijama sistema postoje višestruka RA sa više operatora, organizovana kao podređeni činioci u višestrukom hijerarhijskom sistemu CA, koji su pod jurisdikcijom jednog "Root CA" sistema.

Kao druga veoma značajna osobina, PKI sistem mora podržati eventualno proširivanje sistema dodavanjem određenih modula bez potrebe zaustavljanja rada sistema. Drugim rečima, ako se data organizacija proširuje, ili ako se zahtevi za PKI tehnologijom povećavaju, to se mora rešiti dodavanjem odgovarajućih specifičnih PKI modula [48].

FLEKSIBILNOST

Određeni PKI sistem treba da je dizajniran tako da bude fleksibilan u cilju lakog rešavanja različitih PKI zahteva. U ova obeležja su uključeni:

- Višestruki sistemi za registraciju i dostavu sertifikata i ključeva – potrebno je da, dati PKI sistem podržava različite mehanizme registracije i dostave PKI parametara, uključujući: e-mail servis, web komunikaciju, ličnu dostavu, VPN i drugo;
- Podrška različitim bezbednosnim modulima, malim hardverskim modulima (tokenima) i smart karticama;

- Podrška primeni različitih kriptografskih algoritama, kako javnih, tako i privatnih algoritama definisanih od strane dizajnera ili samih korisnika sistema;
- Višestruki sistemi publikacije izdatih i povučenih sertifikata koji uključuju različite eksterne direktorijumske servise (LDAP[19] i X.500[20]), kao i publikaciju na hard disku u cilju olakšavanja procesa publikacije;
- Podrška različitim metodama provere validnosti (povučenosti) digitalnih sertifikata, kao što su CRL (Certificate Revocation List), CRL distribucione tačke i OCSP (Online Certificate Status Protocol);
- Podrška kompleksnim PKI hijerarhijama – PKI sistem mora podržati hijerarhiju Sertifikacionih tela (bilo koje dubine), višestruka registraciona tela (RA), višestruke operatore RA, i mora podržati proceduru među-Sertifikacije (cross-Certification) sa drugim CA;
- Podrška višestrukim ključevima i sertifikatima po korisniku – politika rada PKI sistema, i samog Sertifikacionog tela (CA), treba da predvidi korišćenje višestrukih ključeva i sertifikata po korisniku, a da se korišćenje ovih ključeva tako konfiguriše da se odvojeni ključevi koriste za digitalno potpisivanje i za šifrovanje (u okviru digitalne envelope);
- Sistem treba da podrži fleksibilni autorizacioni proces – svaki zahtev za izdavanjem sertifikata može biti autorizovan od strane jedne ili više ovlašćenih osoba, što treba definisati u politici rada CA. Dodatno, sistem treba da omogući da se zahtevi za izdavanje sertifikata procesiraju i automatski, bez potrebe za primenom specifične procedure autorizacije.

JEDNOSTAVNO KORIŠĆENJE

U svakom PKI sistemu najvažniji subjekti su:

- Administrator bezbednosti PKI sistema koji uspostavlja i monitoriše rad čitavog PKI sistema;
- Administrator CA;
- Operatori RA koji sakupljaju registracione informacije i koji mogu da autorizuju proces Sertifikacije i povlačenja sertifikata;
- Krajnji korisnici koji podnose zahtev za izdavanjem sertifikata.

PKI sistem treba da bude dizajniran tako da, za sve gore pomenute kategorije korisnika, sistem bude veoma jednostavan za korišćenje i da korisnici jedini imaju pristup funkcijama koje su im omogućene za korišćenje. Ovo minimizuje proces obuke neophodne za svaki tip korisnika i redukuje moguće probleme koje oni mogu imati u cilju korišćenja sistema.

OTVORENOST SISTEMA

U cilju eventualnih zahteva za interoperabilnošću, PKI sistem mora zadovoljavati osobinu da se bazira na otvorenim standardima, od kojih je najvažniji X.509 standard za format digitalnog sertifikata.

KOMPONENTE PKI SISTEMA

Kao što je već rečeno, infrastruktura sistema sa javnim ključevima (PKI sistem) predstavlja kombinaciju hardverskih i softverskih proizvoda, politika i procedura. PKI sistemi omogućuju osnovno bezbednosno okruženje koje se zahteva u sistemima elektronskog poslovanja (e-business) u kome korisnici, koji se ne poznaju ili su distribuirani po svetu i nalaze se na velikim udaljenostima, mogu komunicirati bezbedno kroz mrežu poverenja. PKI sistemi se baziraju na digitalnim identitetima (digital IDs), poznatim pod nazivom digitalni sertifikati koji igraju ulogu svojevrsnih "digitalnih pasoša" ili "digitalnih ličnih karata" i koji povezuju ime vlasnika datog sertifikata sa njegovim javnim ključem asimetričnog kriptografskog sistema, kao što je na primer RSA algoritam [48].

PKI sistem se bazira na politici zaštite informacionog sistema u kome se primenjuje. Politika zaštite uspostavlja i definiše osnovne pravce i strategiju razvoja bezbednosti informacionog sistema date organizacije, i propisuje procedure i principe korišćenja

19. Lightweight Directory Access Protocol. Predstavlja klijent-server protokol za pristup uslugama Direktorijuma (engl. Directory services). Opisan je u dokumentu RFC 2251.

20. Usluge Direktorijuma specifikacije X.500 predstavljaju procese sloja aplikacije. Ove usluge se koriste za različite zadatke kao što su : obezbeđivanje jedinstvene službe za davanje imena svim elementima u mreži, previđenje mrežnih imena i adresa, obezbeđivanje opisa objekata (liste atributa i vrednosti) u direktorijumu, kao i obezbeđenje jedinstvenih imena za sve objekte u Direktorijumu. Sva alternativna imena kao npr. Alias-i na kraju se svode na osnovno jedinstveno ime objekta.

kriptografskih mehanizama u sistemu. Tipično, bezbednosna politika propisuje na koji se način upravlja ključevima i ostalim neophodnim informacijama u sistemu, i propisuje neophodne nivoe kontrole koji odgovaraju nivoima rizika. Internet Engineering Task Force (IETF) je objavio dokument "Certificate Policy and Certification Practices Framework" [48] koji daje okvir onog što bi trebalo biti definisano u politici sertificiranja. Ovaj dokument definiše politiku sertificiranja kao "imenovani skup pravila koji ukazuje na primenljivost sertifikata u određenoj zajednici i/ili klasi aplikacija sa zajedničkim sigurnosnim zahtevima". Skup procedura kojima se provodi politika sertificiranja, u PKI literaturi, naziva se Izjava o praksi sertificiranja (Certification Practice Statement). IETF Framework definiše ovaj dokument kao "izjavu o procedurama koje sertifikacijska ustanova sprovodi pri izdavanju sertifikata". Politika sertificiranja i Izjava o praksi sertificiranja, su obavezujući dokumenti za sertifikacijsku ustanovu. Na osnovu ovih dokumenata treći subjekti mogu oceniti koliko poverenja mogu imati u sertifikate izdate od strane sertifikacijske ustanove.

Konkretna Politika sertificiranja, direktno zavisi od namene infrastrukture javnih ključeva za koju se definiše ova politika. Jednostavno rečeno, Politika sertificiranja se može posmatrati kao dokumentovanje onoga što se želi uraditi [47]. Za internu upotrebu, u zatvorenom sistemu, moguće je napraviti kraći i manje detaljan dokument, ali koji opet mora imati sve bitne elemente.

PKI sistem se sastoji od sledećih osnovnih komponenata:

- Osnovni dokument rada PKI sistema - Politika sertifikacije (CP – Certificate Policy) – utvrđuje osnovne principe rada Sertifikacionog tela i ostalih komponenata PKI sistema;
- Praktična pravila rada (CPS – Certificate Practice Statement) – predstavlja dokument koji praktično opisuje rad Sertifikacionog tela i neophodan je u slučaju komercijalnog CA. CPS predstavlja jedan detaljan dokument koji sadrži operacione procedure za realizaciju principa koji su navedeni u politici Sertifikacije i predstavlja praktičnu podršku sistemu. Tipično, CPS uključuje definicije kako je CA formirano i način rada, kako se generišu digitalni sertifikati, kako se povlače, kako će ključevi biti generisani, registrovani i sertifikovani, gde će se čuvati i kako će biti raspoloživi korisnicima;
- Sertifikaciono telo (CA) – je najvažnija komponenta i osnova poverenja datog PKI sistema, čiji je zadatak da upravlja digitalnim sertifikatima u njihovom čitavom životnom ciklusu. Osnovni zadaci CA su da:
- Generiše digitalne sertifikate tako što povezuje identifikacione podatke određenog korisnika u sistemu sa njegovim javnim ključem asimetričnog kriptografskog sistema, 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 i, u tom smislu, publikuje liste povučenih sertifikata (CRL – Certificate Revocation List);

U postupku formiranja PKI sistema, organizacija može da realizuje sopstveno CA, ili da koristi usluge CA servisa, realizovanog od neke treće strane od poverenja;

Registraciono telo (RA) – obezbeđuje interfejs između korisnika i CA. RA prihvata zahteve i proverava autentičnost korisnika i prosleđuje standardni zahtev za izdavanje digitalnog sertifikata. Kvalitet procedure provere identiteta korisnika određuje nivo poverenja koji se ugrađuje u sertifikat;

- Sistemi za distribuciju sertifikata – Generisani digitalni sertifikati se mogu distribuirati na različite načine, u zavisnosti od strukture čitavog PKI sistema, kao na primer direktno korisnicima ili preko direktorijumskog servera. Direktorijumski server može već postojati u datom informacionom sistemu same organizacije, ili može biti isporučen kao deo čitavog PKI rešenja;
- PKI aplikacije – čitav PKI sistem se kreira da podrži rad većeg broja aplikacija u kojima se koriste digitalni sertifikati i tehnologija digitalnog potpisa, kao što su:
- Zaštita WEB transakcija;
- Zaštita e-mail servisa;
- VPN – virtuelne privatne mreže;
- Bezbedno upravljanje elektronskom dokumentacijom;
- Kontrola radnog vremena i pristupa određenim prostorijama.

U cilju zadovoljenja neophodnih zahteva koji se postavljaju pred sistem zaštite, praktične implementacije PKI sistema i samog CA u obliku softversko-hardverskih sistema, moraju biti modularno

realizovane. Svi moduli komuniciraju međusobno korišćenjem baze podataka, ili korišćenjem zaštićenih TCP/IP konekcija.

Shodno tome, osnovni moduli PKI sistema su:

- Sertifikaciono telo (CA) – digitalno potpisuje digitalne sertifikate i publikuje sertifikate i liste povučenih sertifikata (CA je kompleksno i takođe se sastoji od modula);
- Operator Sertifikacionog tela (CAO) – CAO je bezbednosni administrator čitavog PKI sistema;
- Registraciono telo (RA) – rutira informacije, sertifikate i zahteve za izdavanjem sertifikata kroz hijerarhiju datog PKI sistema;
- Operator RA (RAO) – ima zadatak da potvrdi ili odbije udaljene i lično podnete zahteve za izdavanjem sertifikata;
- Arhivni server – ovo je opcioni modul koji se koristi za eventualno čuvanje korisničkih parova ključeva za šifrovanje digitalnom envelopom.

SERTIFIKACIONO TELO (CA – CERTIFICATION AUTHORITY)

Sertifikaciono telo ili Sertifikacioni autoritet (CA) predstavlja jezgro čitavog PKI sistema. Čitavo poverenje sadržano u PKI infrastrukturi zavisi od digitalnog potpisa CA koji se formira na bazi asimetričnog kriptografskog algoritma (npr. RSA) i asimetričnog privatnog ključa CA. CA funkcioniše na bazi sopstvene fleksibilne politike rada i kontrolisano je od strane CAO i drugih administratora.

Sertifikaciono telo predstavlja softversko-hardversku aplikaciju koja, kao ulazni parametar, uzima javni ključ asimetričnog kriptografskog sistema, smešta ga u okvir digitalnog sertifikata i sve to, zajedno sa ostalim podacima, digitalno potpisuje u cilju garancije da dati javni ključ pripada definisanom korisniku (vlasniku datog digitalnog sertifikata).

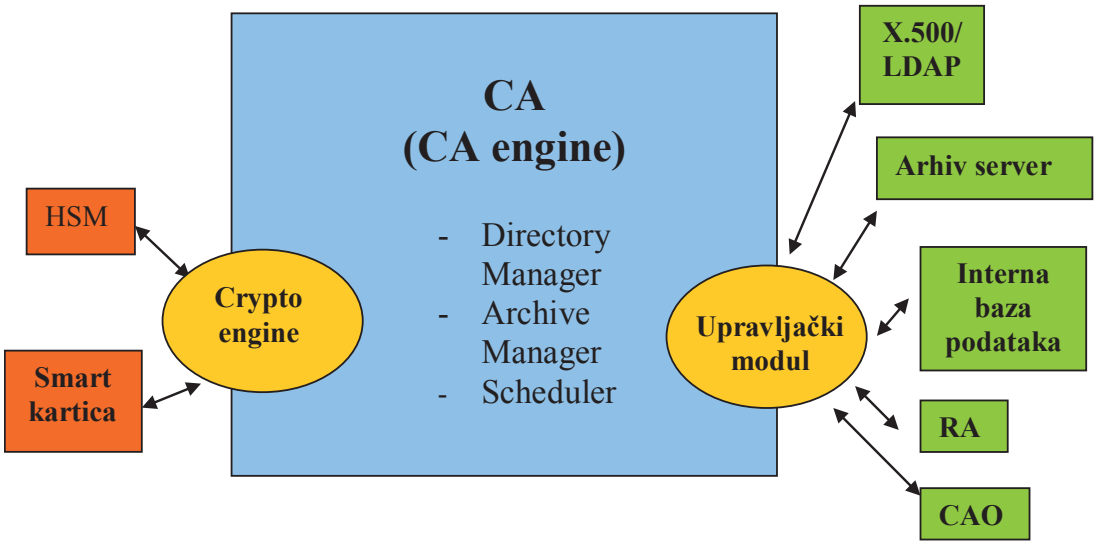
Za razliku od samopotpisanih sertifikata (kao što su digitalni sertifikati Root Sertifikacionih tela), digitalni sertifikati potpisani od strane CA koji se izdaju korisnicima, impliciraju da je CA kao "treća strana od poverenja" (Trusted Third Party) proverila da dati javni ključ pripada definisanom korisniku i da svojim potpisom sertifikuje da je to istinito. U najkraćem, ideja se sastoji u tome da određeno ovlašćeno eksterno telo (CA) preuzme lične podatke određenog korisnika i njegov javni ključ, formatira sve te podatke na standardni način u obliku digitalnog sertifikata, koga zatim digitalno potpiše. Digitalni sertifikat, na osnovu digitalnog potpisa CA, predstavlja pouzdanu vezu identiteta određenog korisnika i njegovog javnog ključa. Naime, ime vlasnika sertifikata, javni ključ i dodatne informacije kao što su: datum izdavanja i rok važnosti, ime CA koje je izdalo sertifikat, itd. formatiraju se u obliku digitalnog sertifikata u standardnom formatu (X.509 standard) tako da ga standardni programi za pretraživanje, (browser) i kriptografski softverski sistemi, mogu procesirati.

Koncept funkcionalnosti CA je grafički prikazan na slici 4.2.1.1.

Funkcionalnost CA

Funkcije koje CA treba da obavlja :

- CA prihvata potvrđene zahteve za generisanjem i povlačenjem sertifikata od registracionih tela (RA) i CAO, i isporučuje digitalne sertifikate i potvrdne poruke;
- Ako je tako predviđeno utvrđenom politikom rada, CA takođe dostavlja krajnjim korisnicima asimetrični par ključeva za šifrovanje (digitalna envelopa) koji se arhiviraju u bazi ključeva u arhivnom serveru;
- Digitalno potpisivanje sertifikata – CA je odgovorno za digitalno potpisivanje infrastrukturnih sertifikata i sertifikata krajnjih korisnika. CA takođe digitalno potpisuje sertifikate podređenih CA, kao i drugih CA u slučaju unakrsne Sertifikacije (cross-Certification);
- Publikovanje CRL (Certificate Revocation List) – CA digitalno potpisuje sve informacije objavljene u formi CRL;
- Digitalno potpisivanje poruka – sve poruke koje se šalju od strane CA i razmenjuju u PKI sistemu su digitalno potpisane;
- Verifikacija poruka – CA verifikuje sve poruke koje dobije u cilju provere autentičnosti i integriteta;
- Šifrovanje podataka – sve poruke koje se razmenjuju preko CA su šifrovane u PKCS#7 formatu;
- Arhiviranje podataka – svi relevantni podaci i log fajlovi se arhiviraju u bazi podataka CA. Sve arhivirane informacije su



Slika 4.2.1.1. Uprošćeni grafički prikaz funkcionalnosti CA

digitalno potpisane od strane CA. Svaki ulazak u bazu poseduje odgovarajući jedinstveni procesni broj;
- Publikacija sertifikata i drugih neophodnih parametara – CA opciono publikuje sertifikate i CRL na LDAP ili X.500 direktorijume. CA podržava i publikaciju pomenutih parametara u okviru fajl strukture na hard disku, kao jedan od mehanizama publikacije sertifikata koji se može lako kastomizovati;
- Opciono – CA može publikovati CRL i na OCSP (Online Certification Status) serveru;
- Generisanje asimetričnog para ključeva – CA generiše svoj sopstveni par ključeva za asimetrični kriptografski algoritam;
- Provera jedinstvenog imena Dname i javnih ključeva – CA može opciono da proverava, da li svi izdati digitalni sertifikati imaju jedinstveno Dname i javni ključ.

Obeležja CA

Karakteristike savremenog CA su:

- CA treba da podrži različite hardverske elemente, kao što su: smart kartice za krajnje korisnike, hardverski bezbednosni moduli (HSM – Hardware Security Module) i drugi tokeni;
- CA treba da podrži mogućnost korišćenja DAP i LDAP mehanizama;
- CA obezbeđuje višestruko generisanje parova asimetričnog ključa. Opciono, CA može imati individualni par ključeva za svaku od funkcija: digitalno potpisivanje sertifikata, digitalno potpisivanje CRL, šifrovanje podataka, šifrovanje ključa;
- CA podržava promenljivo vreme publikovanja CRL;
- CA treba da podrži OCSP servise;
- CA treba da podrži čitavu paletu simetričnih i asimetričnih ključeva. Što se tiče asimetričnih kriptografskih tehnika, CA bi trebalo da podržava sledeće algoritme za realizaciju digitalnog potpisa: RSA, DSA i ECDSA.

OPERATOR SERTIFIKACIONOG TELA (CAO)

Modul operatora Sertifikacionog tela (CAO) predstavlja modul za administraciju, nadzor i bezbednost CA i čitavog PKI sistema koji se bazira na datom CA. CAO kontroliše sve administratorske funkcije u sistemu i dodeljuje odgovarajuće privilegije ostalim administratorima, modulima i podsistemima.

Funkcionalnost CAO

- CAO prosleđuje potvrđene zahteve za izdavanjem sertifikata direktno CA. Zahtevi za izdavanjem sertifikata se smeštaju u CA bazu podataka;
- Kreiranje politike rada CA – CAO je odgovoran za kreiranje i održavanje politike izdavanja sertifikata. CAO takođe održava politike i procedure rada CA i svih RA;
- Ažuriranje novih verzija politike rada CA i celog PKI sistema – CAO dinamički dostavlja nove verzije politike i procedura rada do individualnih operatora registracionih tela (RAO), u cilju obezbeđenja da se svi digitalni sertifikati uvek izdaju u uslovima ažurnih verzija politike datog PKI sistema;
- Povlačenje sertifikata – svaki sertifikat može biti povučen od strane CAO. Zahtevi za povlačenjem sertifikata se smeštaju u CA bazu podataka;
- Razvoj PKI sistema – CAO može dodati nove module ili aplikacije u PKI sistem i dati im odgovarajuće privilegije;
- Generisanje ključeva – CAO je odgovoran za generisanje odgovarajućih ključeva (simetričnih i asimetričnih) za korisnike, ukoliko CA vrši tu funkciju;
- Digitalno potpisivanje poruka – sve poruke koje se šalju od strane CAO su digitalno potpisane;
- Verifikacija potpisanih poruka – sve poruke koje CAO prima prolaze proveru (verifikaciju) digitalnog potpisa u cilju provere autentičnosti potpisnika i integriteta sadržaja poruke;
- Šifrovanje podataka – sve poruke, koje se razmenjuju preko CAO modula, su šifrovane u PKCS#7 formatu;
- Arhiviranje podataka – svi podaci i log fajlovi se arhiviraju u bazi podataka CA. Sve informacije koje se arhiviraju se digitalno potpisuju od strane CAO. Svaki ulazni slog ima svoj jedinstveni procesni broj (tracking number).

Obeležja CAO

- CAO treba da podrži različite hardverske elemente, kao što su: smart kartice za krajnje korisnike, hardverski bezbednosni moduli (HSM – Hardware Security Module) i drugi tokeni;
- Poseduje grafički interfejs, jednostavan za korišćenje;
- Procesira sertifikate i CRL;
- Svaki CAO može imati različite nivoe privilegija;

REGISTRACIONO TELO (RA)

Registraciono telo (RA) igra ulogu rutera između operatora registracionog tela (RAO) i CA. RA može imati svoju sopstvenu politiku rada, koja se održava lokalno ili od strane CAO. RA može biti klijent-server aplikacija koja ima svoju lokalnu bazu i koja sa jedne strane komunicira sa operatorom RA – RAO, a sa druge strane sa CA. U nastavku je obrađen slučaj korišćenja RA u obliku klijent-server aplikacije.

Funkcionalnost RA

- RA prosleđuje potvrđene zahteve za izdavanjem ili povlačenjem sertifikata, dobijene od RAO, do CA. RA dobija sertifikate i potvrdne poruke od strane CA i dostavlja ih do RAO;
- RA prosleđuje zahteve za izdavanjem ili povlačenjem sertifikata, dobijene od korisnika putem određenog komunikacionog kanala, do RAO na proveru i potvrdu;
- Digitalno potpisivanje poruka – sve poruke poslate od strane RA su digitalno potpisane;
- Verifikacija poruka – sve digitalno potpisane poruke koje RA dobija se procesiraju u smislu verifikacije digitalnog potpisa u cilju provere autentičnosti potpisnika i integriteta sadržaja poruke;
- Šifrovanje podataka – sve poruke koje se razmenjuju preko RA su šifrovane u PKCS#7 formatu;
- Arhiviranje podataka – svi podaci i log fajlovi se arhiviraju u bazi podataka RA. Sve arhivirane informacije su digitalno potpisane od strane RA. Svaki ulazni slog ima jedinstveni procesni broj.

Obeležja RA

- RA treba da podrži različite hardverske elemente, kao što su: smart kartice za krajnje korisnike, hardverski bezbedno-

sni moduli (HSM – Hardware Security Module) i drugi tokeni.
- Opcija automatskog potvrđivanja – u slučaju da je to politikom rada predviđeno, RA može biti podešeno tako da automatski potvrđuje (digitalno potpisuje) sve udaljene zahteve koji stižu bez potrebe za intervencijom RAO.

OPERATOR REGISTRACIONOG TELA (RAO)

Operator registracionog tela (RAO) ima prvenstvenu funkciju da potvrđuje (digitalno potpisuje) zahteve za izdavanjem ili povlačenjem sertifikata koji će dalje biti procesirani od strane CA. Međutim, u slučaju da politika rada CA to predviđa i dozvoljava, RAO može realizovati i funkciju generisanja ključeva za krajnjeg korisnika. Tradicionalno, RAO se realizuje kao klijent-server aplikacija u kombinaciji sa RA, a osnovna funkcionalnost i obeležja biće prikazana u nastavku.

Funkcionalnost RAO

- RAO prima zahteve za izdavanjem sertifikata preko RA, ili ih kreira direktno u ličnom kontaktu sa krajnjim korisnikom (face-to-face manner);
- RAO je odgovoran za potvrđivanje ili odbijanje zahteva za izdavanjem sertifikata od krajnjeg korisnika koji su dobijeni u ličnom kontaktu ili elektronskom komunikacijom (ova funkcija zavisi od utvrđene politike rada PKI sistema);
- RAO šalje potvrđene zahteve za izdavanjem ili povlačenjem sertifikata do RA;
- RAO može generisati ključeve (asimetrični par ključeva) za krajnjeg korisnika u softveru ili na kriptografskom hardveru (HSM), ukoliko je to politikom rada predviđeno;
- Digitalno potpisivanje poruka – sve poruke poslate od strane RAO su digitalno potpisane;
- Verifikacija poruka – sve digitalno potpisane poruke koje RAO dobija se procesiraju u smislu verifikacije digitalnog potpisa, a u cilju provere autentičnosti potpisnika i integriteta sadržaja poruke;
- Šifrovanje podataka – sve poruke koje se razmenjuju preko RAO modula su šifrovane u PKCS#7 formatu;
- Arhiviranje podataka – svi podaci i log fajlovi se arhiviraju u bazi podataka RA. Sve arhivirane informacije su digitalno potpisane od strane RAO. Svaki ulazni slog ima jedinstveni procesni broj.

Obeležja RAO

- RAO treba da podrži različite hardverske elemente, kao što su: smart kartice, hardverski bezbednosni moduli (HSM – Hardware Security Module) i drugi tokeni.
- Poseduje grafički interfejs jednostavan za korišćenje.

DIGITALNI SERTIFIKATI, STRUKTURA I STANDARDI

Digitalni sertifikati predstavljaju element kojim se utvrđuje veza između identiteta subjekta i njegovog javnog ključa za primenu asimetričnog kriptografskog algoritma. Raspolaganje javnim ključem potpisnika je uslov za pouzdanu verifikaciju digitalnog potpisa. Naime, strana koja vrši verifikaciju mora biti sigurna da dati javni ključ predstavlja kriptografski par sa tajnim ključem kojim je poruka digitalno potpisana. Javni i tajni ključ, asimetričnog kriptografskog algoritma, su dve velike brojne veličine i nemaju determinističku vezu sa identitetom bilo kog pravnog ili fizičkog lica. Digitalni sertifikati predstavljaju mehanizam za pouzdano pridruživanje datog para brojeva identitetu nekog subjekta, tako da se ta veza ne može falsifikovati. Na taj način, digitalni sertifikati predstavljaju elektronske ekvivalente nekoj vrsti "digitalne lične karte" ili "digitalnog pasoša". Da bi se dobio digitalni sertifikat, mora se prvo formirati zahtev za dobijanje sertifikata (Certificate Request), koji se dostavlja određenom CA u cilju izdavanja digitalnog sertifikata. Ovaj zahtev sadrži sve podatke o korisniku koji će se pojaviti i u digitalnom sertifikatu. Zahtev za sertifikat je digitalno potpisan (samopoptisan) u cilju garancije njegovog integriteta. Sertifikaciono telo proverava autentičnost dobijenog zahteva korišćenjem javnog ključa, koji je u njemu sadržan. Postoje dva korišćena tipa zahteva za izdavanje digitalnog sertifikata, poznati kao PKCS#10 i RFC 2511. PKCS#10 format je daleko jednostavniji. PKCS#10 tip zahteva za izdavanjem sertifikata sastoji se od sledeća 4 polja:

- Broj verzije formata zahteva (od 1 do 3);
- Naziv vlasnika digitalnog sertifikata (Distin-

Verzija formata sertifikata
Serijski broj sertifikata
Identifikator algoritma kojim se vrši digitalni potpis
Naziv Sertifikacionog tela koje je izdalo sertifikat
Rok važnosti sertifikata
Naziv vlasnika sertifikata
Javni ključ vlasnika sertifikata
Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata
DIGITALNI POTPIS SERTIFIKATA TAJNIM KLjUČEM SERTIFIKACIONOG TELA

Slika 4.3.1. Sadržaj digitalnog sertifikata

guishedName - Dname);
- Javni ključ vlasnika digitalnog sertifikata;
- Atributi.

Polje atributa sadrži one elemente za koje postoji potreba da se nađu u digitalnom sertifikatu, kao što je broj telefona, broj faksa, e-mail adresa, najviša vrednost finansijske transakcije u slučaju bankarskih sertifikata i druge karakteristike. U ovom polju se može naći sve ono što ne potpada pod polje Dname a predstavlja jedinstveni string koji identifikuje vlasnika sertifikata. Pored toga, Dname predstavlja put kroz X.500 direktorijum, tako da se jedino može sastojati iz sledećih polja:

- Dvoslovni niz koji označava državu;
- Region;
- Elektronska adresa;
- Firma;
- Odeljenje u firmi;
- Ime vlasnika sertifikata.

Imajući na raspolaganju digitalni sertifikat određenog subjekta, moguće je izvršiti verifikaciju digitalnog potpisa poruka koje je taj subjekt potpisao. Ukoliko je verifikacija uspešna, verifikator je siguran u integritet poruke, u autentičnost njenog potpisnika i u nemogućnost naknadnog poricanja datog potpisnika za izdavanje date poruke. U okviru sistema zaštite savremenih računarskih mreža, digitalni sertifikati se, između ostalog, mogu primenjivati za verifikaciju digitalnog potpisa, kontrolu pristupa subjekata kriptozaštićenim aplikacijama i u procedurama autentikacije. Sadržaj digitalnog sertifikata, u skladu sa standardom X.509, je prikazan je na slici 4.3.1.

X.509 sertifikati postoje u tri verzije, v1, v2 i v3. Sve verzije su standardizovane i kompatibilne unazad, odnosno novije verzije sa većim brojem, imaju sva polja kao i ranije verzije, te još neka dodatna. ITU-T X.509 ili ISO/IEC 9594-8 definiše standardni format sertifikata i kao deo X.500 preporuka za Direktorijume objavljen je 1988. Ovo se naziva verzijom 1. U verziji 2 su 1993. godine dodata još dva polja. Kroz praktična iskustva u upotrebi sertifikata pojavila se potreba za dodatnim poljima. Na osnovu ove potrebe ISO/IEC, ITU-T and ANSI X9 su 1996. godine definisali novi format verzija 3. Ovaj format omogućava dodavanje novih polja, ali ne zahteva njihovo postojanje. Pomenute organizacije su utvrdile skup standardnih ekstenzija za dodatna polja, ali nisu striktno definisale način njihove upotrebe odnosno tumačenja značenja [30]. Da bi se olakšala upotreba sertifikata za Internet aplikacije IETF radna grupa za mreže, podgrupa za PKIX, je 2002. godine objavila RFC3280, koji specificira format X.509 sertifikata i listu opozvanih sertifikata za Internet X.509 PKI. Ovaj dokument potvrđuje namenu osnovnih polja sertifikata verzije 2, te utvrđuje namenu ekstenzija za dodatna polja iz verzije 3. Striktno poštovanje predloga iz ovog dokumenta bi trebalo omogućiti interoperabilnost različitih aplikacija koje izdaju i proveravaju digitalne sertifikate [50]. Treba imati u vidu da je ovo oblast koja je još u razvoju pa se tumačenja nekih dokumenata razlikuju od proizvođača do proizvođača. Posebnu kategoriju sertifikata predstavljaju kvalifikovani elektronski sertifikati. Ovo je termin koji se koristi u Direktivi Evropskog parlamenta i saveta o pravnim okvirima za elektronski potpis [55]. Ovaj dokument je uputstvo članicama Evropske unije za kreiranje pravnih okvira koji podržavaju elektronski potpis. Definicija kvalifikovanog elektronskog sertifikata u Srbiji definisana je u pravnom dokumentu koji reguliše ovu problematiku, a prikazana je u prilogu 1. ovog rada.

Važnost kvalifikovanog sertifikata je u tome, što je i jedan od uslova za pravnu jednakost digitalnog potpisa sa svojeručnim, da je digitalni potpis napravljen koristeći kvalifikovani sertifikat.

Nezavisno od aplikacije koja će biti korišćena kao CA potrebno je utvrditi princip koga će se držati prilikom kreiranja sertifikata. Drugim rečima, potrebno je dati lokalno značenje svakom od polja u sertifikatu. Neke od odluka su pitanje usvojene politike imenovanja subjekata, dok su neke vrlo tehničke prirode. Princip dodeljivanja vrednosti poljima koja nemaju tehničko značenje biće samo naveden. X.509 v3 sertifikat je u suštini digitalno potpisan skup podataka, tako da sam sertifikat ima polja sa podacima, polje sa vrednošću digitalnog potpisa CA nad poljima sa podacima, zatim polje koje informiše o tome koji je od algoritama korišćen za digitalno potpisivanje. Mogući algoritmi za digitalno potpisivanje i druge kriptografske operacije sa X.509 sertifikatima su definisani u RFC3279[57]. Izbor algoritma i njegovih parametara će biti kasnije detaljnije razmatran u ovom poglavlju. Polja sa podacima se sastoje od osnovnih polja i ekstenzija.

STANDARDI KOJI SE ODNOSE NA FUNKCIONISANJE PKI SISTEMA

Standardi koji se odnose na funkcionisanje PKI sistema neophodni su za definisanje:

- Procedure registracije subjekata;
- Formata sertifikata;
- Formata lista opozvanih sertifikata;

- Formata poruka pri registraciji (zahtevi i odobrenja izdavanja sertifikata);
- Formata digitalnih sertifikata;
- Autentikacionih protokola.

Najvažnije telo zaduženo za interoperabilnost PKI standarda je PKI radna grupa IETF (Internet Engineering Task Force) organizacije, poznata i kao PKIX grupa (nastalo od "PKI for X.509 Certificates"). PKIX specifikacija se bazira na dve grupe standarda:

- ITU-T X.509 standardi
- PKCS standardi definisani od strane RSA Data Security

Prihvaćeni i najviše korišćen standard koji podržava PKI sisteme je ITU-T X.509 [30] čija je osnovna svrha u definisanju standardnog formata digitalnih sertifikata. Verzija 3 ovog standarda koja je trenutno važeća, usvojena je 1996. godine. Međutim, ovaj standard nije namenjen za definisanje kompletnih funkcija PKI sistema.

Standardom X.509 definisana je struktura, postupak dobijanja i način predstavljanja sertifikata. Struktura sertifikata opisuje se korišćenjem ASN.1 metoda za opisivanje apstraktnih tipova. U nastavku će biti navedene njegove osnovne karakteristike i struktura sertifikata koja je u skladu sa ovom notacijom. Softverski sistem za proizvodnju digitalnih sertifikata koristi ASN.1 notaciju za opis strukture sertifikata.

Abstract sintax notation one - ASN.1

Open System Interconnections (OSI) je standard kojim su definisana pravila za međusobno povezivanje računarskih sistema i to od osnovnog, fizičkog nivoa, do aplikativnog nivoa. Da bi standard bio nezavistan od implementacionih karakteristika pojedinačnih sistema, objekti se opisuju na apstraktan način, kroz podatke koje sadrže, servise koje pružaju i komunikacione interfejse prema spoljašnjoj sredini. Sistem koji se primenjuje u OSI definisan je standardom X.208 i poznat je pod imenom Abstract Syntax Notation One (ASN.1).

Abstract Syntax Notation One je metod za opisivanje apstraktnih tipova podataka i način za kodiranje vrednosti nekog tipa definisanog ovom metodom. Prema ovom standardu, tip je definisan skupom svojih vrednosti i postoje četiri osnovna oblika tipova:

1. Prosti tipovi, predstavljaju skupove osnovnih vrednosti;
2. Strukturni tipovi koji se sastoje od komponenti;
3. Vezani tipovi, oni se izvode iz drugih tipova;
4. Ostali tipovi.

Tipovi i njihove vrednosti mogu se imenovati i ta se imena mogu koristiti u definisanju drugih tipova i vrednosti. Operator dodeljivanja se označava sa . Svaki ASN.1 tip (osim CHOICE i ANY) određen je pripadnošću klasi i jednim nenegativnim brojem. Postoje četiri klase:

1. Univerzalna, za tipove čije je značenje isto nezavisno od aplikacije;
2. Aplikativna, za tipove kod kojih je značenje definisano unutar aplikacije;
3. Privatne za tipove čije značenje je vezano za lokalno okruženje;
4. Konteksno-zavisna za tipove čije je značenje specifično u okviru strukturnih tipova.

Dva tipa se smatraju jednakim, ako i samo, ako pripadaju istoj klasi i imaju isti broj. Ovim mehanizmom se može opisati svaki apstraktni tip podataka.

Sledeće pitanje adresirano ovim standardom je način predstavljanja vrednosti apstraktno definisanog tipa. To pitanje se razrešava formulisanjem osnovnih pravila za kodiranje, Basic Encoding Rules (BER), kojima se svaka ASN.1 vrednost predstavlja kao niz bajtova. Ovaj, osnovni način kodiranja, nije jednoznačan tj. ista vrednost se može kodirati na više različitih načina. Načini kodiranja su sledeći :

1. Primitivni - sa unapred poznatom dužinom podatka;
2. Konstruktivni - sa unapred poznatom dužinom podatka;
3. Konstruktivni - sa nepoznatom dužinom podatka.

Kod vrednosti nekog tipa sastoji se od najmanje prva tri bloka, od sledeća četiri:

1. Identifikacioni deo - kojim se jednoznačno određuje tip podatka (klasa i broj), metod kodiranja (primitivni ili kostruktivni);
2. Specifikacija dužine podatka - kojom se specificira broj bajtova za registrovanje podatka ili, ako dužina nije unapred poznata, sadrži kod kojim se ta situacija identifikuje;
3. Sadržaj - niz bajtova kojim se reprezentuje vrednost;
4. Oznaka za kraj podatka - ukoliko nije unapred poznate dužine.

Napomenuli smo ranije da BER kodiranje nije jednoznačno, što može izazivati probleme u situacijama kada je jednoznačnost zahtevana osobina. Zbog toga je formulisan niz ograničenja na pravila BER kodiranja, tako da se postigne jednoznačnost u kodiranju vrednosti nekog ASN.1 tipa. Taj restriktivni skup pravila se označava sa DER (Distinguished Encoding Rules). Grubo govoreći, jednoznačnost se postiže zahtevajući da kod vrednosti bude minimalan u pogledu dužine (broja bajtova).

Dakle, ovim sistemom smo u mogućnosti da opišemo i predstavimo vrednost proizvoljnog apstraktnog tipa.

ITU X.509 V3 sertifikat-struktura

Prema ovom standardu digitalni sertifikat se sastoji od tri dela. Prvi deo čine podaci značajni za sam sertifikat predstavljeni promenljivom tbsCertificate, drugi deo predstavlja identifikator algoritma za potpisivanje predstavljen promenljivom signatureAlgorithm, i na kraju sam potpis predstavljen promenljivom signature.

Promenljiva tbsCertificate je strukturnog tipa i sadrži sledeća polja:

- Verzija (Version) – predstavlja oznaku strukture digitalnog sertifikata koja je specificirana u standardu X.509. Moguće vrednosti su v1, v2, v3. Predložena vrednost je v3;
- Serijski broj (Serial Number) – redni broj izdatog sertifikata. Način dodeljivanja serijskih brojeva mora biti jedinstven tj. ime izdavača sertifikata (Sertifikaciono telo) i redni broj sertifikata jedinstveno određuju sertifikat. Serijski broj sertifikata je vrednost koju dodeljuje sertifikacioni autoritet u trenutku kreiranja digitalnog sertifikata. Predstavlja pozitivan celi broj jedinstven unutar CA. Aplikacija koja implementira CA brine se o zadovoljavanju potrebnih uslova;
- Identifikator algoritma - koji je korišćen pri potpisivanju sertifikata od strane CA. Vrednost ovog polja mora biti identična vrednosti ranije pomenutog polja koje ide uz vrednost digitalnog potpisa. CA aplikacije automatski generišu identičnu vrednost u ova dva polja. Identifikator algoritma digitalnog potpisa (Signature Algorithm) je u stvari oznaka asimetričnog kriptografskog algoritma RSA, DSA (Digital Signature Algorithm) i ECDSA (Elliptic Curve Digital Signature Algorithm), i korišćene hash funkcije (MD5, SHA1), koji su primenjeni u procesu generisanja digitalnog potpisa Sertifikacionog tela. SHA-1 je preferirani algoritam za Interenet X.509 PKI. Pošto je SHA-1 sugerisan kao najbolji izbor, razumno je koristiti ga i radi buduće interoperabilnosti sa drugim PKI. U ovom slučaju konzervativno opredeljenje za najstariji i još uvek najraširenij od algoritama, RSA, pruža najveću verovatnoću podržanosti od aplikacije koja će biti izabrana za implementaciju Sertifikacijske ustanove. RSA je takođe dobar izbor i za kompatibilnost sa drugim CA, jer sve vrhovne CA koje su ugrađene u savremene Web browsere koriste RSA algoritam. RSA podržava planirane namene sertifikata: digitalno potpisivanje i neporicanje. Ovaj algoritam za digitalne potpise mora biti kombinovan sa nekim od algoritama za jednosmerno hashiranje. Pošto je za tu namenu izabran SHA-1, onda će izabrani algoritam za digitalno potpisivanje biti RSA sa SHA-1;
- Naziv izdavača digitalnog sertifikata (Issuer) – Ovo polje ima posebne zahteve za kvalifikovane sertifikate u odnosu na standardne definisane u RFC3280. Ti zahtevi su da se identifikuje organizacija odgovorna za izdavanje sertifikata. Ime organizacije koje se ovde upiše mora biti zvanično registrovano ime organizacije. U sklopu ovog imena se minimalno mora nalaziti i ime države izdavanja. Dozvoljeni su i drugi elementi koji bliže definišu organizaciju, ali oni moraju biti definisani u Politici sertificiranja ili Izjavi o praksi sertificiranja. Struktura koja identifikuje Sertifikaciono telo (CA) koje je generisalo dati sertifikat sastoji se iz sledećih elemenata:
  - Ime izdavača sertifikata (commonName);
  - Odeljenje u organizaciji (organizationalUnitName);
  - Organizacija (organization);
  - Mesto (localityName);
  - Elekronska adresa (emailAddress);
  - Region ili republika u okviru držve (stateOrProvinceName);
  - Oznaka države (countryName).
- Validnost – U ovom polju se definiše period validnosti - važnosti sertifikata. Ovaj period je definisan sa dva datuma:

datum početka važenja sertifikata i datum prestanka važenja sertifikata. Predložena vrednost datuma početka važenja sertifikata je datum izdavanja sertifikata, a datum prestanka važenja sertifikata će biti izračunat na osnovu definisanog vremena valjanosti sertifikata. Utvrđivanje trajanja valjanosti sertifikata će biti kasnije razmatrano. Važno je da se ovo trajanje može globalno definisati na nivou CA aplikacije i tipa sertifikata, a aplikacija će se pobrinuti za unošenje gore predloženih vrednosti u sertifikate koje izdaje. Specificira se period unutar kojeg se sertifikat smatra važećim ukoliko nije opozvan. Rok važnosti sertifikata predstavlja vremenske okvire validnosti digitalnog sertifikata. U procesu verifikacije prihvata se samo sertifikat kome nije istekao rok važnosti. Navedeno polje se sastoji od dva elementa:

- Početak važnosti sertifikata (Valid From);
- Kraj važnosti sertifikata (Valid To).

- Vlasnik sertifikata (Subject) –Identifikator (ime) Ovo polje identifikuje entitet asociran sa javnim ključem koji se nalazi u polju "javni ključ vlasnika sertifikata". Za kvalifikovani sertifikat, ovo polje mora imati vrednost prepoznatljivog (distinguished) imena subjekta. U sklopu imena se mora nalaziti odgovarajući podskup atributa koji jedinstveno određuju subjekat. Prvi od atributa mora biti ime i/ili prezime ili pseudonim subjekta. Pošto se jedinstvenost subjekta garantuje unutar domena u kom je izdat sertifikat, uobičajeno je uključiti podatke o organizaciji na način na koji su one predstavljene u polju sa podacima o izdavaču sertifikata. Moguće je uključiti i titulu, što može biti korisno u nekoj Akademskoj instituciji. Ako je potrebno upisuje se i serijski broj koji omogućava razlikovanje dva subjekta, ako su sva ostala polja subjekta iste vrednosti. Ovo polje kao što je već rečeno identifikuje vlasnika digitalnog sertifikata i sastoji se od sledećih komponenti:
  - Ime vlasnika sertifikata;
  - (titula);
  - Odeljenje u organizaciji;
  - Organizacija;
  - Mesto;
  - Elekronska (e-mail) adresa;
  - Region ili republika u okviru države;
  - Oznaka države.
- Javni ključ (Public Key) – javni ključ vlasnika sertifikata i identifikator algoritma za koji je namenjen. Informacija o javnom ključu vlasnika sadrži numeričku reprezentaciju javnog ključa i identifikator asimetričnog algoritma (RSA, DSA) sa kojim se dati ključ primenjuje. Broj algoritama predloženih za javne ključeve je najveći. Predloženi algoritmi su: RSA, DSA, Diffie-Hellman razmena ključeva, KEA (key exchange algorithm) i eliptičke krive sa DSA i sa Diffie-Hellman. Pošto je RSA izabran za digitalno potpisivanje, sasvim je logično i da se za javne ključeve izabere RSA;
- Polje dodatnih informacija (Extension) – sadrži skup polja (ekstenzije) koja, po potrebi, mogu nositi još neke informacije osim ovih osnovnih. Neke od ovih dodatnih informacija mogu posedovati atribut CRITICAL ili NONCRITICAL. Ukoliko aplikacija koja koristi sertifikat pronađe informaciju označenu sa CRITICAL i ne prepozna je, mora sertifikat odbaciti kao neispravan. Polje dodatnih informacija može sadržati informacije pomoću kojih se identifikuje javni ključ kojim se sertifikat proverava, ukoliko izdavač ima više parova javnih i tajnih ključeva. Takođe dato polje može da sadrži informacije o nameni javnog ključa koji vlasnik sertifikata poseduje, opis uslova pod kojima je sertifikat kreiran i za šta se može koristiti, alternativna imena izdavača i vlasnika sertifikata;
- Digitalni potpis (Digital Signature) sertifikata od strane CA.
- Prema dosadašnjim iskustvima ovakva struktura sertifikata ispunjava zahteve savremenih kriptografkih sistema zaštite. Shodno tome, većina (ako ne i svi) savremenih sistema zaštite, koji uključuju infrastrukturu sistema sa javnim ključevima (PKI sisteme), bazira se na primeni X.509 digitalnih sertifikata. Dati sertifikati se još nazivaju PKI digitalni sertifikati.

ITU X.509 v2 lista opozvanih sertifikata

Prema ovom standardu lista opozvanih sertifikata se sastoji od tri dela. Prvi deo čini lista opozvanih sertifikata, predstavljena promenljivom tbsCertList, drugi deo predstavlja identifikator algoritma za potpisivanje liste opozvanih sertifikata predstavljen promenljivom signatureAlgorithm i na kraju sam potpis predstavljen promenljivom signature.

Promenljiva tbsCertList je strukturnog tipa i sadrži sledeća polja:

- Verzija – označava verziju standarda koja je primenjena pri generisanju liste opozvanih sertifikata;
- Potpis – sadrži identifikator algoritma kojim izdavač liste opozvanih sertifikata vrši potpis liste opozvanih sertifikata;
- Ime izdavača liste – identifikuje izdavača liste;
- Datum izdavanja tekuće liste opozvanih sertifikata;
- Datum sledećeg ažuriranja liste opozvanih sertifikata;
- Spisak opozvanih sertifikata;
- Polje dodatnih informacija;

Spisak opozvanih sertifikata se sastoji od niza rednih brojeva sertifikata koji, zajedno sa identifikatorom izdavača sertifikata na jedinstven način, određuju opozvani sertifikat.

X.509 v2 lista opozvanih sertifikata - formiranje

Izdavač sertifikata registruje i formira zahteve za opoziv sertifikata shodno svojoj politici, formira novu listu opozvanih sertifikata. Zatim se kao i kod generisanja sertifikata od BER koda, korišćenjem dogovorenih algoritama, formira otisak i potpis liste opozvanih sertifikata.

U cilju dodatne standardizacione podrške X.509 standardu, proizvođači, korisnici i komiteti za standarde su se uglavnom okrenuli korišćenju de facto PKI standarda, definisanih u PKCS (Public Key Cryptographic Standards).

PKCS predstavlja seriju standarda koji pokrivaju funkcije PKI sistema u oblastima registracije obnavljanja izdatih digitalnih sertifikata i distribucije lista opozvanih sertifikata. Za interoperabilnost PKI sistema, najvažnija su sledeća četiri PKCS standarda:

- PKCS#1 standard za opis realizacije procedura digitalnog potpisivanja i digitalne envelope na bazi RSA asimetričnog kriptografskog algoritma;
- PKCS#7 standard za sintaksu kriptografskih poruka (Cryptographic Message Syntax Standard);
- PKCS#10 standard za sintaksu zahteva za izdavanje digitalnog sertifikata (Certificate Request Syntax Standard);
- PKCS#12 standard za sintaksu razmene ličnih informacija (Personal Information Exchange Syntax Standard).

EKSTENZIJE U SERTIFIKATU

Ekstenzije u sertifikatu su uvedene kada je definisan X.509v3 standard za format sertifikata. U prethodnim verzijama (v1, v2) ukoliko bilo koja informacija, koja nije iz domena Dname, treba da se unese u sertifikat, ona je upisivana kao deo Dname strukture. Upotreba ekstenzija čini savremene sertifikate izuzetno fleksibilnim, time što se povećava mogućnost uvođenja i podrške novih PKI aplikacija. Dakle, ekstenzije se mogu koristiti u cilju pridruživanja novih atributa korisniku u odnosu na one informacije koje se mogu uneti u Dname strukturu. Ekstenzije mogu biti, takođe, korišćene za kreiranje hijerarhije digitalnih sertifikata. Takođe, postoji nekoliko predefinisanih i međunarodno prepoznatih ekstenzija. Pored toga, mogu se takođe realizovati nove ekstenzije za privatne potrebe korišćenjem generičkih ekstenzija. Polja za ekstenzije u sertifikatu mogu biti korišćena da se obezbede identifikacione informacije, autorizacioni podaci i polja kontrole pristupa. Ukratko, ekstenzije sertifikata mogu biti korišćene da sadrže informacije za koje korisnik smatra da mogu biti korisne u procesu analize digitalnih sertifikata.

Sve ekstenzije u sertifikatu mogu biti označene kao kritične (critical) ili nekritične (noncritical). Ako je ekstenzija označena kao nekritična, to znači da će, ako neka PKI aplikacija ne prepozna datu ekstenziju, ona biti ignorisana i da će se dati sertifikat dalje normalno procesirati. Ekstenziju treba označiti kao kritičnu, ukoliko se želi osigurati ograničenje na korišćenje datog sertifikata. Neke ekstenzije moraju biti obavezno proglašene kritičnim u skladu sa standardom X509v3. Međutim, za većinu ekstenzija se preporučuje da budu nekritične.

Potrebno je, takođe, pažljivo procenjivati potrebu za dodavanjem svake ekstenzije, jer one doprinose uvećanju samog sertifikata. Takođe, što više ekstenzija se doda, to je veća verovatnoća da će u budućnosti neke informacije iz ekstenzija biti nevalidne

i da će se zbog toga morati povući sertifikat. U tom smislu, preporuka je da se u sertifikat dodaju samo suštinski važne ekstenzije i da se ne povećava nepotrebno veličina sertifikata dodavanjem nepotrebnih informacija.

Ekstenzije su karakteristične za verziju 3 digitalnih serifikata. U polju ekstenzija se nalaze dodatne informacije vezane za vlasnika i izdavača sertifikata. Standardne ekstenzije u sertifikatu su [55]:

- 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).

Navedene ekstenzije u sertifikatu su predložene od strane PKIX radne grupe (Internet X.509 Public Key Infrastructure Certificate and CRL profile, RFC2459).

Najčešće korišćene ekstenzije

Najčešće ekstenzije prisutne u verziji 3 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 serifikatu. 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 (Key Encipherment) koje se primenjuje u procesu kreiranja sesijskog ključa ili digitalne envelope;
  - Šifrovanje poruka (Data Encipherment);
  - Kreiranje digitalnog potpisa sertifikata (Certificate Signing).
- Dodatna specifikacija primene ključa (Enhanced 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 (CodeSigning);
  - Digitalno potpisivanje poruka koje se prenose posredstvom elektronske pošte (Secure Email);
  - Autentikacija servera prilikom kreiranja kriptografskog tunela sa klijentskim računarom (Server Authentication);
  - Autentikacija klijenta prilikom kreiranja kriptografskog tunela sa serverskim računarom (Client Authentication).
- Politika primene digitalnog sertifikata (Certificate Policy). Data ekstenzija pobliže definiše politiku i način primene datog digitalnog serifikata. 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).
- Izjava o kvalifikovanom sertifikatu – Ovo polje je neophodno da bi sertifikat bio kvalifikovan [55]. Sadržaj ovog polja je zapravo izjava izdavača da je sertifikat izdat kao kvalifikovani sertifikat u skladu sa važećim zakonom u odgovarajućem pravnom siste-

mu. Ovakva izjava i više detalja se obično daju u Politici sertificiranja i Izjavi o praksi sertificiranja na koje se u sklopu sertifikata upućuje posebnom ekstenzijom.

METODE REGISTRACIJE KORISNIKA

CA može bilo da dobije javni ključ od samog korisnika i da ga sertifikuje, ili da generiše za svakog korisnika par javnog i tajnog ključa asimetričnog kriptografskog sistema i da distribuira zajedno tajni ključ i PKI digitalni sertifikat. Iz razloga sigurnosti, smatra se boljom praksom ako korisnik sam generiše par asimetričnih javnih ključeva (javni i tajni ključ), a zatim da zahtev za izdavanjem sertifikata koji sadrži njegov javni ključ dostavi CA na sertifikaciju. Ovaj metod obezbeđuje da se tajni ključ uvek čuva na jednoj lokaciji – kod korisnika. Međutim, pomenuti razlozi sigurnosti se mogu opravdati samo sa stanovišta korisnika. Sa stanovišta PKI sistema (CA), sigurnije je da samo CA bude nadležno za generisanje parova asimetričnih ključeva, jer se jedino na taj način može kontrolisati i održati jedinstven kvalitet izgenerisanih ključeva i jedinstvenost procedure bezbednog čuvanja izgenerisanih ključeva. U tom slučaju, tajni ključevi se distribuiraju na bezbednim medijumima, kao što su smart kartice ili USB smart tokeni.

Da bi se dobio digitalni sertifikat, mora se prvo formirati zahtev za dobijanje sertifikata – Certificate request, i da se dostavi određenom CA u cilju izdavanja digitalnog sertifikata. Ovaj zahtev sadrži sve lične informacije koje će se pojaviti i u digitalnom sertifikatu.

Postoje generalno dva moguća načina generisanja para javnog i tajnog ključa i kreiranja digitalnog sertifikata na bazi javnog ključa:

- CA generiše par javnog i tajnog ključa, formira digitalni sertifikat i dostavlja tajni ključ i sertifikat vlasniku;
- Generisanje para javnog i tajnog ključa lokalno od strane samog vlasnika sertifikata korišćenjem hardverskih ili softverskih mehanizama. Zatim se izvrši kreiranje zahteva za izdavanjem sertifikata koji sadrži javni ključ vlasnika, koji se šalje ka CA.

U okviru datog PKI sistema, politika rada po kojoj se izdaju sertifikati od strane CA određuje nivo poverenja koje će strane u komunikaciji imati u datom sertifikatu. To je publikovano u okviru osnovnih dokumenata Sertifikacionog tela: Politika Sertifikacije (Certificate Policy - CP) i Praktična pravila rada (Certificate Practise Statement – CPS). Tako su definisane politike po kojima se izdaju sertifikati sa različitim nivoima pouzdanosti i u skladu sa tim definišu se različite metode registracije koje moraju biti primenjene u vezi sa licima koja zahtevaju sertifikate. U stvari, proces registracije podrazumeva prikupljanje i odgovarajuću proveru različitih podataka od krajnjih korisnika, direktno u ličnom kontaktu ili u indirektnom udaljenom zahtevu preko gejtveja (na primer web pretraživačkog programa).

U smislu procesa registracije, politika Sertifikacije PKI sistema detaljno definiše sledeće:

- Kako treba primeniti proces registracije;
- Koje informacije o licima je potrebno proveriti ili zapisati;
- Broj parova asimetričnih ključeva (i samim tim broj različitih sertifikata) koje treba generisati za datog korisnika (tipično se različiti parovi ključeva generišu za digitalno potpisivanje i za digitalnu envelopu (šifrovanje);
- Gde će se i na kom medijumu generisati ključevi; ključevi mogu biti generisani od strane samih korisnika, od strane RAO ili od strane CA, i mogu biti sačuvani na hard disku, disketi, mini CD medijumu, smart kartici ili nekom drugom tokenu;
- Format sertifikata koji treba da se generišu;
- Dodatne poslovne informacije koje treba da budu prikupljene za vreme procesa registracije.

REGISTRACIJA U LIČNOM KONTAKTU

Za određene PKI sisteme, direktne registracione procedure na bazi ličnog kontakta predstavljaju jedini bezbedni način za korektnu autentikaciju krajnjih korisnika i distribuciju i generisanje ključeva i sertifikata.

U Intranet okruženju, organizacija može da primeni politiku rada prema kojoj korisnici moraju lično da kontaktiraju osobu nadležnu za poslove bezbednosti u cilju preuzimanja tokena ili smart kartice sa njihovim ključevima i sertifikatima. Ova registracija zahteva da korisnik pokaže ID karticu zaposlenih, ličnu kartu, vozačku dozvolu, pasoš ili neki drugi metod identifikacije.

U Internet okruženju, organizacije sa javnim poslovnicama, kao što su banke, pošte, itd., mogu zahtevati od korisnika da lično dođu u datu poslovnicu i daju svoje lične podatke.

Registracija ličnim kontaktom se odvija tako što službenik koji koristi aplikaciju RAO modula unese lične informacije korisnika i potvrdi zahtev za izdavanje sertifikata (svojim digitalnim potpisom). Ključevi se mogu generisati od strane same RAO aplikacije i sačuvani na disku u zaštićenom obliku putem lozinke izabrane od strane korisnika, ili korisnik može da generiše sopstvene ključeve, a da dostavi samo zahtev za izdavanje sertifikata do RAO modula.

Određene RA aplikacije mogu koristiti i određene terminalne uređaje za akviziciju biometričkih podataka, kao što je fotografija, otisak prsta, glas, parametri zenice oka, itd., i da te netekstualne podatke takođe čuva u odgovarajućem obliku u bazi podataka.

Kada se izgeneriše digitalni sertifikat za datog korisnika, taj sertifikat može biti sačuvan na disketi, mini CD medijumu, hard disku, smart kartici ili na nekom drugom tokenu.

Proces izdavanja digitalnog sertifikata na bazi ličnog dolaska vlasnika u RA sastoji se iz sledećih koraka:

- Budući vlasnik digitalnog sertifikata dostavlja RAO svoje podatke lično;
- RAO formira zahtev za izdavanje sertifikata na bazi dobijenih podataka;
- RAO šalje kreirani zahtev do baze, označava ga kao procesirani i digitalno ga potpisuje;
- RA uzima procesirani zahtev iz baze, verifikuje ga, digitalno potpisuje i šalje ga kao zaštićenu standardizovanu poruku putem TCP/IP konekcije do CA;
- CA verifikuje dobijeni zahtev. Ukoliko je zahtev validan, CA izdaje i potpisuje digitalni sertifikat u X.509 standardnom formatu za dati zahtev i smešta ga u bazu podataka;
- CA publikuje sertifikate na X.500/LDAP direktorijum. CA takođe periodično publikuje listu povučenih sertifikata (CRL – Certificate Revocation List) i listu povučenih autoriteta (ARL – Authority Revocation List). Sve liste koje se izdaju moraju biti digitalno potpisane. ARL se referiše na sertifikate samih PKI komponenata (samo CA, CAO, RA, RAO, itd.), dok se CRL odnosi na vlasnike digitalnih sertifikata u okviru datog PKI sistema;
- CA šalje izdati sertifikat do RA preko TCP/IP. Digitalni sertifikat se sadrži u zaštićenoj (digitalno potpisanoj i šifrovanoj) standardizovanoj poruci;
- RA verifikuje datu poruku, digitalno je potpisuje i pridružuje je bazi podataka;
- RAO preuzima izdati sertifikat iz baze, verifikuje ga i čuva ga u zahtevanom formatu (PKCS#7, PKCS#12, ili drugi);
- RAO obezbeđuje dostavljanje digitalnog sertifikata vlasniku koji ga je tražio.

Prethodno navedeni proces predstavlja proces koji se sprovodi u slučaju da su CA, RA i RAO tradicionalno bazirane klijent-server aplikacije. U slučaju da se radi o modernijim WEB baziranim CA sistemima, proces registracije korisnika se sastoji u sledećim koracima:

- Budući vlasnik digitalnog sertifikata dostavlja RAO svoje podatke lično;
- RAO formira zahtev za izdavanje sertifikata na bazi dobijenih podataka;
- RAO digitalno potpisuje kreirani zahtev i šalje ga do CA (WEB server CA);
- CA (WEB server CA) verifikuje dobijeni zahtev. Ukoliko je zahtev validan, CA izdaje i potpisuje digitalni sertifikat u X.509 standardnom formatu za dati zahtev i smešta ga u bazu podataka;
- CA publikuje sertifikate na X.500/LDAP direktorijum. CA takođe periodično publikuje listu povučenih sertifikata (CRL – Certificate Revocation List) i listu povučenih autoriteta (ARL – Authority Revocation List). Sve liste koje se izdaju moraju biti digitalno potpisane. ARL se referiše na sertifikate samih PKI komponenata (samo CA, CAO, RA, RAO, itd.), dok se CRL odnosi na vlasnike digitalnih sertifikata u okviru datog PKI sistema;
- CA šalje izdati sertifikat do RAO preko TCP/IP. Digitalni sertifikat se sadrži u zaštićenoj (digitalno potpisanoj i šifrovanoj) standardizovanoj poruci;
- RA verifikuje datu poruku i obezbeđuje dostavljanje digitalnog sertifikata vlasniku koji ga je tražio.

UDALJENA REGISTRACIJA

U mnogim slučajevima, zahteva se metoda registracije koja se ne oslanja na registraciju ličnim kontaktom. Najčešće, ove metode se primenjuju kada je korisnik udaljen od RA. U tom slučaju,

omogućuje se registracija putem slanja zahteva za izdavanje sertifikata korišćenjem Internet pretraživačkih programa i WEB komunikacije, e-mail servisa ili VPN konekcija. Međutim, najčešće se u ove svrhe koristi metoda registracije korišćenjem web komunikacije. U tim slučajevima, korisnik svoj zahtev dostavlja do baze RA preko web komunikacije. Korišćenjem RAO modula se dati zahtev dalje procesira na isti način kao i u slučaju registracije putem ličnog kontakta. Alternativno, ako politika rada to dozvoljava, moguće je da RA bude konfigurisano tako da se dobijeni zahtevi automatski prosleđuju do CA, bez potvrđivanja od strane RAO.

Proces udaljene Sertifikacije uobičajeno uključuje sledeće korake:

- Budući vlasnik digitalnog sertifikata dostavlja zahtev za izdavanje sertifikata - Certificate service request (CSR - obično u PKCS#10 formatu) do web servera CA (web sajt CA) preko TCP/IP mreže;
- WEB server CA šalje dobijeni zahtev preko TCP/IP mreže do RA gde se dobijeni zahtev digitalno potpisuje i smešta u bazu podataka RA. Za ovu svrhu, postoji odgovarajuće RA na lokaciji CA;
- Operator RA (RAO) preuzima dobijeni zahtev iz baze podataka i procesira ga;
- RAO zatim vraća procesirani zahtev nazad u bazu pri čemu ga prethodno digitalno potpisuje i označava kao procesiranog;
- RA uzima procesirani zahtev iz baze, digitalno ga potpisuje i šalje ga kao zaštićenu standardizovanu poruku preko TCP/IP konekcije do CA;
- CA verifikuje dobijeni zahtev. Ukoliko je zahtev validan, CA izdaje i potpisuje digitalni sertifikat u X.509 standardnom formatu i smešta ga u bazu podataka;
- CA publikuje sertifikate na X.500/LDAP direktorijum. CA takođe periodično publikuje listu povučenih sertifikata (CRL – Certificate Revocation List) i listu povučenih autoriteta (ARL – Authority Revocation List). Sve liste koje se izdaju moraju biti digitalno potpisane. ARL se referiše na sertifikate samih PKI komponenata (samo CA, CAO, RA, RAO, itd.), dok se CRL odnosi na vlasnike digitalnih sertifikata u okviru datog PKI sistema;
- CA šalje izdati sertifikat do RA preko TCP/IP. Digitalni sertifikat se sadrži u zaštićenoj standardizovanoj poruci;
- RA verifikuje datu poruku, digitalno je potpisuje i pridružuje je bazi podataka;
- RA uzima digitalni sertifikat iz svoje baze podataka i šalje ga do web servera preko TCP/IP mreže;
- Web server omogućuje pristup digitalnom sertifikatu od strane vlasnika koji ga je zahtevao. U zavisnosti od konfiguracije, digitalni sertifikat se čuva na određenom direktorijumu na hard disku a URL adresa se šalje elektronskom poštom vlasniku.

SISTEMI ZA DISTRIBUCIJU SERTIFIKATA

Distribucija sertifikata je jedna od osnovnih funkcija koje dati PKI sistem treba da realizuje na fleksibilan način. Postoje tri različita tipa distribucije sertifikata:

- dostavljanje izdatih sertifikata do krajnjeg korisnika,
- publikovanje CA sertifikata,
- publikovanje izdatih i povučenih sertifikata krajnjih korisnika na odgovarajući način (putem odgovarajućih direktorijuma) u cilju da budu dostupni svim drugim korisnicima, kao i svim zainteresovanim stranama.

Sve ovo treba da bude realizovano tako da bude u službi krajnjeg korisnika i da koristi organizacionoj infrastrukturi.

Sertifikati za krajnje korisnike moraju biti isporučeni licu koje je podnelo zahtev na način i u formatu koji odgovara njegovim potrebama. Na primer, sertifikati koji su zahtevani ličnim kontaktom mogu biti izdati bilo u softveru bilo na kriptografskom hardveru, kao na primer smart kartici. Sertifikati izdati na osnovu udaljenih zahteva uglavnom su distribuirani na isti način kao što su zahtevi i stigli, na primer web komunikacijom.

Sertifikat samog CA mora biti javan i raspoloživ koliko god je to moguće. Svaki korisnik u sistemu mora biti sposoban da poseduje sertifikat CA pre nego što počne da koristi servise datog PKI sistema. Sertifikat CA je neophodan da bi se verifikovao digitalni potpis sertifikata svih učesnika u sistemu – tj. da bi se proverila autentičnost veze između identiteta određenog učesnika u sistemu i

njegovog javnog ključa asimetričnog kriptografskog sistema. Sertifikat CA, kao i ostali izdati sertifikati u sistemu, mogu biti isporučivani u različitim formatima, kao i publikovani na X.500 ili LDAP direktorijumu. Takođe, sledeća lista formata za zapis sertifikata treba da bude podržana u sistemu: PEM; DER, PKCS#7 i PKCS#10.

Korišćenje direktorijuma može značajno poboljšati funkcionalnost sistema. Naime, u cilju šifrovanja poruke i njenog slanja u obliku digitalne envelope, neophodno je posedovati sertifikat namenjenog primaoca. Takođe, u cilju verifikacije digitalnog potpisa neke poruke, potrebno je imati sertifikat potpisnika i mogućnost da se izvrši validacija datog sertifikata (da li je u važećem roku i da li nije povučen). Zbog ovih razloga, obično se sertifikati i CRL smeštaju na direktorijum koji je raspoloživ svim ovlašćenim učesnicima u sistemu.

Sertifikati i CRL mogu biti publikovani i na WEB sajtu CA, raspoloživi preko OCSP[21] servisa ili da budu distribuirani e-mail servisom do svih učesnika u sistemu, u zavisnosti od utvrđene politike rada CA.

UPRAVLJANJE ŽIVOTNIM VEKOM SERTIFIKATA

Sigurnost sertifikata, odnosno privatnog ključa, ne zavisi samo od dužine ključa već i vremenskog perioda u kom se koristi. Jedan od razloga je napredak u algoritmima za rastavljanje na proste faktore i napredak računarske tehnologije. Drugi, do sada ne spomenuti razlog, je izloženost ključa napadima. Što je duže ključ valjan, duži je i period u kom je javni ključ javno dostupan i može biti testiran na slabosti. Iz ovih razloga odluka o dužini vremena valjanosti sertifikata i pripadajućih ključeva zavisi od dužine ključa i namene sertifikata. Sertifikati koji se više koriste su više izloženi opasnosti. Kraći životni vek sertifikata povećava njihovu sigurnost, ali povećava i administrativne zadatke oko njihovog obnavljanja ili ponovnog izdavanja. U sklopu hijerarhijske infrastrukture javnih ključeva potrebno je takođe voditi računa o međusobnoj zavisnosti sertifikata. Kada sertifikat CA, koja je izdala druge sertifikate istekne, automatski ističu i svi njeni sertifikati. Znači da, sertifikati viši u hijerarhiji poverenja moraju imati duži vek trajanja, a da se ovaj vek smanjuje kako se spušta niz hijerarhiju do krajnjih korisnika. Sertifikati krajnjih korisnika označavaju povezanost krajnjeg korisnika sa institucijom koja je izdala sertifikat. Vreme valjanosti sertifikata krajnjih korisnika, odnosno period na koji se izdaju, treba da odražava najkraći planirani period pripadanja krajnjeg korisnika instituciji. Sertifikat izdavačke CA mora imati period važenja duži od jedne godine, da bi se osiguralo da sertifikati, koje izdaje, važe celu godinu nakon izdavanja. Ovaj sertifikat će biti najkorišćeniji u celom sistemu i prema tome najizloženiji. Sertifikat vrhovne CA treba imati najduže vreme valjanosti u sistemu. Preporuka je da trajanje sertifikata vrhovne CA bude duže od pet godina. Vrhovna Sertifikaciona ustanova će izdavati vrlo mali broj sertifikata, samo korisničkim Sertifikacijskim ustanovama i biće izdvojena od računarske mreže (offline) na fizički sigurnoj lokaciji, što je čini neizloženom i vrlo sigurnom. Prema ranijoj diskusiji o dužini ključeva, planirani ključ od 4096 bita, bi trebalo da garantuje sigurnost i za narednih dvadeset godina. Međutim, ovo je ogroman period za oblast računarske sigurnosti, a takođe se može očekivati da će biti i nekih administrativnih promena u ovom periodu. Period važenja mora da bude dovoljno siguran i dovoljno dug da se ne poremeti vreme valjanosti svih podsertifikata [50].

U okviru Politike Sertifikacije datog Sertifikacionog tela, neophodno je specificirati sve prethodno iznete procedure upravljanja životnim vekom sertifikata, kao što su: povlačenje, obnavljanje i suspenzija. U nastavku su opisane pomenute procedure.

OBNAVLJANJE SERTIFIKATA

Korisnički sertifikati važe ograničeni vremenski period, na primer godinu dana, što je propisano u okviru Politike Sertifikacije CA. Takođe može biti propisan period pre isteka perioda važnosti sertifikata kada će se u okviru aplikacije zaštite, dati korisnik automatski upozoriti da je blizu vreme isticanja validnosti sertifikata i da ga treba obnoviti. Ukoliko korisnici poseduju dva sertifikata čiji periodi validnosti moraju da se poklapaju, obnavljanje se istovremeno vrši za oba sertifikata (dva serijska broja) koji su povezani istim registarskim brojem – korisničkim imenom.

Potrebno je dodatno istaći da se obnavljanje mora izvršiti pre isteka roka važnosti sertifikata. Ako period važnosti sertifikata istekne, moraju se

21. On-line Certificate Status Protocol (OCSP). Predstavlja Internet protokol koji se koristi da klijent od servera dobije sve relevante infrormacije vezane za status sertifikata. Opisan je u dokumentu RFC 2560.

generisati potpuno novi sertifikati (novi ključevi) za datog korisnika. Takođe, treba istaći da se obnavljanje vrši tako da uvek bude izdat novi sertifikat koji ima rok važnosti tačno godinu dana posle datuma isticanja roka, uz obezbeđenje da bude uvek validan. Dakle, obnavljanje se vrši na period, 12 meseci plus odgovarajući broj dana (maksimalno 15), koliko je pre kraja roka validnosti zahtev za obnavljanjem predat. Ovo se reguliše u okviru upravljačke aplikacije CA.

POVLAČENJE SERTIFIKATA

Korisnički sertifikati se mogu povući (opozvati) iz dva razloga:

- Došlo je do nekih promena informacija iz sertifikata za datog korisnika;
- Došlo je do gubitka asimetričnog privatnog ključa korisnika ili je iz bilo kog razloga došlo do kompromitacije ključa datog korisnika.
-

U oba slučaja, korisnik je dužan da odmah prijavi CA ili RA nastalu promenu. Politikom Sertifikacije su specificirani odgovarajući službenici CA (najčešće RAO i CAO) koji imaju pravo povlačenja sertifikata.

Potrebno je dodatno istaći da se povlačenje, kao i obnavljanje, ukoliko korisnik ima dva sertifikata, uvek mora izvršiti za oba sertifikata koji su izdati.

SUSPENZIJA SERTIFIKATA

Postoji mogućnost i privremene suspenzije sertifikata određenog korisnika koja se vrši ako je primenjena odgovarajuća suspenzivna mera pružanja usluga Sertifikacije datom licu, ili zbog odlaska na duže odsustvo (možda čak i godišnji odmor). Procedura suspenzije je praktično ista kao i procedura povlačenja sertifikata jer se sertifikati publikuju na CRL listu. Razlika je u tome što suspendovani sertifikati mogu ponovo biti aktivni posle isteka suspenzije, dok se jednom povučeni sertifikati ne mogu nikada ponovo aktivirati. Proceduru suspenzije sertifikata uglavnom vrše ista lica kao i u slučaju povlačenja.

LISTA POVUČENIH SERTIFIKATA

Za vreme životnog veka sertifikata moguće je da se steknu razlozi da se dati sertifikat proglasi nevažećim i da se datom korisniku ne dozvoli pristup sistemu. U tom smislu, povlačenje sertifikata se odnosi na praksu proglašavanja nevažećim javnog ključa datog korisnika, čime se automatski i njegov tajni ključ proglašava nevažećim i datom korisniku se tako onemogućava validno digitalno potpisivanje poruka. Međutim, od suštinske je važnosti da informacija o povučenosti datog sertifikata bude što je moguće pre javno objavljena i dostupna svim učesnicima u sistemu (direktorijum, WEB sajt ili OCSP servis). Funkcija povlačenja sertifikata je u odgovornosti CAO, RAO, kao i samih krajnjih korisnika.

Obeležja PKI sistema koja podržavaju servis povlačenja sertifikata uključuju:

- Kreiranje liste povučenih sertifikata (CRL) verzije 2;
- Kreiranje interfejsa za povlačenje sertifikata u okviru CAO i RAO;
- Obezbeđivanje da se, ako je to u skladu sa politikom rada CA, zahtevi za povlačenjem sertifikata dostavljaju i od strane samih krajnjih korisnika;
- Publikovanje CRL na direktorijumu i korišćenje OCSP servisa;
- Korišćenje distributivnih tačaka za sertifikate (CDP – Certificate Distribution Points) koje omogućavaju deljenje CRL na manje delove i stoga njihovo brže pretraživanje;
- Korišćenje funkcije suspenzije sertifikata, umesto povlačenja jer se suspendovan sertifikat može ponovo učiniti validnim, dok se jednom povučeni sertifikat ne može učiniti ponovo validnim nego se mora izdati novi sertifikat;
- Zapisivanje razloga za povlačenje sertifikata je omogućeno korišćenjem CRL verzija 2;
- Periodično publikovanje CRL ili njeno ažuriranje sa svakom novom promenom u smislu dodavanja povučenih sertifikata. Vreme i učestalost ažuriranja CRL je propisano u Politici Sertifikacije CA;
- Zapisivanje vremena povlačenja sertifikata što je omogućeno korišćenjem CRL verzije 2;
- Opciono uključivanje lozinki u politiku izdavanja sertifikata koje omogućavaju krajnjim korisnicima da povuku njihove sopstvene sertifikate.

Lista povučenih sertifikata (CRL – Certificate Revocation List) omogućuje klijentima i serverima, kao i drugim entitetima koji komuniciraju u datom

PKI sistemu, proveru validnosti digitalnih sertifikata druge strane u komunikaciji.

CRL je binarna datoteka koja sadrži sledeće informacije:

- Listu povučenih sertifikata sa razlogom njihovog povlačenja;
- Naziv izdavaoca CRL;
- Vreme kada je CRL izdato;
- Vreme kada će sledeća verzija CRL biti publikovana.

Veoma važno je istaći da u slučaju kada CA koje izdaje sertifikate istovremeno publikuje i CRL, tada je CRL digitalno potpisana od strane CA, čime se omogućuje svim korisnicima da budu sigurni u informacije koje CRL sadrži.

Pristup CRL i provera validnosti sertifikata se vrši kada je potrebno koristiti javni ključ iz PKI sertifikata određenog korisnika kome treba poslati šifrovanu poruku ili treba verifikovati digitalni potpis primljene poruke od strane tog korisnika.

Bilo koja od pomenutih aktivnosti treba da sadrži sledeće korake:

- Proveriti validnost digitalnog sertifikata datog korisnika;
- Uzeti serijski broj sertifikata;
- Pristupiti (učitati) CRL (obično se to radi download-ovanjem sa X.500 direktorijuma korišćenjem LDAP pretrage i LDAP odgovora ili uzimanjem iz lokalno sačuvane CRL);
- Proveriti digitalni potpis CRL, vreme njenog publikovanja i vreme kada će sledeća verzija biti publikovana;
- Proveriti da li se dati sertifikat nalazi u CRL (na bazi serijskog broja);
- Alarmirati datog korisnika ako je sertifikat povučen;
- Izvršiti željenu kriptografsku aplikaciju ukoliko se sertifikat ne nalazi u CRL ili ako namenjeni korisnik, nakon alarma, preduzme aktivnosti da njegov sertifikat ne bude više u CRL.

Uobičajeno, CA je odgovorno za neporecivost transakcija, obezbeđujući audit log datoteke i čuvajući sve publikovane verzije CRL. Alternativno, korisnička aplikacija može realizovati mehanizme kojima se obezbeđuje neporecivost transakcija. Međutim, u tom slučaju, za svaku izvršenu transakciju, mora se čuvati sama poruka kao i CRL koje je korišćeno u trenutku kada je verifikovan digitalni potpis poruke (ili je poruka šifrovana javnim ključem korisnika). Jedino ste tada u mogućnosti da dokažete da ste koristili javni ključ namenjenog korisnika za verifikaciju ili šifrovanje u trenutku kada njegov digitalni sertifikat nije bio povučen.

Prednosti CRL:

- CRL je široko podržana tehnologija u okviru PKI industrije;
- CRL može biti distribuirano do krajnjih korisnika na različite načine, uključujući push i pull metodu;
- CRL može biti arhivirano da obezbedi neporecivost za prethodno izvršene transakcije;
- CA izdaje i PKI sertifikate i CRL;
- Mnoge PKI aplikacije mogu dobiti CRL sa X.500 direktorijuma korišćenjem DAP/LDAP protokola.

Prepoznata su sledeća ograničenja upotrebe CRL:

- Korisnik mora imati tekuću verziju CRL u trenutku verifikacije digitalnog potpisa ili šifrovanja podataka. Pošto je CRL datoteka, korisnikova aplikacija mora obezbediti novu verziju CRL, ako je kopija na njegovom lokalnom sistemu zastarela. U velikom PKI okruženju, korisnik može imati potrebu da obezbeđuje CRL veoma često, a samo CRL može biti veoma veliko. Stoga, sve to može značajno usporiti rad neke PKI aplikacije zbog neophodnosti da se uvek obezbeđuje poslednja verzija CRL sa veoma zauzetog direktorijumskog servera (ili neke druge CRL distribucione tačke);
- CRL se kreira i publikuje periodično, pri čemu je taj period određen Praktičnim pravilom rada CA (CPS – Certificate Practice Statement). U sistemu je potrebno veoma studiozno evaluirati koliko često treba kreirati i publikovati CRL u okviru datog PKI sistema. Prečesto publikovanje CRL može zagušiti čitavu infrastrukturu, dok nedovoljno često publikovanje može rezultovati u potencijalnoj mogućnosti da se neki sertifikati koriste iako su već povučeni.

CA periodično kreira CRL datoteku na bazi primljenih zahteva za povlačenjem izdatih digitalnih sertifikata. Po kreiranju, CRL uključuje informacije od kada je CRL validna, do kada je validna i kada će se kreirati nova verzija CRL koja će zameniti prethodnu verziju. Kao što je ranije rečeno, CA digitalno potpi-

suje CRL tako da krajnji korisnici mogu biti sigurni u integritet i autentičnost informacija u okviru CRL.

Kada istekne važnost digitalnih sertifikata, njihov status u vezi povučenosti se više ne prikazuje u okviru CRL. Ova mera pomaže da se minimizuje veličina CRL za vreme rada datog CA a i smatra se da status povučenosti nema značaja za sertifikat kome je istekla važnost.

Pored procedure povlačenja sertifikata, postoji i još jedno specijalno stanje koje se naziva suspenzija sertifikata koje je već pomenuto. Za razliku od povučenog sertifikata, suspendovan sertifikat ima karakteristiku da ponovo može biti validan. CA obično suspenduje sertifikate kada postoji bilo kakva sumnja da je tajni ključ korisnika kompromitovan ili izgubljen. To takođe može biti veoma korisno stanje sertifikata u slučajevima kada je krajnji korisnik siguran da jedno vreme neće koristiti svoj tajni ključ. Suspendujući svoj sertifikat, krajnji korisnik u stvari onemogućuje korišćenje svog tajnog ključa sve dok CA ne učini dati sertifikat ponovo validnim. Uslovi pod kojima se vrši suspenzija, prestanak suspenzije ili povlačenje sertifikata definisano je u CPS datog CA. Serijski broj suspendovanog sertifikata je uključen u CRL uz navedenu karakteristiku povlačenja: "suspendovan". Ako je sertifikat ponovo validan, njegov serijski broj se briše iz naredne publikovane verzije CRL.

Profil CRL koji odgovara standardu X.509v2 (RFC 2459) definiše osnovni skup informacija koje se očekuju da budu sadržane u svakoj CRL. Pomenuti profil takođe definiše lokacije u okviru CRL za često korišćene atribute, kao i zajedničke reprezentacije tih atributa.

Prema pomenutom standardu, profil nazvan CertificateList sadrži sledeća polja:

- tbsCertList koje sadrži sledeće podatke:
- version – kada se koriste ekstenzije, kako je specificirano standardom X.509 v2 profilom, ovo polje mora postojati i mora specificirati verziju 2;
- signature – sadrži identifikator algoritma kojim se digitalno potpisuje CRL;
- issuer – predstavlja izdavaoca CRL (najčešće je to CA koje izdaje digitalne sertifikate);
- thisUpdate – ukazuje na datum publikovanja date CRL;
- nextUpdate – ukazuje na datum kada će sledeća verzija CRL biti publikovana. Nova verzija može biti publikovana i pre navedenog datuma, ali nikako kasnije od toga;
- RevokedCertificates – digitalni sertifikati povučeni od strane CA su jedinstveno identifikovani njihovim serijskim brojem. Vreme povlačenja i druge CRL ekstenzije su takođe definisane;
- CRLextensions – polje koje može biti korišćeno samo ako se radi o verziji 2 i sadrži dodatne atribute koji mogu biti od koristi, kao što su: redni broj CRL, distribucionu tačku;
- signatureAlgorithm – sadrži identifikator algoritma koji CA koristi za digitalno potpisivanje polja tbsCertList i mora sadržati isti algoritam kao i prethodno navedeno polje signature;
- signatureValue – sadrži digitalni potpis polja tbsCertList kodovan po standardu ASN.1 DER.

CA je odgovorno za distribuciju i raspoloživost CRL i za okruženje koje opslužuje. Najčešće je to postignuto publikovanjem CRL na X.500 direktorijumskom serveru, kao tipičnom servisu podržanom od strane CA. Nakon toga je u odgovornosti krajnjeg korisnika, ili njegove softverske aplikacije, da preuzima CRL iz X.500 direktorijuma. Postoje i alternativni načini distribucije CRL, kao što je slanje CRL svim korisnicima putem elektronske pošte (push metod) ili objavljivanje CRL na odgovarajućem WEB sajtu CA sa koga korisnici mogu preuzeti (download-ovati) CRL datoteku (pull metod kao što je i preuzimanje CRL sa X.500 direktorijumskog servera). Pomenute dve alternative su manje prisutne u PKI okruženju iz razloga pogodnosti X.500 pristupa i široke rasprostranjenosti primene LDAP komunikacionog protokola korišćenog za interakciju sa X.500 direktorijumom.

DAP (Directory Access Protocol) je jedan od četiri protokola definisanih u okviru X.500 standarda u cilju podrške otvorenim i standardizovanim direktorijumskim servisima. Direktorijum, u X.500 standardnom smislu, predstavlja specijalnu formu baze podataka koja je dizajnirana da bude posebno pogodna za korišćenje na Internet-u i drugim distribuiranim sistemima.

X.500 standard definiše dve osnovne komponente direktorijuma:

- Direktorijumski sistemski agent (DSA) – za upravljanje informacijama u okviru

direktorijuma;
- Direktorijumski korisnički agent (DUA) – korisnička aplikacija koja omogućuje korisnički pristup direktorijumskim servisima.

DAP definiše protokol komunikacije između DUA i DSA koji omogućuje uspostavu konekcije između klijentske aplikacije i direktorijuma, preuzimanje informacije iz direktorijuma i ažuriranje informacija unutar direktorijuma.

LDAP (Lightweight Directory Access Protocol) pojednostavljuje pristup direktorijumskim servisima koji su modelovani na bazi X.500 standarda. LDAP ima slične funkcije kao i DAP ali radi direktno na TCP/IP protokolu.

BEZBEDNOST SERTIFIKACIONOG TELA

S obzirom da je CA srce čitavog PKI sistema, osnovni zahtev bezbednosti koji se postavlja pred PKI sistem je potpuna bezbednost samog CA. Ako je CA sistem kompromitovan internim ili eksternim napadom, i čitav PKI sistem je kompromitovan. Konkretno, CA sistem mora da realizuje sledeće:
- Potpunu bezbednost tajnih ključeva CA;
- Da spreči napade spoljašnjih zlonamernih korisnika;
- Da obezbedi redudantnost sistema i obezbeđenje operativnosti u slučaju bilo kakve havarije;
- Da obezbedi personalnu identifikaciju svih aktivnosti koje se sprovode od strane CAO i RAO.

Dakle, sistem bezbednosti CA treba da osigura potpunu bezbednost tajnih ključeva, integritet podataka i kontinuiranu raspoloživost sistema. Ove performanse sistema se ostvaruju primenom smart kartica za kontrolu pristupa važnim resursima sistema, za digitalno potpisivanje i zaštitu tajnosti poruka, kao i primenom hardverskih bezbednosnih modula (HSM) za ostvarivanje bezbednosno najkritičnijih aplikacija u sistemu (generisanje tajnog ključa CA i digitalno potpisivanje sertifikata (izdavanje sertifikata)). U tom smislu, tajni ključevi CA i RA sistema, kao i njihovih operatora, treba da su zaštićeni kriptografskim mehanizmima najvišeg nivoa. Svi važni podaci korišćeni od strane CA i RA se čuvaju u bazama podataka, što olakšava primenu redudantnih mehanizama u cilju sprečavanja gubitka podataka. Sve interakcije i razmene podataka između elemenata PKI sistema se digitalno potpisuju i šifruju u postupku digitalne envelope što osigurava nemogućnost pristupa datoj komunikaciji od strane zlonamernih korisnika. Obeležja koja bi trebalo da su podržana od strane konkretnog CA sistema:

- CA sistem treba da podrži korišćenje hardverskog bezbednosnog modula (HSM) za generisanje tajnog ključa samog CA, za bezbedno skladištenje podataka i za digitalno potpisivanje sertifikata;
- Sistem treba da podrži korišćenje smart kartica za bezbedno čuvanje podataka, kontrolu pristupa i generisanje/distribuciju ključeva i sertifikata na svim ključnim tačkama datog PKI sistema;
- Korišćenje standardnih poruka (u standardnom formatu) digitalno potpisane i šifrovane (digitalna envelopa) za svu komunikaciju između pojedinih elemenata i modula PKI sistema;
- Svaki pristup bazama podataka treba da ima jedinstveni procesni broj;
- CA sistem treba da ima mogućnost da bezbedno arhivira korisničke parove asimetričnih ključeva za šifrovanje u proceduri digitalne envelope u cilju omogućavanja njihovog naknadnog oporavka u slučaju da je potrebno dešifrovati podatke koji su šifrovani pomoću ovih ključeva;
- Potrebno je da dati PKI sistem prođe određenu zvaničnu Sertifikaciju od strane ovlašćenih laboratorija za tu svrhu u smislu sposobnosti za realizaciju aktivnosti za koje je dati sistem namenjen.

Kao što je već rečeno, bezbednost PKI sistema je određena bezbednošću pre svega tajnog ključa CA, ali i svih ostalih tajnih ključeva koji se koriste u sistemu. Ovaj nivo bezbednosti se može ostvariti samo uz korišćenje odgovarajućeg kriptografskog hardvera kako na strani korisnika sistema, tako i na strani samih ključnih elemenata u sistemu. U tom smislu, potrebno je koristiti smart kartice, kao kriptografski hardver prilagođen korišćenju za krajnje korisnike i za operatere u okviru PKI sistema, i hardverske kriptografske module (HSM), neophodne za korišćenje u serverskim aplikacijama i u samom CA sistemu. U sistemima u kojima se zahteva najviši nivo bezbednosti, HSM moduli se predviđaju za korišćenje i na nivou RAO i CAO operatora. U cilju obezbeđenja funkcije neporecivosti u sistemu, potreb-

no je da krajnji korisnici svoj asimetrični par ključeva generišu i čuvaju na kriptografskom hardveru (smart kartici). Drugim rečima, fundamentalni zahtev i svrha kriptografskog hardvera je da osigura da tajni ključ nikad ne napusti hardverski modul, u kom slučaju bi eventualno mogao biti kompromitovan.

SERVER ZA ARHIVIRANJE KLJUČEVA

PKI sistem treba da bude sposoban da se oporavi u smislu pune funkcionalnosti u slučaju sistemskih ili komunikacionih oštećenja koja se mogu desiti u korišćenju. Dakle, potrebno je da sistem ima realizovanu strategiju oporavka i neometanog daljeg rada u slučaju oštećenja prouzrokovanog višom silom. Uglavnom su dva osnovna kritična elementa PKI sistema: tajni ključevi i baza podataka. Ukoliko se realizuje pouzdana back-up funkcija ovih elemenata, čitav PKI sistem će biti sposoban da se kompletno oporavi i da se vrati u prethodno stanje.

Interna baza podataka PKI sistema (baza podataka CA i RA) koristi se uglavnom:

- Za čuvanje svih zahteva za izdavanje sertifikata, izdatih sertifikata i CRL;
- Kao baza za razmenu poruka između CA i RA;
- Za čuvanje log fajlova u čitavom sistemu i svih aktivnosti koje su realizovane od strane operatora;
- Za čuvanje detalja o registracionim politikama;
- Za čuvanje registracionih informacija koje nisu uključene u sertifikate (kao na primer atributi definisani od strane samih korisnika, skenirane fotografije, biometrički podaci, itd.).

Bezbednost čitavog sistema je ojačana tako što je svaki unos u bazu, ili postupak čitanja, digitalno potpisan uz pomoć tajnog ključa određenog procesa ili operatora koji je datu transakciju uradio. Pored toga, svaki zahtev za izdavanje sertifikata poseduje pridruženi identifikacioni broj transakcije, koji se koristi tokom procesiranja datog zahteva u datom PKI sistemu.

Korišćenje postupka digitalne envelope znači da šifrovanu informaciju može pročitati samo korisnik kome je ta informacija namenjena. Svaka organizacija, koja svoju bezbednost bazira na PKI sistemu, želi da bude sposobna i da može naknadno u izuzetnim slučajevima, da dešifruje neke podatke. U tom smislu, ne sme se dopustiti da se tajni asimetrični ključevi, kojima se jedino mogu dešifrovati simetrični ključevi, kojima su šifrovane određene poruke, izgube jer su tada izgubljene i te šifrovane poruke. Ovaj zahtev povlači za sobom sledeće:

- Važnim podacima firme, koji su šifrovani i namenjeni nekom službeniku, ne može se pristupiti ukoliko dati službenik u tom trenutku nije prisutan;
- Podaci se ne mogu dešifrovati ako je tajni ključ izgubljen ili oštećen;
- Podaci se ne mogu dešifrovati ako je lozinka zaboravljena;
- Krajnji korisnici mogu biti onda demotivisani (ili u strahu) da šifruju važne podatke plašeći se da ti podaci kasnije neće moći biti dešifrovani.

Navedeni problemi se mogu razrešiti ako bi se kopije tajnih ključeva čuvale na bezbednom mestu. To bi omogućilo oporavak u svakom trenutku šifrovanih podataka. Međutim, to bi takođe omogućilo verovatnoću pronevere digitalnih potpisa od strane zlonamerne osobe koja ima pristup bazi tajnih ključeva. To je neprihvatljivo sa stanovišta postizanja funkcije neporecivosti u sistemu.

Ovi problemi se na zadovoljavajući način mogu rešiti tako što se u sistemu omogući korisnicima da imaju više parova asimetričnih ključeva, a posledično i više sertifikata (po jedan sertifikat na svaki par ključeva). Jedan par ključeva treba da bude za šifrovanje, a drugi za digitalno potpisivanje. Najprihvatljivija šema je, da par ključeva za digitalno potpisivanje generiše sam korisnik, po mogućstvu na kriptografskom hardveru (smart kartici) koji obezbeđuje funkciju neporecivosti, a da par ključeva za šifrovanje generiše CA za datog korisnika i da mu ih dostavlja. U tom slučaju, CA može čuvati kopiju tajnog ključa za šifrovanje na serveru za arhiviranje podataka, što omogućuje potpun oporavak šifrovanih podataka (ukoliko na primer korisnik izgubi smart karticu), bez uticaja na funkciju neporecivosti datog korisnika.

Server za arhiviranje ključeva (Arhiv Server - AS) ima funkciju da bezbedno uskladišti tajne ključeve asimetričnog kriptografskog sistema krajnjih korisnika koji se primenjuju u okviru postupka digitalne envelope. Ova funkcija omogućuje kasniji oporavak datih ključeva, kao i eventualnog dešifrovanja šifrovanih poruka (postupkom digitalne envelope), u slučajevima gubitka ili oštećenja ključeva, ili u slučajevima kada određeni autoritet nalaže dešifrovanje poruka (u sudskim ili arbitražnim procesima, itd.). Ključevi se čuvaju na serveru za arhiviranje ključeva jedino u slučaju da je to izričito predviđeno politikom rada PKI sistema.

Funkcionalnost servera za arhiviranje ključeva

- Server za arhiviranje ključeva šifruje tajni ključ koga treba uskladištiti primenom određenog simetričnog algoritma sa odgovarajućim DEK (Data Encipherement Key) ključem, jedinstvenim za svaki tajni ključ koji se arhivira. Tako se šifrovani tajni ključ smešta u posebnu bazu podataka (AS baza podataka).
- DEK ključ se takođe šifruje posebnim simetričnim algoritmom i posebnim ključem i takođe se smešta u bazu podataka.
- Digitalno potpisivanje poruka – sve poruke poslate od strane arhiv servera su digitalno potpisane.
- Verifikacija poruka – sve digitalno potpisane poruke koje arhiv server dobija se procesiraju u smislu verifikacije digitalnog potpisa u cilju provere autentičnosti potpisnika i integriteta sadržaja poruke.
- Arhiviranje podataka – svi podaci i log fajlovi se arhiviraju u AS bazi podataka. Sve arhivirane informacije su digitalno potpisane od strane AS. Svaki ulazni slog ima jedinstveni procesni broj.

Obeležja Arhiv servera

- Arhiv server mora da poseduje grafički interfejs jednostavan za korišćenje sa interfejsom koji se može prilagoditi korisnikovim potrebama.
- Arhiv server treba da podrži različite hardverske elemente, kao što su: smart kartice, hardverski bezbednosni moduli (HSM) i drugi tokeni.

TIPOVI SERTIFIKACIONIH TELA I MOGUĆI NAČINI REALIZACIJE

Postoji nekoliko tipova CA, od kojih su četiri tipa najznačajnija:

- Pojedinačna CA određenih preduzeća (Corporate CA);
- CA zatvorenih grupa korisnika;
- CA vertikalnih industrija (finansijski sistemi, medicina, telekom, ...);
- Javna CA (domaća – internacionalna).
- Što se tiče načina realizacije CA, postoje generalno tri načina:
- Korišćenje usluga postojećeg CA (outsourced CA);
- Izgradnja sopstvenog CA u okviru date organizacije na bazi inostrane CA tehnologije (insourced CA);
- Izgradnja sopstvenog CA u okviru date organizacije na bazi domaće CA tehnologije (insourced CA).

Prva varijanta predstavlja najpovoljnije rešenje za kompaniju koja želi da implementira PKI tehnologiju isključivo u svojoj organizaciji (za svoje zaposlene i saradnike), a ne želi da investira previše u rešenje CA. U tom smislu, određene organizacije koje predstavljaju javna međunarodna CA (kao što su GlobalSign i VeriSign), nude outsourced CA rešenje u kojem oni praktično izdaju digitalne sertifikate korisnicima date organizacije, koja u tom slučaju igra ulogu RA.

Međutim, ukoliko organizacija pretenduje da ima određene ekonomske koristi od javne prodaje digitalnih sertifikata zainteresovanim korisnicima iz njihovog domena, tada su prikladnije druge dve varijante realizacije CA. To rešenje je onda značajno skuplje od prvo pomenutog rešenja outsourced CA. Od dve navedene insourced varijante, varijanta koja podrazumeva stranu CA tehnologiju je sigurno skuplja nego varijanta sa domaćom tehnologijom. Sa druge strane, realizacija CA sa domaćom tehnologijom omogućuje adaptivnost i skalabilnost rešenja u skladu sa definisanom politikom korisnika.

GENERIČKI PKI SISTEM

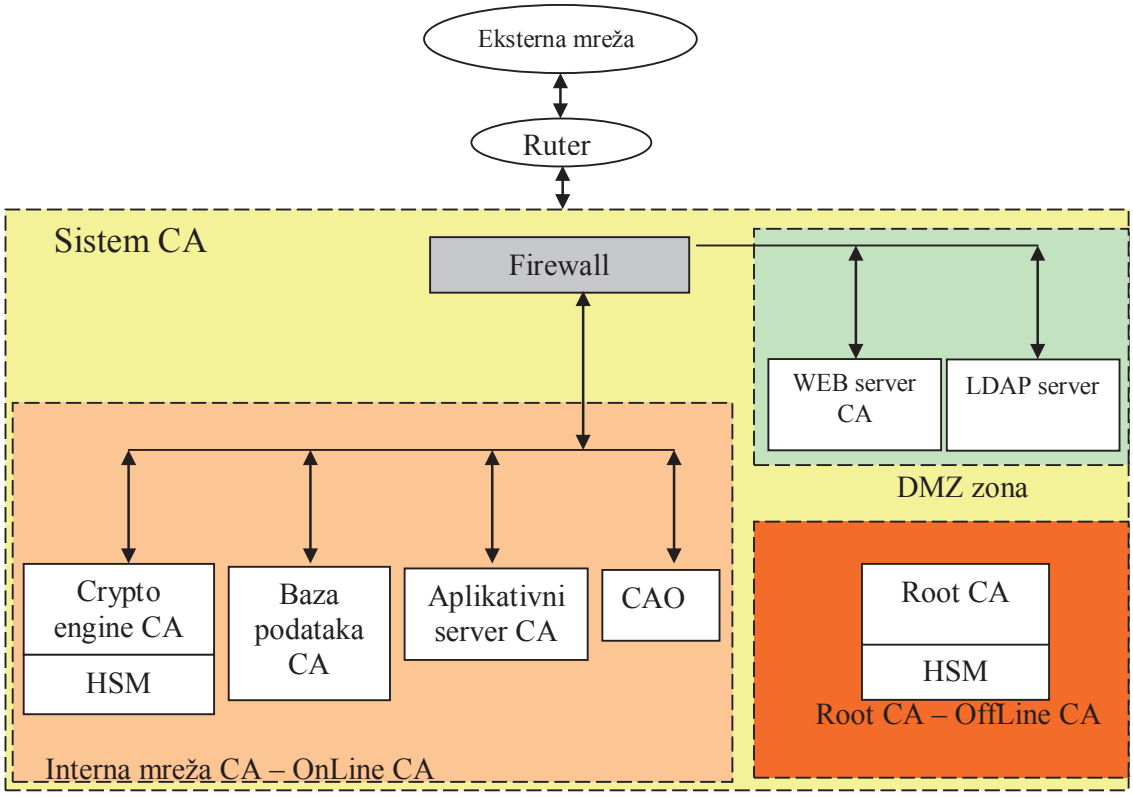
Generički CA sistem je WEB orijentisan CA sistem koji podržava zatvorene PKI sisteme sa striktno definisanim internim korisnicima. Ovi korisnici mogu biti podeljeni u jedan ili dva tipa korisničkih profila. Takođe, CA sistemi podržavaju i javne PKI sisteme koji imaju više korisničkih profila i više različitih načina registracije korisnika. Generički CA sistem predstavlja javni CA sistem, koji se u potpunosti može prilagoditi rezličitim potrebama korisnika. Glavne karakteristike generičkog CA sistema su sledeće:

- Realizovan u skladu sa važećim svetskim standardima;
- Primenjen X.509 v3 standard za sertifikate;
- Primenjen X.509 v2 standard za liste opozvanih sertifikata;
- PKCS standardi – najnovije verzije;
- Modularna realizacija;
- Fleksibilnost – prilagodljivost potrebama korisnika;
- Bezbedan sistem – primena najnovijih rezultata iz oblasti generisanja kriptografskih ključeva i primene kriptografskih algoritama;
- Različite baze podataka kao što su: MSSql, Oracle, DB2;
- Predstavlja WEB orijentisanu CA aplikaciju koja se bazira na korisničkim smart karticama;
- Podržava sistem sa jednim asimetričnim parom ključeva, sa dva para ključeva i kombinovanim sistemom;
- Podržava hijerarhijsku PKI strukturu i sadrži offline Root CA, kao i mnoge online Intermediate CA;
- Podržava različite načine registracija korisnika kao što su :
- - kroz registraciona tela (RA) i operatere registracionih tela (RAO),
- - direktne (za specifične korisničke profile), preko WEB CA servera;
- Sadrži proceduru distribuirane odgovornosti (deljena tajna, neophodnost prisustva tačnog broja određenih korisnika) u smislu kreiranja Root CA asimetričnog privatnog ključa za generisanje novog sertifikata Intermediate CA;
- Podržava funkcionisanje životnog ciklusa sertifikata (izdavanje suspenzija i povlačenje);
- Ima mogućnost elektronske personalizacije smart kartica i to omogućuje klijentima da to učine sami, ili uz pomoć RAO ili CAO;
- Sistem ima podršku za štampanje Pincoda, koji user dobija uz smart karticu;
- Sistem omogućuje štampanje različitih izveštaja u zavisnosti od potreba korisnika.
- Kao jedan primer centralnog sistemskog okruženja CA, navedena je uprošćena blok šema prikazana na slici 5.1, kao primer CA koje predstavlja višeslojnu WEB aplikaciju.

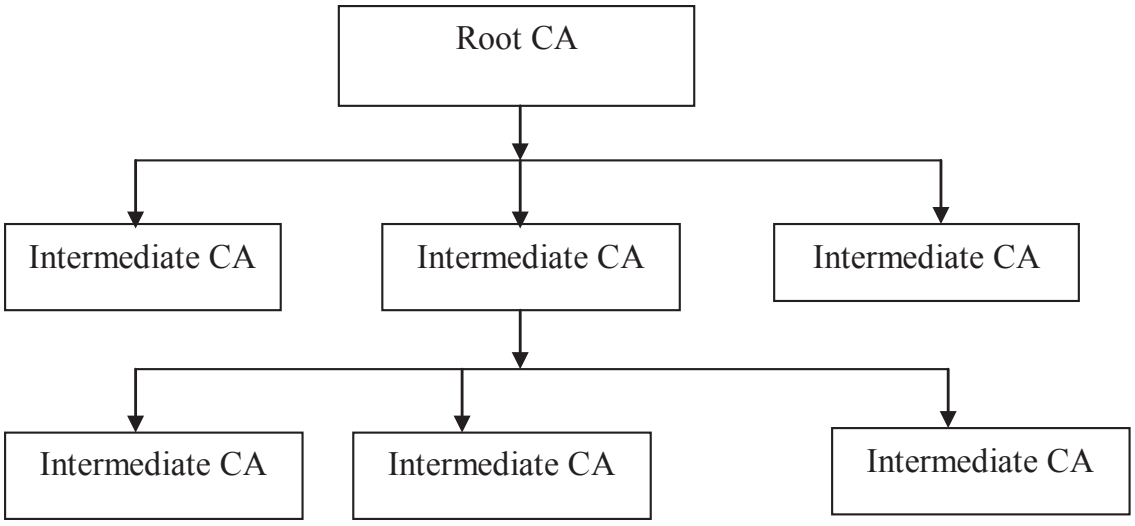
Kao što se vidi sa slike 5.1, Generički CA sistem se sastoji od OnLine i OffLine dela. OffLine deo predstavlja Root CA, koje se koristi samo u izuzetnim slučajevima kada se formira asimetrični privatni ključ i sertifikat za novi Intermediate CA u hijerarhijskoj strukturi, slika 5.2, koja preovladava u savremenim PKI sistemima. Root CA se nalazi u potpuno odvojenoj prostoriji od ostalog dela CA i u njemu postoji trezor u kome se čuvaju delovi privatnog ključa Root CA koji se propisanom procedurom distribuirane odgovornosti koriste u slučajevima generisanja novog Intermediate sertifikacionog tela (ta procedura se naziva “CA ceremonija”).

U proceduri CA ceremonije, potrebno je da prisustvuje odgovarajući minimalan broj specijalnih službenika CA koji imaju pristup pojedinim delovima privatnog ključa, koji se čuvaju u posebnim pretincima u trezoru i to najčešće u obliku smart kartica. Dakle, odgovarajući broj smart kartica mora biti prisutno, da bi se u HSM uređaju Root CA mogao formirati privatni ključ Root CA u skladu sa praktičnim pravilima rada sertifikacionog tela. Nakon toga se u HSM uređaju izvrši generisanje asimetričnog para ključeva za novi Intermediate CA i izgeneriše se njegov sertifikat primenom digitalnog potpisa na bazi privatnog ključa Root CA. Tako dobijenim privatnim ključem i sertifikatom isprogramira se najčešće smart kartica (u nastavku će biti više reči o smart karticama) Intermediate CA koja se zatim postavi u HSM uređaj novog, posebno za taj Intermediate CA obezbeđenog, Crypto Engine servera. Zatim se obriše privatni ključ Root CA iz HSM uređaja i specijalne smart kartice, sa delovima ključa, se vrate u trezor.

Dakle, kao što se može zaključiti, moguće je da istovremeno rade više Intermediate CA u OnLine režimu rada, tj. da više Intermediate CA Crypto Engine servera bude aktivirano u OnLine rad generisanja digitalnih sertifikata. OnLine procedura se odvija na sledeći način. Zahtevi za izdavanjem sertifikata čiji je digitalni potpis uspešno proveren od strane WEB servera CA (bilo da se radi o samopotpisanim sertifi-



Slika 5.1. Blok šema WEB baziranog generičkog CA sistema



Slika 5.2. Hijerarhijska struktura sertifikacionih tela

katima koje su korisnici dostavili direktno do WEB servera CA ili su to zahtevi potpisani od strane odgovarajućeg RAO u okviru RA gde je korisnik fizički došao da mu se izda sertifikat), se od strane aplikativnog servera CA, upućuju do odgovarajućeg Intermediate CA Crypto Engine servera iz kog domena je dati korisnik. Na datom Crypto Engine serveru (u okviru HSM uređaja datog servera) izvrši se formiranje digitalnog sertifikata (u slučaju samopotpisanog zahteva) ili se izvrši generisanje asimetričnog para ključeva i formiranje digitalnog sertifikata za datog korisnika. Ovi podaci se vraćaju aplikativnom serveru koji ih smešta u bazu podataka CA i šalje ih na odgovarajući način direktno korisniku ili u RA gde je korisnik podneo zahtev.

U DMZ zoni sistema CA se, pored WEB servera CA, nalazi i LDAP server koji služi za publikovanje CRL i ARL lista, kao i eventualno za publikaciju izdatih digitalnih sertifikata. Metode registracije korisnika već su opisane detaljno u glavi 4.4.

OPŠTA OBELEŽJA HSM

Hardverski bezbednosni moduli, realizovani u vidu računarskih koprocesora, predstavljaju veoma bitnu karakteristiku savremenih rešenja zaštite računarskih mreža. Ovi moduli povećavaju performanse sistema tako što se vremenski kritične kriptografske funkcije izvršavaju na specijalizovanom hardveru a ne u softveru host računara. Postojanje hardverskog koprocesorskog kriptografskog modula od suštinske je važnosti za realizaciju kvalitetnog i performantnog sistema zaštite, kao i za ispunjenje koncepta poverljive aplikacije u punom smislu. Svi bezbednosni mehanizmi (kriptografski algoritmi i funkcije kontrole pristupa) smešteni su na hardverskom modulu i nikada se ne učitavaju u radnu memoriju korisnikovog računara. Ovakvi kriptografski proizvodi su raspoloživi na svetskom tržištu i kreću se od PCI baziranih koprocesorskih modula, kao što su: CryptoSwift firme Rainbow Technologies, HSP4000 firme Baltimore Technologies, Luna VPN firme Chrysalis-ITS, itd. do PCMCIA baziranih rešenja, kao što su: FORTEZZA kartica firme Mykotronx, Luna 2, Luna CA 3 firme Chrysalis-ITS, itd. Osnovne funkcije navedenih proizvoda su povećanje bezbednosti sistema i ubrzavanje kriptografskih funkcija, kao što su asimetrični i simetrični kriptografski algoritmi.

Primena HSM modula je neophodan uslov za bezbednu realizaciju funkcija Sertifikacionog tela. Pomenuti proizvodi uglavnom realizuju standardne javne asimetrične i simetrične kriptografske i hash algoritme, kao što su: RSA, DSA, DES, 3-DES, RC2, RC4, SHA-1, MD2, MD5, itd. Postoje i eksterni kriptografski moduli, kao na primer Thales (Racal) WebSentry, koji mogu imati bolje performanse u smislu brzine i zaštite velike količine po-

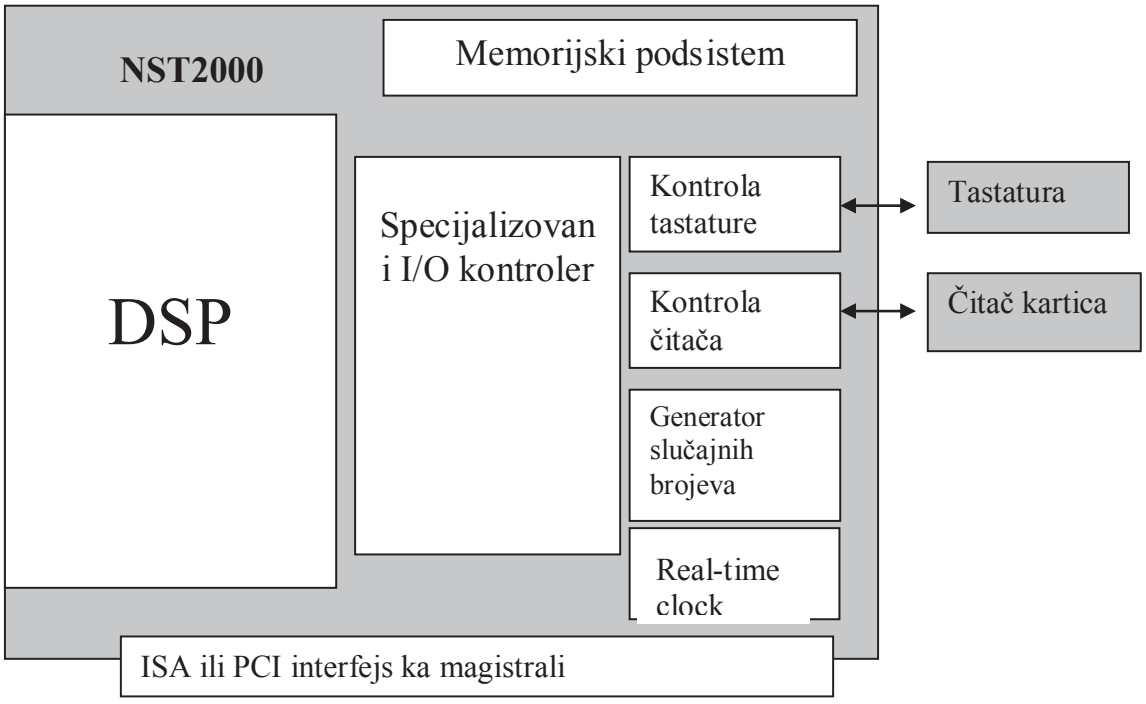
dataka. Interni kriptografski moduli su optimalni u slučaju kriptografskih sistema koji koriste princip rada sa porukama i primenjuju tehnologije digitalnog potpisa.

Hardverski kriptografski koprocesori se predviđaju za korišćenje u serverskim aplikacijama i eventualno u klijentskim aplikacijama gde se zahteva visok nivo bezbednosti (državni organi, vojska, policija, SMIP, specijalizovane službe). Sa druge strane, za najširi vid korišćenja sistema zaštite (npr. pojedinci), korišćenje smart kartica kao poverljive hardverske platforme je primerenije. U stvari, svi ti sistemi sa povišenim nivoom bezbednosti predstavljaju uglavnom kombinovane softversko-hardverske sisteme, pri čemu je hardverski deo ili koprocesor ili smart kartica. Sistemi sa najvišim nivoom bezbednosti koriste kombinovani softversko-hardverski sistem koji se sastoji od softverske aplikacije, kriptografskog koprocesora za realizaciju kriptografskih algoritama i smart kartica, kao bezbednih nosioca ključeva i digitalnih sertifikata.

HSM moduli u okviru sertifikacionih tela imaju sledeću funkcionalnost:

- Generisanje ključeva na HSM – generisanje para ključeva asimetričnog kriptografskog algoritma, kao i zahtevanog broja simetričnih ključeva (opciono), realizuje se unutar HSM;
- Bezbedno čuvanje kriptografskih parametara – ključevi i ostali kriptografski parametri se bezbedno čuvaju (u šifrovanom obliku) na HSM modulu;
- Bezbedni back-up kriptografskog materijala – ključevi i drugi kriptografski parametri se mogu bezbedno sačuvati (back-up-ovati) na smart karticama ili drugim HSM modulima;
- HSM mora realizovati funkciju detekcije pokušaja zlonamernog pristupa modulu (tamperproof) – modul treba da obezbedi detekciju zlonamernog pristupa i uništenje bezbednosnog materijala na modulu, ako je detektovan pristup;
- Modul mora biti sposoban da realizuje kriptografske funkcije – ovo je jedna od osnovnih namena HSM i ovi moduli su optimizovani za realizaciju funkcija generisanja ključeva, kao i realizaciju simetričnih i asimetričnih kriptografskih algoritama mnogo efikasnije nego u softveru ili na smart karticama;
- Bezbedno korišćenje PIN broja – modul se aktivira unošenjem PIN broja.

Postoje i domaći HSM moduli. Uprošćena blok šema jednog domaćeg HSM modula je prikazana na slici 5.1.1 [28].



Slika 5.1.1. Pojednostavljeni blok dijagram jednog domaćeg prototipa hardverskog koprocesorskog modula

OPŠTA OBELEŽJA 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
- logovanje na sistem.

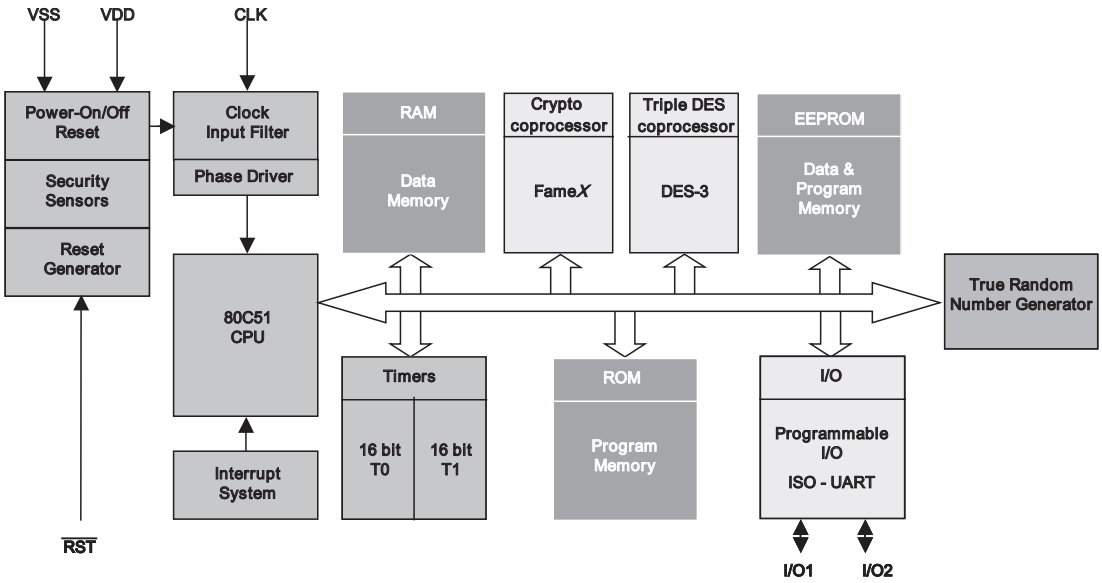
S obzirom da poseduju memoriju koja je mikroprocesorski zaštićena od neautorizovanog pristupa, skladištenje osetljivih informacija kao što su kriptografski ključevi, digitalni sertifikati, lozinke i druge forme ličnih informacija, na smart karticama je značajno bezbednije nego na drugim medijumima (kao na primer disketama ili mini CD medijumima). Pored toga, karakteristike disketa degradiraju u vremenu, one su nepouzdan medijum i ne postoje garancije da će korektno raditi u različitim tipovima drajvera, ukoliko se koriste nestandardni tipovi zapisa. 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.

Iskustva iz savremenih Internet mreža pokazala su da su smart kartice neuporedivo bezbednije od softverskih sistema baziranih na standardnim lozinkama. U savremenim računarskim mrežama predlažu se smart kartice za generisanje digitalnog potpisa, generisanje asimetričnih ključeva, za bezbednu identifikaciju subjekata, kao i da budu portabilni nosioci javnih i tajnih kriptografskih parametara. Kartica sadrži javno dostupni deo i PIN (Personal Identification Number) cod-om zaštićeni deo memorije u kojima se smeštaju kriptografski parametri.

Postoji nekoliko vrsta smart kartica:

- memorijske kartice,
- mikroprocesorske smart kartice sa korišćenjem PIN cod-a 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 bili 8-bitni mikrokontroleri, i to najčešće iz klase Intel 80C51 mikrokontrolera, a sada su to 16-bitni i 32-bitni mikrokontroleri. Jedan primer logičke arhitekture mikrokontrolera smart kartice koja ima PKI mogućnosti – digitalni potpis na samoj kartici (PKI smart kartica) je dat na slici 5.2.1. Ovaj čip je osmobitni čip i predstavlja jedan od ranije najzastupljenijih čipova koji su se koristili na smart karticama. U poslednje vreme su sve popularnije smart kartice bazirane na 16-bitnim i 32-bitnim mikrokontrolerima.



Slika 5.2.1. Primer arhitekture čipa mikroprocesorske smart kartice sa PKI mogućnostima – Phillips P8WE50xx familija kripto kontrolera

Ovi čipovi po pravilu poseduju dodatne kripto koprocesore 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 koprocesor) za realizaciju zaštićene razmene podataka (secure messaging) između smart kartice i odgovarajućeg softvera (middleware) na računaru. Primena smart kartica umnogome 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,
- multos kartice,
- JAVA smart kartice.

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

Sa druge strane, Multos i JAVA kartice nude veću mogućnost kastomizacije zahvaljujući postojanju Multos i JAVA virtualnih mašina koje izvršavaju Multos ALU-ove (Application Load Unit) i JAVA aplete, definisane od strane korisnika, na samoj kartici. Međutim, s obzirom da su se pojavile u skorije vreme, Multos i JAVA kartice bolje rade na čipovima koji se baziraju na jačim mikroprocesorima (16-bitni i 32-bitni). Multos i JAVA kartice su multiaplikativne kartice.

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 isporučioci 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, Infineon, Atmel, ST Microelectronics, Samsung, Hitachi, itd. su tradicionalni proizvođači čipova, dok su: Gemalto, Oberthur, Giesecke & Devrient, Sagem Orga, Austria Card, 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 kriptozaštićene aplikacije (kontaktni čip), da se koriste i za realizaciju bezbednog sistema kontrole 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 (parova) 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 i ne postoji mogućnost da generisani asimetrični ključ izađe sa kartice;
- Generisanje digitalnog potpisa na samoj kartici korišćenjem privatnog ključa koji nikada ne može da se izvadi i koristi van kartice;
- Smart kartice su same po sebi „tamperproof“ moduli, tj. moduli koji imaju zaštitu od pokušaja fizičkog narušavanja bezbednosti.

Kod primene smart kartica, neophodno je posedovati sledeće:

- smart karticu sa čipom koji omogućava primenu asimetričnih kriptoalgoritama (na primer RSA – RSA koprocesor);
- instaliranu PKI aplikaciju na samoj smart kartici koja prihvata veći broj parova, asimetrični privatni ključ – sertifikat (ova aplikacija obično automatski dolazi sa smart karticom);
- čitač smart kartica koji ima instaliran odgovarajući drajver na računaru;
- middleware softver koji se instalira na radnoj stanici i koji obezbeđuje proizvođač operativnog sistema smart kartica (može biti od samog proizvođača ili od neke treće strane koja je angažovana od strane proizvođača), a koji se sastoji, između ostalog, od:
  - CSP (Cryptographic Service Provider) za datu karticu;
  - PKCS#11 biblioteke;
  - Neke vrste Token manager-a koji služi za administraciju kartice (pregled sadržaja kartice, PIN i PUK administracija, brisanje objekata, itd.).

MICROSOFT PKI REŠENJE

Potrebno je istaći da navedeni generički primer realizacije sistema CA predstavlja jedan od mogućih načina realizacije. Drugi način je primenom Microsoft CA. Dizajn generičkog modela i Microsoft CA modela je manje više sličan i svodi se na izbor kakva će CA hijerarhija da izgleda (broj nivoa CA i njihova uloga), na koji način će se štititi privatni ključevi CA (na USB tokenu, smart karticama, HSM uređaju), gde će se publikovati CRL liste i CA javni ključevi. Mesta publikovanja se naziva CDP (Certificate distribution points). Najveća prednost Microsoft CA leži u činjenici da je besplatan jer se nalazi kao sastavni deo Microsoft 2003 server operativnog sistema u okviru njegove licence. Takođe licence po sertifikatima su besplatne za razliku od bilo kog drugog brand name CA. Osim iznetih prednosti postoji još i čitav niz benefita koje Microsoft Enterpise CA donosi, kao i dodatnih funkcija kao što su windows logon, različite integracije, za razliku od drugih besplatnih CA (Open source, EJBCA itd).

Za realizaciju internog PKI sistema u organizaciji koja ima interne korisnike potrebno je da se za potrebe internih korisnika implementacija bazira na MS Enterprise CA. Pri tome, oba pomenuta CA mogu biti Intermediate (subordinate) CA jednog jedinstvenog Root CA koji je offline, i koji može biti MS Standalone Root CA. Pored toga, najveći benefiti primene Subordinate Enterprise CA za interne korisnike je ako se čitav sistem bazira na smart karticama za interne korisnike i uvođenju sistema logovanja na Windows domen prilikom uključivanja računara na bazi smart kartice i odgovarajućeg sertifikata izdatog na njoj. Ovo se najlakše i najpriprodnije može realizovati ukoliko se u organizaciji uspostavi MS Enterprise CA koje je integrisano sa Active Directory-jem. Takođe, neophodno je izabrati i odgovarajući templejt za sertifikate koji se izdaju internim korisnicima u cilju postizanja optimalne funkcionalnosti. Uvođenjem Windows logon karakteristike, organizacija u potpunosti realizovala sistem jake (dvo-faktorske) autentikacije internih korisnika. Na osnovu do sada iznetog predlažu se osnovne komponente PKI sistema za interne korisnike u organizaciji:

- Microsoft Stand-alone Root CA koji je podignut za potrebe PKI sistema Organizacije kao vrh u PKI hijerarhiji (Top Level CA – Root CA Organizacije);
- Microsoft Enterprise Subordinate CA koji je integrisan sa Aktivnim direktorijumom kao CA izdavalac (issuing CA) sertifikata korisnicima;
- Smart kartice za zaposlene (uz čitač smart kartica) na kojima se izdaju sertifikati za Windows logon, zaštićeno slanje S/MIME email poruka (korporativni zaštićeni mail) i SSL klijentsku autentikaciju;
- E-mail klijenata (MS Outlook i MS Outlook Express) u kojima se koriste pomenute kartice za digitalno potpisivanje i šifrovanje, kao i Internet browser program ili odgovarajuća aplikacija za SSL zaštićen pristup web aplikacijama i web servisima.

U poglavlju eksperimentalne implementacije MS CA biće izložen korak po korak način podizanja MS CA u Organizaciji kojim bi se obezbedila laka implementacija, niski troškovi, i dovoljan nivo sigurnosti saglasno FIPS 140-2 (Federal Information Processing Standard)[19] .

PLAN IZGRADNJE INTERNOG PKI SISTEMA U ORGANIZACIJI NA BAZI MS CERTIFICATE SERVICES

Na osnovu iskustava u radu sa PKI sistemima, može se reći da je svetski trend, da kompanije koje koriste sisteme, elektronskog poslovanja, a pored toga imaju interne korisnike (zaposlene) i eksterne korisnike (korisnike i partnere), svoje PKI sisteme za potrebe realizacije sistema zaštićenog elektronskog poslovanja realizuju na sledeći način:

- Uspostava Microsoft Enterprise CA (CA – Certification Authority) koji je integrisan sa Aktivnim Direktorijumom za potrebe izdavanja digitalnih sertifikata internim korisnicima jer obezbeđuje Windows logon funkciju, kao i funkcije klijentske SSL autentikacije i zaštićenog standardnog S/MIME e-mail sistema;
- Uspostava posebnog privatnog CA za potrebe izdavanja sertifikata eksternim korisnicima koji može biti takav da zadovoljava uslove za izdavanje kvalifikovanih elektronskih sertifikata, ukoliko je to potrebno. To je potrebno u slučaju da data Organizacija želi da izdaje kvalifikovane sertifikate fizičkim i pravnim licima za javne potrebe;

Pomenuta dva CA mogu da budu (češći slučaj) dva intermediate CA pod jedinstvenim offline Root CA (u jedinstvenoj PKI hijerarhiji) ili mogu imati razdvojene Root CA sertifikate;

19. Standard koji je propisan od strane vlade SAD-a, a koji se odnosi na IT proizvode sa osetljivom namenom.

U okviru ovog rada, biće opisana realizacija offline Standalone MS Root CA koji treba da bude vrh u PKI hijerarhiji Organizacije. Predlaže se da pomenuti Root CA izda sertifikat i Subordinate MS Sertifikacionom telu koje će izdavati sertifikate za potrebe internih korisnika, tj. za potrebe uspostave PKI okruženja koje omogućuje: zaštićeno logovanje internih korisnika na Windows domen Organizacije, zaštićene razmene fajlova putem e-maila u okviru informacionog sistema Organizacije, kao i zaštićene SSL klijentske autentikacije za potrebe odgovarajućih web aplikacija i web servisa Organizacije;

Ukoliko bude potrebno kasnije dodavati odgovarajući CA sistem, koji će izdavati kvalifikovane sertifikate eksternim korisnicima, tada je moguće da tom posebnom intermediate Sertifikacionom telu sertifikat izda pomenuti Standalone Root CA. Druga opcija je da to bude intermediate CA u uspostavljenoj nacionalnoj PKI hijerarhiji akreditovanih kvalifikovanih CA sa Root CA u okviru Nacionalnog PKI organa. Sve to mora biti usklađeno sa trenutnom pravnom regulativom u vezi elektronskih potpisa u našoj zemlji. U tom smislu, u Prilozima 1 - 3 ovog rada su bliže razmatrane sledeće teme:

- Kvalifikovani elektronski potpis;
- Zakon o elektronskom potpisu;
- Odgovarajući podzakonski akti.

PREDLOG INTERNE PKI HIJERARHIJE U OKVIRU ORGANIZACIJE

Pre nego što se implementiraju Microsoft Windows Server 2003 Certificate Services u nekoj organizaciji, neophodno je pažljivo definisati i dizajnirati hijerarhiju Sertifikacionih tela. Drugim rečima, potrebno je definisati elemente CA hijerarhije, kao što su:

- Broj nivoa koji se koriste u okviru CA hijerarhije;
- Kako će Sertifikaciona tela biti pozicionirana u okviru CA hijerarhije;
- Tipovi sertifikata koje će svaki CA da izdaje;
- Tipovi sertifikata koji će biti implementirani na svakom nivou;
- Koliko sertifikacionih tela će biti na svakom nivou;
- Bezbednosne mere koje treba da štite CA;
- Da li će biti potrebne različite politike sertifikacije da se primenjuju u isto vreme.

Pošto se radi o privatnom sistemu i veoma zatvorenoj grupi korisnika (CUG – Closed User Group) u kome svi korisnici komuniciraju samo i isključivo u okviru informacionog sistema organizacije, nema nijednog razloga da se zahteva izgradnja komplikovanog i skupog “brand-name” PKI sistema za ove potrebe.

Takođe, s obzirom na zatvorenost sistema, od datog PKI sistema se, u ovom trenutku, ne očekuje da bude sa takvim karakteristikama da može i da treba da bude akreditovan za izdavanje kvalifikovanih sertifikata od strane ovlašćenog Nacionalnog autoriteta za PKI infrastrukturu u Srbiji.

U tom smislu, predlaže se implementacija hijerarhijske infrastrukture na bazi Microsoft Certificate Servisa kao kombinacije stand-alone Root CA i Enterprise Subordinate CA. Ova varijanta se predlaže iz sledećih razloga:

- MS Certificate servisi su uključeni u licencu Microsoft Windows 2000 ili 2003 servera – nema dodatnih troškova za nabavku CA. Naime, u ovom trenutku nema razloga da se investira u neki “brand-name” PKI proizvod sa tržišta jer se radi o zatvorenoj grupi relativno malog broja internih korisnika;
- Ne postoji posebna licenca za izdati sertifikat od strane MS Certificate servisa što nije slučaj kod drugih PKI rešenja.

Ukoliko se ukaže odgovarajuća potreba za izdavanjem sertifikata za javne potrebe od strane organizacije, može se razmišljati i o nabavci PKI sistema koji će biti takav da može da bude akreditovan od strane nadležnog Nacionalnog Srpskog PKI autoriteta za izdavanje kvalifikovanih sertifikata za odgovarajuće eksterne korisnike u Republici Srbiji. S obzirom na specifičnost organizacije koja ima zatvorenu strukturu poslovanja, predlaže se realizacije dvo-nivoiske CA hijerarhije sa sledećim karakteristikama:

- Root CA – Standalone offline Microsoft CA;
- Subordinate CA – Enterprise Micrososft Subordinate CA koje predstavlja u isto vreme i Policy i Issuing CA (prema MS terminologiji) koje izdaje sertifikate internim korisnicima Organizacije računarske mreže;
- U predloženoj hijerarhiji postojaće jedno Root CA i jedno Subordinate CA koje izdaje sertifikate internim korisnicima,

- Naravno, na drugom nivou je neophodno obezbediti sve potrebne back-up operacije, kao i formirati redundantno okruženje, radi eliminisanja jedinstvene tačke ispada (single point of failure) ukoliko bi se primenilo samo jedno issuing CA.

Dvo-nivoiska CA hijerarhija se sastoji od jednog Root CA, kao i jednog ili više policy/issuing CA, slika 6.2.1.

Da bi se osigurala maksimalna bezbednost rešenja u okviru dvo-nivoiske CA hijerarhije, Root CA se implementira kao standalone offline Root CA koje je izdvojeno izvan računarske mreže Organizacije. Za tu svrhu se koristi Standalone Root CA (Organizacije Root CA). CA koje izdaje sertifikate internim korisnicima se implementira kao Subordinate Enterprise CA – online issuing CA, a izdati sertifikati će na vrhu svog lanca sertifikata imati Root CA sertifikat koji je izdat offline Standalone Root CA sistemu u ovoj konfiguraciji.

Da bi se povećala redundantnost i pouzdanost sistema, potrebno je obezbediti redundantnost online issuing CA bilo kao hot stand-by ili cold stand-by sistem. Najjednostavnije rešenje je korišćenje cold stand-by rešenja koje omogućava relativno brzi oporavak (doduše ne trenutni) ukoliko glavni CA server otkaže uz mnogo manju komplikovanost rešenja u odnosu na hot stand-by rešenje.

OSNOVNE PROCEDURE RADA U OKVIRU INTERNOG PKI SISTEMA ORGANIZACIJE

Predlog osnovnih postupaka u radu internog CA Organizacije:

1. CA Organizacije obavlja sledeće zadatke:

   - prima zahteve za izdavanje sertifikata (uključujući i proveru identiteta podnosioca zahteva),
   - izdaje digitalne sertifikate,
   - ukoliko se to traži, daje pozitivan ili negativan odgovor na upit o validnosti sertifikata,
   - prima zahteve za povlačenje digitalnih sertifikata,
   - proverava autentičnost zahteva za povlačenja digitalnih sertifikata,
   - povlači digitalne sertifikate,
   - čuva podatke o sertifikatima na sigurnom mestu.

2. Procedure pri izdavanju sertifikata:

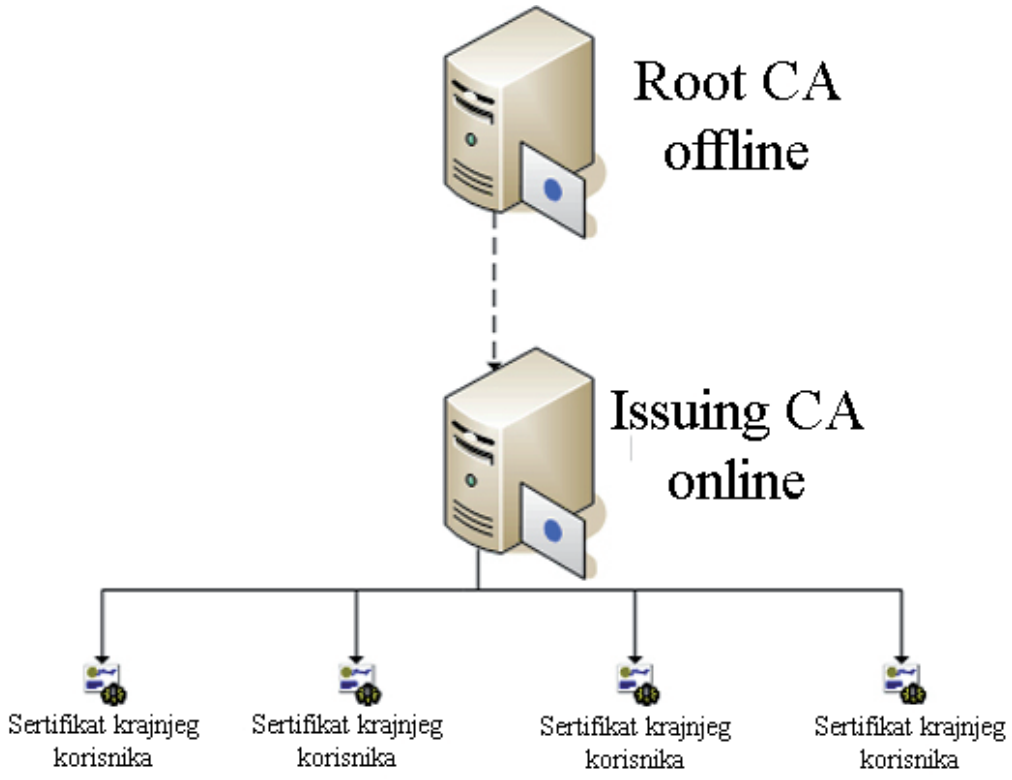
   - primanje zahteva za izdavanje sertifikata,
   - sakupljanje podataka o podnosiocu zahteva,
   - provera identiteta podnosioca zahteva,
   - provera da li podnosilac zahteva ispunjava uslove za izdavanje sertifikata,
   - provera validnosti PIN koda,
   - upoznavanje podnosioca zahteva sa odredbama polise o korišćenju digitalnog sertifikata,
   - upoznavanje podnosioca zahteva sa korišćenjem digitalnog sertifikata,
   - kreiranje korisničkog naloga za podnosioca zahteva,
   - generisanje para ključeva na smart kartici,
   - kreiranje digitalnog sertifikata i smeštanje na SmartCard,
   - provera funkcionalnosti kombinacije SmartCard-a i digitalnog sertifikata,
   - arhiviranje dokumentacije o zahtevu.

3. Pri izdavanju sertifikata, podacima o korisniku se pridružuju i podaci o licu koje je izdalo sertifikat (enrollment agent), datumu i vremenu prijema zahteva, kao i datumu i vremenu izdavanja sertifikata.
4. Uslovi za povlačenje sertifikata:

   - podaci o korisniku sertifikata su se izmenili u odnosu na podatke na osnovu kojih je sertifikat izdat,
   - korisnik je prekršio odredbe politika i pravila o korišćenju digitalnih sertifikata,
   - privatni ključ korisnika je kompromitovan,
   - korisnik ili neko drugo lice koje na to ima pravo su zatražili povlačenje.

5. U toku produkcionog rada sertifikacionog tela potrebno je raditi dnevnu rezervnu kopiju podataka koja sadrži sledeće:

   - dnevnik događaja (event log),
   - bazu izdatih i povučenih sertifikata



Slika 6.2.1. Dvo-nivoiska CA hijerarhija

6. Privatni ključevi CA se ne smeju arhivirati van rezervne kopije CA baze.
7. Ukoliko je istekao sertifikat, privatni ključ koji je pridružen tom sertifikatu mora biti uništen, a u slučaju da je smešten na smart kartici, smart kartica mora biti formatirana.

Potrebno je napomenuti da je gore navedena i opisana procedura po kojoj se privatni ključ CA kreira putem softverskog CSP-a, kao i da se traži njegov bezbedni back-up. Međutim, u kasnijoj fazi iz razloga bezbednosti, preporučuje se generisanje privatnog ključa na nekoj hardverskoj platformi (HSM ili smart kartica) kada ne bi bilo potrebe za softverskim back-up-om privatnog ključa CA. Kratak opis rada HSM uređaja je bio detaljno objašnjen u poglavlju 5.1.

IMPLEMENTACIJA

U nastavku će biti prikazan način implementacije dvo-nivoiske hijerarhije sa jednim Root CA i jednim Policy/Issuing CA. Da bi se osigurala maksimalna bezbednost rešenja u okviru dvo-nivoiske hijerarhije, Root CA se implementira kao Offline Standalone Root i predstavlja vrh u PKI hijerarhiji Organizacije. Root CA će izdavati sertifikate za Microsoft Subordinate CA, koje će izdavati sertifikate za interne korisnike Organizacije. Da bi se realizovala ova dvo-nivoiska hijerarhija, neophodno je instalirati MS Certificate servise kao MS Stand-alone CA za Root CA. Za tu svrhu je neophodno obezbediti jedan poseban server i na njemu instalirati Microsoft Windows Server 2003, Standard Edition. Taj server će predstavljati offline Stand-alone CA u Microsoft terminologiji. CA koje izdaje sertifikate internim korisnicima se implementira kao MS Enterprise Subordinate CA. Za tu svrhu takođe je neophodno obezbediti jedan poseban server i na njemu instalirati Microsoft Windows Server 2003, Enterprise editon.

Implementacija svakog CA se može primeniti u 3 koraka :

-preinstalaciona konfiguracija
-instalacija Certificate services
-postinstalaciona konfiguracija

PREINSTALACIONA KONFIGURACIJA

Prvi korak u podešavanju konfiguracije je kreiranje CAPolicy.Inf fajla. CAPolicy.Inf fajl sadrži podatke koji su neophodni za instalaciju CA i ponovno izdavanje CA sertifikata. CAPolicy.Inf fajl se smešta u folder %windir%.

Podaci koji mogu da se upišu u CAPolicy.Inf fajl su:

- CDP (Certificate revocation list publication points) su: Web lokacije, LDAP lokacije i putanje u lokalnom fajl sistemu na kojima će se publikovati CRL liste. Koriste se kada se verifikuje lanac sertifikata.
- CA certificate publication points - Mesta publikovanja CA sertifikata su takođe predstavljena: Web lokacijama, LDAP lokacijama ili putanjama u lokalnom fajl sistemu.
- Enhanced Key Usage nam govori koje sve vrste sertifikata može da izdaje sertifikaciono telo.
- The renewal configuration - Parametri za obnavljanje para ključeva Root CA sadrže podatak o dužini ključa i periodu validnosti CA sertifikata i obično se poklapaju sa inicijalnom dužinom ključa i dužinom trajanja Root CA sertifikata.
- Certification practice statement informacije sadrže procedure i praktična pravila rada koja se primenjuju u radu sertifikacionog tijela. Mogu da se navode u CAPolicy.Inf fajlovima: Root CA jednonivovske hijerarhije, Policy/Issuing CA dvonivovske hijerarhije i Policy CA tronivovske hijerarhije.
- CRL publication interval - Period publikovanja CRL lista definiše nakon kog vremena će se ponovo publikovati CRL lista.
- Delta CRL publication interval - Period publikovanja delta CRL lista definiše nakon kog vremena će se ponovo publikovati delta CRL liste. Ako je on 0 delta CRL liste uopšte neće biti publikovane.
- Basic Constraints Dozvoljavaju onemogućavanje kompleksnih hijerarhija a mogu i sadržati informaciju o tome da li CA izdaje sertifikate samo Issued CA telima ili krajnjim korisnicima.

Primer Capolicy.inf fajla prikazan je na slici 7.1.1. (na sledećoj strani).

U ovom primeru možemo primetiti OID brojeve. OID brojevi su jedinstvene sekvence brojeva koji identifikuju pojedini objekt direktorijuma ili attribut. OID brojevi (Object Identifier) koji se nalaze u sekcijama [LegalPolicy1] i [LegalPolicy2] se besplatno mogu dobiti od IANA[19] organizacije. OID brojevi koji se nalaze u sekciji [EnhancedKeyUsageExtension] su predefinisani IANA brojevi.

U ovom primeru se takođe može primetiti da su u sekcijama CDP i AIA korišćene AIA i CDP varijable. U tabeli 7.1.1. (strana 70) su date njihove definicije [51]:

Sledeći korak je instalacija Certificate Services uz obaveznu proveru tačnog vremena na računaru. Ova instalacija će biti detaljno objašnjena kako za Root CA tako i za Enterprise Subordinate CA.

POSTINSTALACIONA KONFIGURACIJA

Postinstalaciona konfiguracija se sastoji od upisivanja niza podataka u registar CA računara i može se obaviti na tri načina:

- Korišćenjem certutil.exe alata sa komandne linije ili pisanjem skripte sa nizom certutil naredbi;
- korišćenjem Certification Authority snap-

19. Internet Assigned Numbers Authority, http://www.iana.org

```
[Version]
Signature= "$Windows NT$"
[PolicyStatementExtension]
Policies = LegalPolicy1
Policies = LegalPolicy2
Critical = 0
[LegalPolicy1]
OID = 1.3.6.1.4.1.311.21.43
Notice = "Legal policy statement 1 text."
URL = "http://ime_web_servera.organizacija.com/certdata/cps.asp"
[LegalPolicy2]
OID = 1.3.6.1.4.1.311.21.44
Notice = "Legal policy statement 2 text ."
URL = "http://ime_web_servera.organizacija.com/certdata/cps.asp"
[AuthorityInformationAccess]
Empty = true
;URL = http://%1/certdata/Ime_CA.crt
;URL = ftp://ftp.organizacija.com/certdata/ Ime_CA.crt
;URL = file://\\%1\certdata\ Ime_CA.crt.crt
Critical = false
[CRLDistributionPoint]
Empty = true
;URL = http://%1/certdata/Ime_CA.crl
;URL = ftp://%1/ftp.organizacija.com/Ime_CA.crl
;URL = file://\\%1\certdata/Ime_CA.crl
Critical = true
[EnhancedKeyUsageExtension]
OID = 1.3.6.1.4.1.311.21.6 ; szOID_KP_KEY_RECOVERY_AGENT
OID = 1.3.6.1.4.1.311.10.3.9 ; szOID_ROOT_LIST_SIGNER
Critical = false
[basicconstraintsextension]
pathlength = 4
critical=false
[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=20
RenewalValidityPeriod=years
CRLPeriod = days
CRLPeriodUnits = 2
CRLDeltaPeriod = hours
CRLDeltaPeriodUnits = 4
```

Slika 7.1.1. Sadržaj Capolicy.inf fajla

Varijabla	Ime	Opis
%1	ServerDNSName	DNS ime CA računara (npr. organizacija.com)
%2	ServerHostName	NetBIOS ime CA računara (npr. Organizacija)
%3	CAName	Logičko ime CA
%4	CertificateName	Ime fajla sertifikata CA
%5	DomainDN	Ne koristi se od Windows Server 2003
%6	ConfigDN	LDAP putanja konfiguracije u šumi
%7	CATruncatedName	Skraćeni naziv CA
%8	CRLNameSuffix	Ekstenzija CRL liste
%9	DeltaCRLAllowed	Pokazuje da li su delta CRL liste podržane od CA
%10	CDPObjectClass	Pokazuje da je objekat CDP objekat u AD
%11	CAObjectClass	Pokazuje da je objekat CA sertifikat objekat u AD

Tabela 7.1.1. Definicije CDP i AIA varijabli

in-a MMC konzole i izmenama u prozoru Properties sertifikacionog tela;
- Direktnim upisivanjem u Registry bazu.
- Sve tri metode za posledicu imaju upis podataka u sekciju Registry baze:
- MyComputer\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\CertSvc\Configuration\ime_CA videti sliku 7.2.1. (sledeća strana)
- Neke podatke koje je neophodno promeniti su dati u tabeli 7.2.1 (sledeća strana):

Jedinice vremena mogu imati sledeće vrednosti: Years, Months, Weeks, Days i Hours

Nakon izmena tokom postinstalacione konfiguracije, potrebno je prvo restartovati Certificate Services, a zatim ponovo generisati CRL liste i publikovati ih ako su izmenjene putanje u CACertPublicationURLs i CRLPublicationURLs varijablama.

IMPLEMENTACIJA STANDALONE ROOT CA

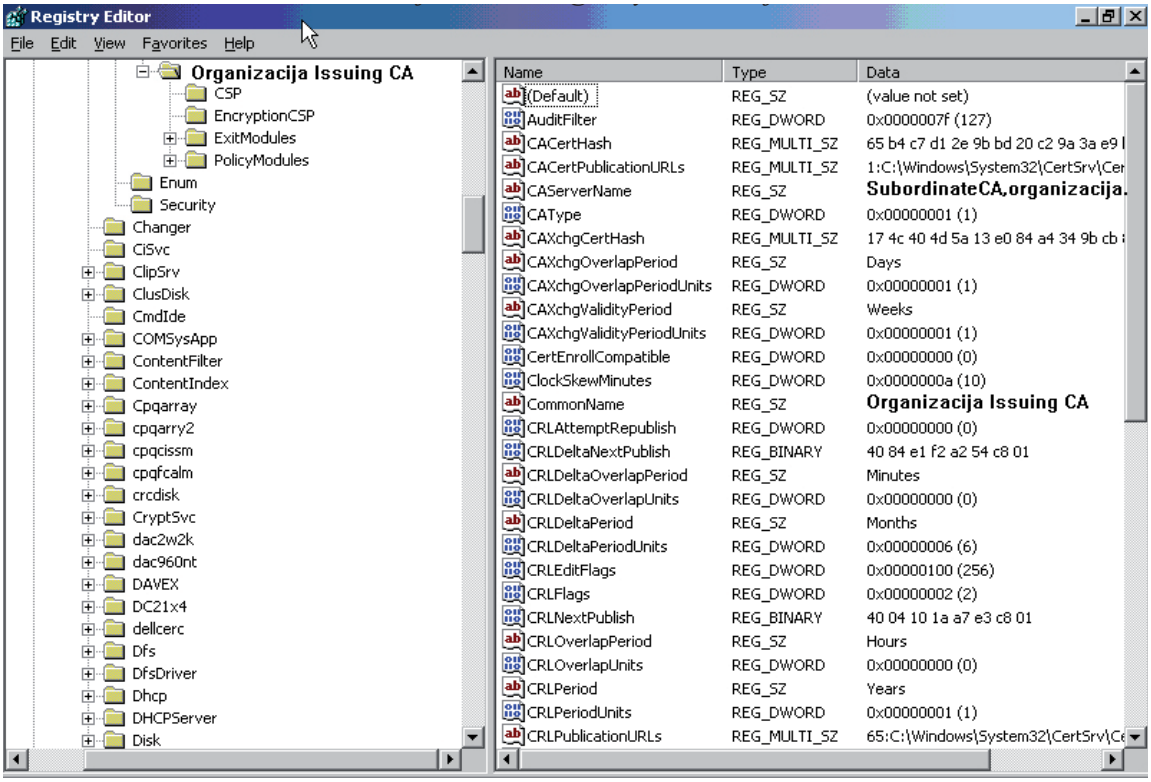
Nakon instaliranog operativnog sistema Microsoft Windows 2003 server Standard edition na server mašini, može se pokrenuti postupak instalacije Root CA kao Microsoft Standalone CA. Postupak instalacije se može podeliti u nekoliko koraka:

-preinstalaciona konfiguracija koja podrazumeva kreiranje capolicy.inf fajla;
-instalacija Windows Certificate services;
-publikovanje CRL listi;
-postinstalaciona konfiguracija.

Prvi korak u podešavanju konfiguracije preinstalacije Certificate services je kreiranje Capolicy.inf fajla (videti sliku 7.3.1. strana 72). Ovaj fajl sadrži podatke koji su neophodni za instalaciju CA i ponovno izdavanje CA sertifikata. Ovaj fajl smešta se u folder %windir%\capolicy.inf.

Jedini način da osiguramo da su CDP i AIA ekstenzije prazne je putem kreiranja Capolicy.inf fajla. Ovo je neophodno za ispravnu verifikaciju sertifikata jer Root CA nema nadređeno sertifikaciono telo, a samim tim ni CRL listu na kojoj bi se nalazilo. Ovim fajlom smo definisali sledeće vrednosti:

- Da CA ključeve treba obnoviti nakon 20 godina;
- Da je dužina ključa 4096;
- Da se CRL liste publikuju svakih 26 nedelja;
- Da se delta CRL liste ne publikuju.
- Osigurati da su korektni datum i vreme na Root CA serveru.
- Sledeći korak je instalacija Certificate servisa. To se radi na sledeći način :
- Iz Start menu-ja, kliknuti Settings, Control Panel i kliknuti Add or Remove Programs,
- U Add or Remove Programs prozoru, kliknuti Add/Remove Windows Components,
- U Windows Components Wizard, u Windows Components listi, kliknuti u selekcije Certificate Services check box a onda kliknuti Next,
- Ukoliko želite da koristite web komponente Certificate servisa (preporučeno) kliknuti takođe da se selektuje Internet Informa-



Slika 7.2.1. Parametri servisa Certification Services u Registry bazi

Naziv varijable	**Opis**
AuditFilter	Decimalni ekvivalent 7-bitnog binarnog broja koji predstavlja flegove koj pokazuju koje događaje treba upisivati u log fajl
CACertPublicationURLs	Lokacije na kojima će se publikovati sertifikati ovog CA
CRLPeriodUnits	Jedinica vremena za CRLPeriod
CRLPeriod	Učestalost publikovanja CRL lista
CRLDeltaPeriodUnits	Jedinica vremena za CRLDeltaPeriod
CRLDeltaPeriod	Učestalost publikovanja delta CRL lista
CRLPublicationURLs	Lokacije na kojima će se publikovati delta i CLR liste
ValidityPeriod	Period važnosti izdatih sertifikata
ValidityPeriodUnits	Jedinica vremena za ValidityPeriod

Tabela 7.2.1. Neke varijable iz Registry baze koje se odnose na CA

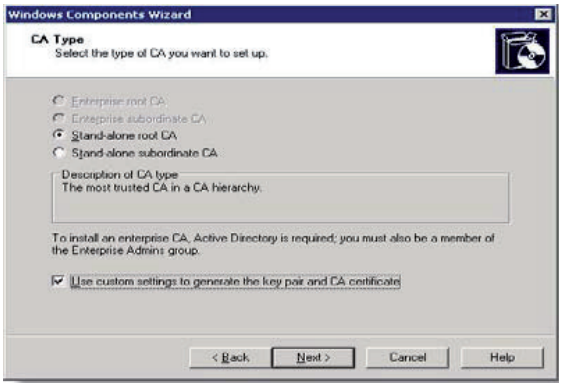
```
[Version]
Signature="$Windows NT$"

[certsrv_server]
renewalkeylength=4096
RenewalValidityPeriodUnits=20
RenewalValidityPeriod=years

CRLPeriod=weeks
CRLPeriodUnits=26
CRLDeltaPeriodUnits=0
CRLDeltaPeriod=days

[CRLDistributionPoint]
Empty=True

[AuthorityInformationAccess]
Empty=True
```

Slika 7.3.1. Root CA capolicy.inf fajl

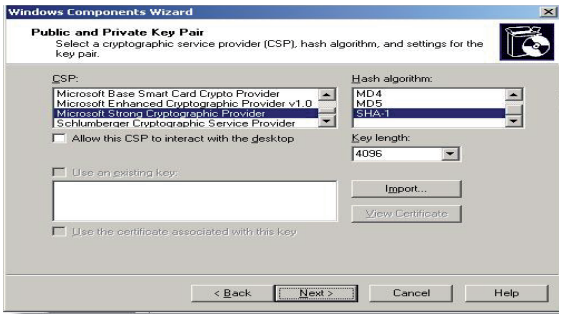
tion Services (IIS) (ili Internet Explorer Enhanced Security Configuration) check box, zatim Next i kada (i ukoliko) se pojavi upozoravajuća poruka kliknuti Ok. Web komponenta Certificate servisa omogućava:

- Konekciju na web stranu cilju enroll-ovanja (slanja zahteva) za izdavanje sertifikata,
- Download-ovanje CA sertifikata sa web stranice,
- Smeštanje zahteva za izdavanje sertifikata u fajl tako da se može procesirati od strane eksternog CA.

- Na CA Type stranici (slika 7.3.2.), kliknuti Stand-alone Root CA, kliknuti Use Custom Settings to Generate the Key Pair and CA Certificate check box, i onda kliknuti Next,
- Na Public and Private Key Pair stranici (slika 7.3.3), postaviti na primer sledeće opcije:
  CSP: Microsoft Strong Cryptographic Service Provider
  Allow the CSP to interact with the desktop Disabled
  Hash algorithm: SHA-1
  Key length: 4,096

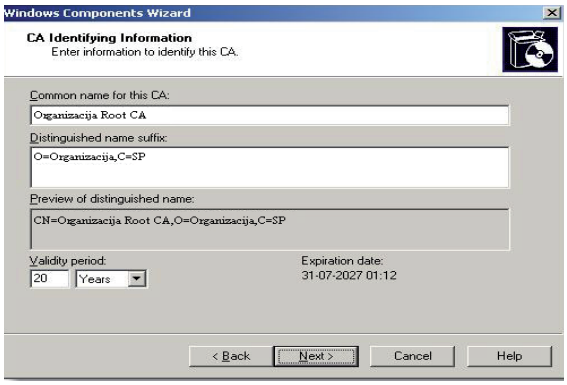


Slika 7.3.2. Biranje tipa CA



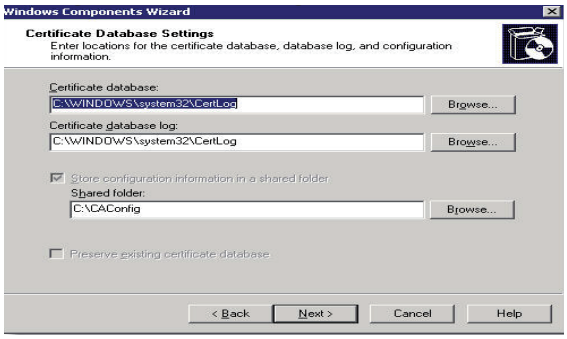
Slika 7.3.3. Način generisanja javnih i privatnih ključeva CA

- Na Public and Private Key Pair stranici, kliknuti Next,
- Na CA Identifying Information stranici (slika 7.3.4.), uneti sledeće informacije na primer:
  Common Name for this CA: Organizacija Root CA;
  Distinguished name suffix: O=Organizacija, C=SP;
  Validity Period: 20 Years;



Slika 7.3.4. Identifikacija CA

- Na CA Identifying Information stranici, kliknuti Next.
- Na Certificate Database Settings stranici (slika 7.3.5.), obezbediti sledeći settings i kliknuti Next:



Slika 7.3.5. Identifikacija CA

Certificate database: C:\WINDOWS\ system32\CertDB
Certificate database log: C:\WINDOWS\ system32\CertLog
CA configuration: C:\CAConfig

- U Microsoft Certificate Services dijalog boksu, kliknuti Yes u cilju kreiranja neophodnih direktorijuma.
- Na odgovarajućem dijalog boksu kliknuti OK da se stopira IIS server. Morate stopirati IIS da bi se instalirale web komponente. Ako IIS nije instaliran, ovaj dijalog boks se neće pojaviti.
- Installing Components dijalog boks se pojavljuje. Sačekajte da se instalacija završi i onda kliknite Finish.
- Na Completing the Windows Components Wizard stranici (slika 7.3.6), kliknuti Finish.
- Zatvoriti Add or Remove Programs dijalog boks.

Nakon nakon uspešne instalacije Certificate servisa ide sledeći korak. U pitanju je ručno publikovanje CRL liste. To se radi na sledeći način (slika 7.3.7.)

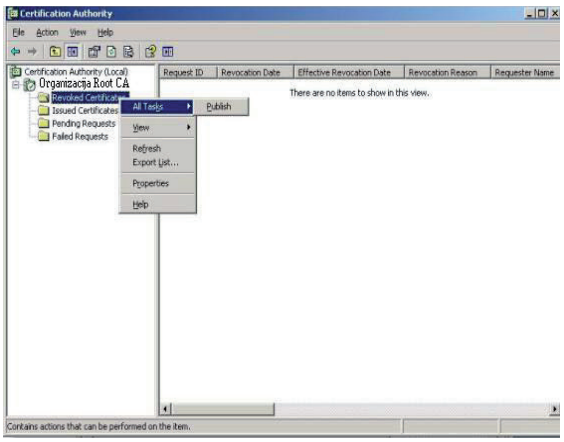
Sledeće, što treba uraditi, je da se iskopiraju svi fajlovi iz %windir%\system32\certsrv\certenroll*. crt and *.crl na USB ili disketu. Ovi fajlovi će nam biti potrebni za Subordinate CA. Takođe je potrebno ove fajlove iskopirati na HTTP lokaciju koju budemo odredili kao CDP u sledećem koraku.

Sledeći korak je postinstalaciona konfiguracija. Jedan od načina da se ona izvrši je ručnom izmenom u Registry bazi ili pravljenjem skripte koja

Slika 7.3.6. Potvrda o uspešnosti instalacije

koristi alat certutil i sleep iz Windows Resource kit paketa. Predloženi parametri postinstalacione skripte (slika 7.3.8. strana 74):

Ako je sve bilo uredu nakon izvršenja skripte svi fajlovi .crt i .crl su iskopirani na disketu. Kod preinstalacije i postinstalacije Root CA, ne treba da zbunjuje jedna važna činjenica:



Slika 7.3.7. Ručno publikovanje povučenih sertifikata preko CA konzole

CAPolicy.Inf fajl :
[CRLDistributionPoint]
Empty=True
[AuthorityInformationAccess]
Empty=True

Registry:

CRLPublicationURLs
65:%windir%\system32\CertSrv\ CertEnroll\%3%8%9.crl
79:ldap:/// CN=%7%8,CN=%2,CN=CDP,CN=Public Key Services,CN=Services,%6%10

```
::Deklarisanje konfiguracije
certutil -setreg CA\DSConfigDN CN=Configuration,DC=organizacija,DC=com

::Definisanje intervala publikovanja CRL
certutil -setreg CA\CRLPeriodUnits 26
certutil -setreg CA\CRLPeriod "Weeks"
certutil -setreg CA\CRLDeltaPeriodUnits 0
certutil -setreg CA\CRLDeltaPeriod "Days"

::Primenjivanje potrebnih CDP ekstenzija kroz URL
certutil -setreg CA\CRLPublicationURLs
"65:%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n6:http://ime_web_servera.org
anizacija.com/CertData/%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=
Public Key Services,CN=Services,%%6%%10"

:: Primenjivanje potrebnih AIA ekstenzija kroz URL
certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:http://ime_web_servera.org
anizacija.com/CertData/%%1_%%3%%4.crt\n3:ldap:///CN=%%7,CN=AIA,CN=Public Key
Services,CN=Services,%%6%%11"

::Omogućiti praćenja svih događaja vezanih za Organizacija Root CA
certutil -setreg CA\AuditFilter 127

::Setovanje perioda trajanja sertifikatima koji treba da se izdaju
certutil -setreg CA\ValidityPeriodUnits 10
certutil -setreg CA\ValidityPeriod "Years"

::Restartovanje Certificate Servisa
net stop certsvc & net start certsvc
sleep 5
certutil -crl

::Kopiranje Root CA sertifikata i CRL na floppy disk
Echo Ubaci Floppy disk u drajv A:
sleep 5
copy /y %windir%\system32\certsrv\certenroll\*.cr? a:\
```

Slika 7.3.8. Parametri postinstalacione skripte

6:http://ime_web_servera.organizacija.com/CertData/%3%8%9.crl
CACertPublicationURLs:
1:%windir%\system32\CertSrv\CertEnroll\%1_%3%4.crt
3:ldap:///CN=%7,CN=AIA,CN=Public Key Services,CN=Services,%6%11
2:http:// ime_web_servera.organizacija.com /CertData/%1_%3%4.crt

Root CA ne može da se nađe niti na jednoj CRL listi i zato su [CRLDistributionPoint] i [AuthorityInformationAccess] sekcije prazne. To nikako ne znači da CA neće imati svoj samopotpisani sertifikat i CRL listu koja će negde ručno biti publikovana. Svi sertifikati koje Root CA izda moraju znati koje su te lokacije da bi mogla biti obavljena verifikacija sertifikata. Root CA se ne može naći niti na jednoj CRL listi. Postavlja se pitanje kako onda sertifikat Root CA može biti opozvan? To je moguće opozivom svih sertifikata koje je Root CA izdao[49]. Root CA nije član domena niti je na bilo koji način umrežen sa ostalim računarima u hijerarhiji ali se podrazumeva postojanje Aktivnog direktorijuma i web servera.

Postinstalaciona skripta se snima sa ekstenzijom .cmd. Na primer, snimiti je kao post_conf_rootCA.cmd. Izvršiti pokretanje ove skripte. Nakon izvršenja skripte, offline Standalone Root CA je uspešno instaliran.

IMPLEMENTACIJA MS SUBORDINATE ENTERPRISE CA ORGANIZACIJE

U nastavku je opisan proces instalacije i implementacije MS Enterprise Subordinate CA Organizacije sistema (issuing CA u MS terminologiji) za interne korisnike kome digitalni sertifikat izdaje Root CA Organizacije. Osnovne karakteristike MS Enterprise CA sistema su date u narednim poglavljima. Podrazumeva se instalacija operativnog sistem Microsoft Windows Server 2003 Enterprise editon. Postupak instalacije se može podeliti u nekoliko koraka:

-Preinstalaciona konfiguracija koja podrazumeva instalaciju root sertifikata;
-Preinstalaciona konfiguracija koja podrazumeva kreiranje capolicy.inf fajla;
-Instalacija IIS (Internet Information services);
-Instalacija Windows Certificate services;
-Podnošenje zahteva Subordinate CA do Root CA;
-Instaliranje Enterprise Subordinate CA sertifikata;
-Postinstalaciona konfiguracija;
-Publikovanje CRL listi;

Prvi korak je priprema CAPolicy.inf fajla za potrebe Issuing CA. Neophodni parametri su prikazani na sledećoj slici 7.4.1.

Posle kreiranja ovog fajla potrebno ga je iskopirati u folder %windir%capolicy.inf [46]. Sledeći korak je instalacija IIS-a. Da bi bio omogućen Web Enrollment MS Certificate Servis mora se instalirati IIS server na Issuing CA serveru. Ne moraju da se instaliraju sve IIS komponente već samo one koje su zahtevane od strane Certificate Services Web Enrollment stranica. To se radi na sledeći način:

```
[Version]
Signature="$Windows NT$"
[PolicyStatementExtension]
Policies=OrganiyacijaCPS

[OrganizacijaCPS]
OID=1.3.6.1.4.1.311.509.3.1
NOTICE=Organizacija Certification Practice Statement
URL=http://ime_web_servera.organizacija.com/CPS/CP Statement.asp

[certsrv_server]
renewalkeylength=2048
RenewalValidityPeriodUnits=10
RenewalValidityPeriod=years

CRLPeriod=3
CRLPeriodUnits=days
CRLDeltaPeriodUnits=hours
CRLDeltaPeriod=12
```

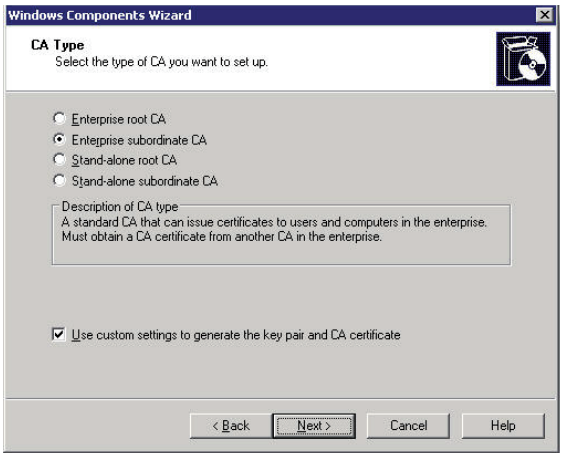
Slika 7.4.1. CAPolicy.inf fajl za potrebe Issuing CA

1. Iz Start menija, kliknuti Control Panel a zatim kliknuti Add or Remove Programs.
2. U Add or Remove Programs prozoru, kliknuti Add/Remove Windows Components.
3. U Windows Components Wizard-u, u Windows Components listi, kliknuti Aplication server i u okviru njega čekirati IIS i kliknuti next. Time će se instalirati IIS komponenta.
4. Kada su definisani i instalirani CAPolicy.inf fajl i IIS sledeći korak je instalacija MS Enterprise Certificate Services. Da bi se startovala instalacija MS Enterprise Certificate Services, potrebno je logovati se kao član Enterprise administratorske grupe. Dodatno, osigurati da je Enterprise

administratorska grupa član lokalne administratorske grupe na lokalnom nalogu baze podataka enterprise CA.

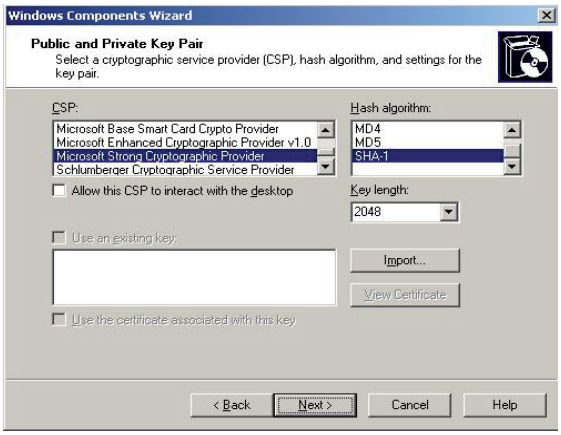
Ukoliko je prethodno ispunjeno, koristi se sledeća proceduru da se instalira Enterprise CA.

1. Obezbediti da je Enterprize CA (issuing CA server) član domena u forest-u.
2. Obezbediti da su datum i vreme korektno podešeni.
3. Iz Start menija, kliknuti Control Panel a zatim kliknuti Add or Remove Programs.
4. U Add or Remove Programs prozoru, kliknuti Add/Remove Windows Components.
2. U Windows Components Wizard-u, u Windows Components listi, kliknuti Certificate Services check box.
3. U Microsoft Certificate Services dijalog box-u, kliknuti Yes.
4. Na Windows Components stranici, kliknuti Next.
5. Na CA Type stranici (slika 7.4.2.), kliknuti Enterprise Subordinate CA, i omogućiti (enable) the Use Custom Settings To Generate the Key Pair and CA Certificate check box i kliknuti Next.
6. Na Public and Private Key Pair stranici (slika 7.4.3.), postaviti sledeće opcije:



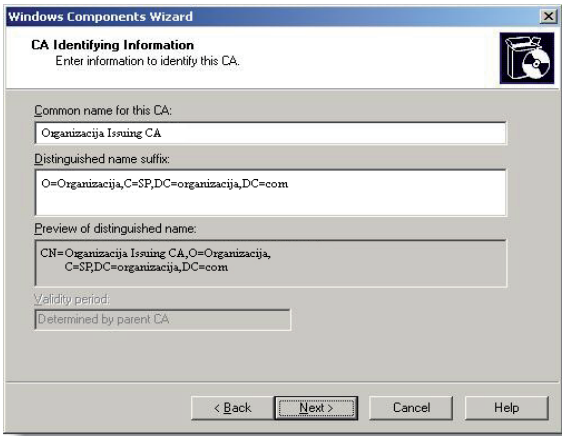
Slika 7.4.2. Odabir tipa CA

- CSP: Microsoft Strong Cryptographic Service Provider
- Allow the CSP to interact with the desktop: Disabled
- Hash algorithm: SHA-1
- Key length: 2,048



Slika 7.4.3. Način generisanja privatnog i javnog ključa

10. Na Public and Private Key Pair stranici, kliknuti Next.
11. Na CA Identifying Information stranici (slika 7.4.4.), uneti sledeće informacije:
- Common Name za ovaj CA: Organizacija Issuing CA
- Distinguished name suffix: O=Organizacija, C=SP
12. Na CA Identifying Information stranici,



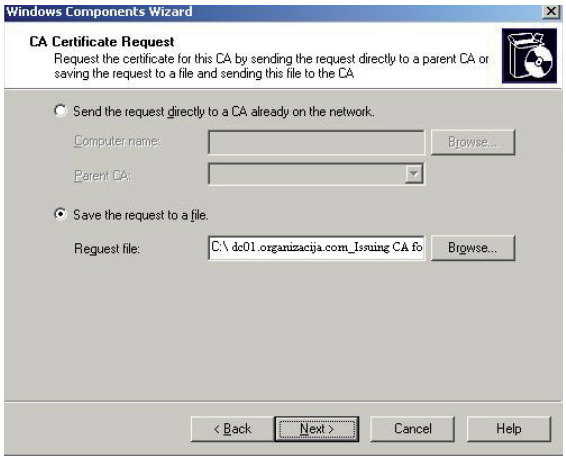
Slika 7.4.4. Identifikacione informacije CA

kliknuti Next.

13. Na Certificate Database Settings stranici, postaviti sledeću konfiguraciju i kliknuti Next.
- Certificate database: E:\CertDB
- Certificate database log: D:\CertLog

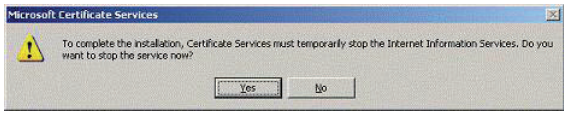
14. U okviru Microsoft Certificate Services dijalog box-a, kliknuti Yes da bi se kreirali neophodni direktorijumi.

15. Na CA Certificate Request stranici (slika 7.4.5.), kliknuti Save the Request to a File.
    U okviru Request File box-a, otkucati kompletnu putanju gde će biti smešten fajl zahteva (na primer A:\dc01.organizacija.com_IssuingCA for organizacija.req).



Slika 7.4.5. Issuing CA zahtev

    Ovim se formira zahtev za sertifikaciju Subordinate CA kod nadređenog sertifikacionog tela u hijerarhiji.
    Kliknuti Next.
16. U Microsoft Certificate Services dijalog box-u (slika 7.4.6.), kliknuti Yes da bi privremeno zaustavili IIS.
17. Ukoliko se zahteva, insertovati Windows Server 2003, Enterprise Edition, CD u CDROM drajv i izabrati \i386 folder. (Uvek koristiti Windows Server 2003,



Slika 7.4.6. IIS obaveštenje i privremenom stopiranju

    Enterprise Edition, za enterprise CA da bi omogućili korišćenje verzije 2 templejta za sertifikate, omogućili arhiviranje ključeva i sproveli separaciju rola.
    Ove opcije nisu raspoložive na Windows Server 2003, Standard Edition.
18. U okviru Microsoft Certificate Services message box-a, potvrditi da je CA instalacija nekompletna i kliknuti OK.
19. Ukoliko se pojavi Microsoft Certificate Services dijalog box, kliknuti Yes da bi se omogućile Active Server stranice.
20. Na Completing the Windows Components Wizard stranici, kliknuti Finish.
21. Zatvoriti Add or Remove Programs dijalog box.
22. Zatvoriti sve prozore.
23. Izvući disketu (ili neki drugi medijum) na kome se nalazi fajl sa zahtevom za sertifikat.

Pre nego što se nastavi mora se uraditi jedan veoma važan korak. Naime, na issuing CA telu mora se osigurati da postoji „trust“ za Root CA, kao i da je moguće download-ovati Root CA sertifikat i CRL, izdat od strane Root CA, za proveru povučenosti sertifikata. Ova operacija se može realizovati i manuelnim instaliranjem pomenutih sertifikata na sledeće lokacije [51]:

- Trusted root store i intermediate CA store na lokalnom računaru. Ova lokacija se zahteva ako ste u nemogućnosti da publikujete sertifikat na Active Directory ili na HTTP URL koji je referenciran u AIA i CDP ekstenzijama sertifikata izdatog od strane Root CA. Ova lokacija se takođe zahteva ukoliko je issuing CA u stvari standalone CA.
- Active Directory. Root CA sertifikat i CRL lista mogu biti publikovani na Active Directory. Publikacija na Active Directory omogućava automatski download sertifikata svim Windows 2000, Windows XP i Windows Server 2003 računarima koji su članovi „šume“ (forest-a).
- HTTP URL-ovi koji su referencirani u AIA i CDP ekstenzijama. Root CA sertifikati i CRL liste moraju manuelno da se publikuju na ove lokacije u cilju omogućavanja download-a CA sertifikata i CRL lista svim klijentima korišćenjem tih URL-ova za kreiranje lanca sertifikata i proveru statusa povučenosti. U svakom slučaju, morate osigurati da su CA sertifikati raspoloživi na URL putanjama koje su definisane u AIA ekstenziji sertifikata, kao i da su CRL-ovi raspoloživi na URL putanjama definisanim kao URL putanje u CDP ekstenziji sertifikata.

Preferirani metod publikovanja Root CA sertifikata i CRL liste u okruženju forest-a je da se oni publikuju na Active Directory. Sledeći put kada je Grupna Polisa primenjena na računar koji je član forest-a,

sertifikati će biti automatski dodati u Trusted root ili intermediate CA store lokalne mašine kroz autoenrollment mehanizam. Publikovanje Root CA sertifikata i CRL liste u Aktivni direktorijum i u lokalni trusted root vrši se na sledeći način [46] :

1. Prvo se iskopiraju *.crt i *.crl fajlovi koje smo generisali tokom instalacije Root CA sa diskete na lokaciju %systemroot%\system32\certsrv\certenroll folder našeg Issuing CA servera.

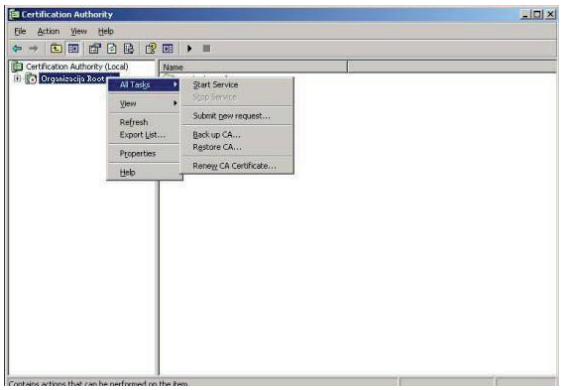
2. Zatim se pokrene skripta sa sledećim komandama u istom folderu našeg Issuing CA servera (slika 7.4.7.):

Skriptu pokreće korisnik koji je član Cert Publishers grupe u Aktivnom direktorijumu (naravno neko sa domenskim administratorskim pravima). Posle izvršenja skripte ide sledeći korak koji podrazumeva prebacivanje zahteva za izdavanjem sertifika sa Issuing CA do Root CA. Disketa mora biti preneta na Root CA računar da bi se podneo zahtev za izdavanjem sertifikata, izdao sertifikat, kao i da bi se on kopirao nazad na Enterprise issuing CA. U tom smislu, sledeći proces treba realizovati na Root CA serveru:

```
@echo off
for %%c in (*.crt) do certutil -addstore -f Root "%%c"
for %%c in (*.crl) do certutil -addstore -f Root "%%c"
for %%c in (*.crt) do certutil -dspublish -f "%%c" Rootca
for %%c in (*.crt) do certutil -dspublish -f "%%c" Subca
for %%c in (*.crl) do certutil -dspublish -f "%%c"
gpupdate /force
```

Slika 7.4.7. Publikovanje Root CA sertifikata i CRL liste pomoću skripte

1. Ubaciti disketu (ili neki drugi medijum) koji sadrži fajl zahteva za izdavanje sertifikata.
2. Iz Start menu-ja, kliknuti Administrative Tools a zatim kliknuti Certification Authority.
3. U konzolnom stablu, desnim klikom kliknuti na Organizacija Root CA, kliknuti na All Tasks i kliknuti Submit new request (slika 7.4.8.).
4. U Open Request File dijalog box-u, u okviru File Name box-a, otkucati kompletnu putanju do fajla sa zahtevom (primer A:\dc01.organizacija.com_Issuing CA for organizacija.req) i kliknuti Open.
5. U konzolnom stablu, ekspandovati Organizacije Root CA i kliknuti Pending Requests.
6. U details pane, desnim klikom kliknuti na zahtev za sertifikat, kliknuti na All Tasks i kliknuti na Export Binary Data.
7. U Export Binary Data dijalog box-u, u Columns That Contain Binary Data drop-down listu, selektovati Binary Request i kliknuti OK.
8. Pregledati detalje zahteva zbog sigurnosti:

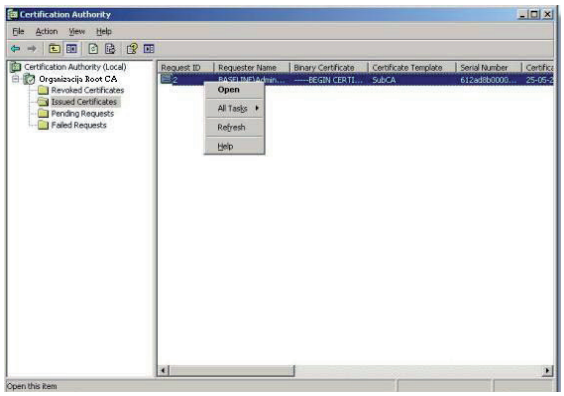


Slika 7.4.8. Podnošenje zahteva kod Root CA

- Verifikovati da je ime subjekta: Organizacija Issuing CA.
  Subject:
  CN=Organizacija Issuing CA
  O=Organizacija
  C=SP

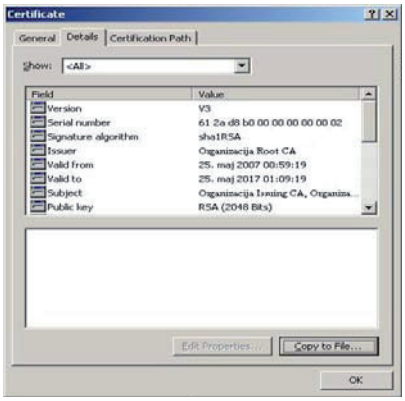
a. Osigurati da je dužina javnog ključa 2048 bita.
   Public Key Length: 2048 bita
b. Osigurati da vrednost ekstenzije u sertifikatu Basic Constraints indicira da je Subject Type=CA.
   Basic Constraints Subject type=CA
c. Verifikovati da potpis (samopotpisanog zahteva za izdavanjem sertifikata) odgovara javnom ključu. Potpis odgovara javnom ključu (Signature matches Public Key).

9. Zatvoriti Binary Request prozor.
10. U details pane, desnim klikom kliknuti na pending SubCA Certificate, kliknuti na All Tasks i kliknuti Issue.
11. U konzolnom stablu, kliknuti Issued Certificates (slika 7.4.9.).
12. U details pane, dvostruko kliknuti na issued Certificate.
13. U Certificate dijalog box-u, kliknuti Details tab.
14. U okviru Details tab-a, kliknuti Copy to File (slika 7.4.10.).



Slika 7.4.9. Izdat sertifikat od strane Root CA

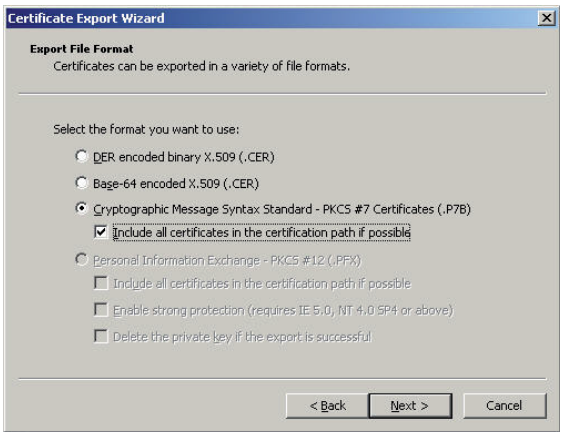
15. U Certificate Export Wizard-u, kliknuti Next.
16. Na Export File Format stranici (slika 7.4.11.), kliknuti Cryptographic



Slika 7.4.10. Detalji vezani za sertifikat

Message Syntax Standard—PKCS #7 Certificates (.P7B), omogućiti Include All Certificates in the Certification Path If Possible check box, i kliknuti Next.

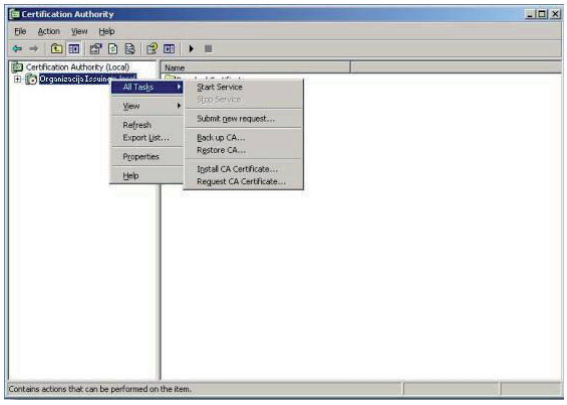
17. Na File to Export page, u File Name box-u, otkucati kompletnu putanju za čuvanje fajla (na primer A:\IssuingCA.p7b) i kliknuti Next.
18. Na Completing the Certificate Export Wizard stranici, kliknuti Finish.
19. U Certificate Export Wizard message box-u, kliknut OK.
20. U Certificate dijalog box-u, kliknuti OK.
21. Zatvoriti Certification Authority konzolu.
22. Izvući disketu (ili neki drugi medijum) koji sadrži eksportovan fajl.



Slika 7.4.11. Izbor formata za eksportovanje sertifikata

Nakon ovih operacija, Root CA se može ponovo isključiti. Kada se izdati sertifikat eksportuje na disketu, ili neki drugi medijum, može se koristiti sledeća procedura za završetak instalacije instaliranjem dobijenog sertifikata na Enterprise Issuing CA računar:

1. Ubaciti disketu (ili neki drugi medijum) koja sadrži PKCS#7 fajl u floppy drive.
2. Iz Start menu-ja, kliknuti Administrative Tools i kliknuti Certification Authority.
3. U konzolnom stablu, desnim klikom kliknuti na Organizacija Issuing CA, kliknuti na All Tasks i kliknuti Install CA Certificate kao na slici 7.4.12.
4. U Select File to Complete CA Installation dijalog box-u, u File Name box-u, otkucati kompletnu putanju do fajla sa sertifikatom (kao na primer A:\IssuingCA.p7b) a zatim kliknuti na Open.
5. U konzolnom stablu, desnim klikom



Slika 7.4.12. Instalacija sertifikata izdatog od strane Root CA

kliknuti na Organizacija Issuing CA, kliknuti na All Tasks i kliknuti Start Service.

Kada se instalira prethodno pomenuta CA hijerarhija, potrebno je osigurati da su URL-ovi AIA i CDP ekstenzija u sertifikatima konfigurisani korektno pre nego što se pokrene izdavanje sertifikata. Ako su pomenuti URL-ovi nepravilno konfigurisani, sistem za proveru lanca sertifikata rezultuje u greškama kada se pokušava da se download-uju CA sertifikati i CRL-ovi sa referenciranih URL-ova.

Sada je na redu postinstalaciona konfiguracija kojom na jedan od tri ranije pomenuta načina izvršimo izmene u registru. Jedan od načina koji smo već koristili pri kreiranju Root CA je putem skripte. Parametri ove skripte prikazani su na slici 7.4.13.

Posle pokretanja skripte pokrenuti konzolu Certification Authority i desnim klikom na Revoked Certificates selektovati All task/Publish i kliknuti na New CRL. Time je postupak instalacije CA gotov. Da bismo verifikovali da li je PKI ispravno konfigurisan koristi se alat PKI Health tool koji je sastavni deo paketa Windows Server 2003 Resource kit. Pokreće se komadom pkiview.msc. Ako je sve ispravno status kolone će davati vrednost OK. Issuing CA je sada spreman za izdavanje korisničkih sertifikata.

PREDLOG PRIMENE TEMPLEJTA ZA SERTIFIKATE U MS PKI SISTEMU ORGANIZACIJE

Za potrebe Windows logon sistema u organizaciji, pored MS Enterprise CA koje je domenski integrisano (sa Active Directory-jem), neophodno je na svakoj radnoj stanici u domenu, na kojoj se očekuje logovanje korisnika, instalirati čitač smart kartica i odgovarajući middleware za karticu koja će se koristiti za realizaciju Windows logon funkcije.

Microsoft sertifikaciono telo (CA) koje koristi enterprise politiku se odnosi na enterprise CA i bazira se na:

- Active Directory. Enterprise CA je integrisano sa Active Directory-jem i zavisno je od prisustva Active Directory-ja;
- Autentikacija. Enterprise CA koristi impersonaciju za autentikaciju onoga koji zahteva sertifikat i upoređuje klijentski token u odnosu na diskrecionu listu kontrole pristupa DACL (Discretionary Access Control List) koja je postavljena na templejt sertifikata i dati servis;
- Templejti sertifikata (Certificate Templates). Enterprise CA koriste templejte sertifikata
da izdaje sertifikate koji se koriste za po sebnu svrhu i kao sredstvo za definisanje enrollment politike za forest u datoj mreži.

U jednoj Windows mreži, instalacija bilo enterprise ili stand-alone CA od strane root domain administrator ili enterprise administrator kreira CA i CRL objekte na Active Directory-jumu. Kao posledica, u oba slučaja, većina procesa za kreiranje lanca sertifikata i provere statusa povučenosti sertifikata, izvršava se korišćenjem LDAP upita na Active Directory. Dodatno, instalacija Root CA (bilo stand-alone ili enterprise) od strane root domain administratora ili enterprise administratora automatski smešta root sertifikat na Active Directory, a svi Windows klijenti na enterprise mreži automatski dobijaju kopije datog CA sertifikata.

I enterprise i stand-alone CA mogu izdati sertifikate za svrhe, kao što su: digitalni potpisi, zaštićen e-mail korišćenjem S/MIME protokola, kao i bezbedna autentikacija na WEB servere korišćenjem SSL (Secure Sockets Layer) ili TLS (Transport Layer Security) protokola. Dodatno, enterprise CA može izdavati sertifikate za logovanje na Windows domen korišćenjem smart kartica (koje će biti izvedeno u narednom poglvalju). U okviru dodatne bezbednosti koju enterprise CA obezbeđuje kada autentikuje one koji zahtevaju sertifikate, svi Smart Card Logon sertifikati i Enrollment Agent sertifikati moraju biti izdati od strane enterprise CA. Ako se želi ta funkcionalnost u datoj organizaciji, mora se instalirati enterprise CA u okviru PKI hijerarhije.

Windows Enterprise CA ima najjednostavniji administrativni model koji radi sa sledeća dva Windows servisa u cilju minimizacije administrativnih aktivnosti u vezi izdavanja sertifikata uz obezbeđenje integrisane jedinstvene tačke upravljanja:

- Active Directory. Enterprise CA koristi Active Directory kao registracionu bazu podataka. Kreiranje korisnika na Windows domenu automatski registruje korisnika svakom enterprise CA u forest-u. Ovo omogućuje korisnicima koji imaju odgovarajuće dozvole da zahtevaju sertifikat od bilo kog enterprise CA. Enterprise CA koristi informacije publikovane na Active Directory za sadržaj subject polja u sertifikatu.

```
:: Deklarisanje konfiguracije
certutil -setreg CA\DSConfigDN CN=Configuration,DC=organizacija,DC=com

:: Definisanje intervala publikovanja CRL
certutil -setreg CA\CRLPeriodUnits 3
certutil -setreg CA\CRLPeriod "days"
certutil -setreg CA\CRLDeltaPeriodUnits 12
certutil -setreg CA\CRLDeltaPeriod "Hours"

:: Primenjivanje potrebnih CDP ekstenzija kroz URL
certutil -setreg CA\CRLPublicationURLs
"65:%WINDIR%\system32\CertSrv\CertEnroll\%%3%%8%%9.crl\n6:http://ime_web_servera.organizacija.
com/CertData/%%3%%8%%9.crl\n79:ldap:///CN=%%7%%8,CN=%%2,CN=CDP,CN=Public Key
Services,CN=Services,%%6%%10"

:: Primenjivanje potrebnih AIA ekstenzija kroz URL
certutil -setreg CA\CACertPublicationURLs
"1:%WINDIR%\system32\CertSrv\CertEnroll\%%1_%%3%%4.crt\n2:http://ime_web_servera.organizacija.
com/CertData/%%1_%%3%%4.crt\n3:ldap:///CN=%%7,CN=AIA,CN=Public Key
Services,CN=Services,%%6%%11"

:: Omogućiti praćenja svih događaja vezanih za Issuing CA
certutil -setreg CA\AuditFilter 127

:: Setovanje perioda trajanja sertifikatima koji treba da se izdaju
certutil -setreg CA\ValidityPeriodUnits 2
certutil -setreg CA\ValidityPeriod "Years"

:: Restartovanje Certificate Servisa
net stop certsvc & net start certsvc
sleep 5
certutil -crl
```

Slika 7.4.13. Postinstalaciona skripta za Issuing CA

- Windows bezbednosni model. Enterprise CA koristi Windows bezbednosne servise da identifikuje korisnika koji zahteva sertifikat i verifikuje korisnikova prava na bazi korisnikovog Windows grupnog članstva.

The next three subsections describe these features of enterprise CAs:

- Enterprise CA certificate templates
- Enterprise CA enrollment
- Enterprise CA security model

Enterprise CA certificate templates

Windows enterprise CA koristi templejte sertifikata da kontroliše sadržaje sertifikata koje izdaje. Ovi templejti definišu informacije koje idu u sertifikat, ekstenzije u sertifikatu, kao i izvorište informacija. Windows ima široki skup templejta, koji su publikovani u Active Directory i globalni su u odnosu na čitav Windows forest. Dva tipa templejta postoje:

- Templejti sa jednom svrhom (Single-purpose templates) generišu sertifikate koji mogu da se koriste samo za jednu aplikaciju. Na primer, Smart Card Logon templejt sertifikata je kreiran da se koristi za smart card logon funkciju.
- Višenamenski templejti (Multi-purpose templates) generišu sertifikate koji mogu biti korišćeni od strane više aplikacija, kao što su: SSL, S/MIME, i EFS[20]. Templejti postoje i za računare i za korisnike da bi se koristili od SSL servera ili Key Distribution cantara (KDC).

Enterprise CA enrollment

Here is how an enterprise CA lets users and computers request certificates:

Domenska autentikacija korisnika. Enterprise CA koristi domensku autentikaciju da identifikuje korisnika; tj. koristi koristi personalni Windows korisnički pristupni token kao dokaz identiteta.

Computer auto-enrollment. Enterprise CA koristi domensku autentikaciju da identifikuje računar; tj. koristi sistemski Windows računarski pristupni token kao dokaz identiteta. Computer auto-enrollment, koji se aktivira korišćenjem Windows servisa grupnih polisa, predstavlja mehanizam po kome računari automatski dobijaju sertifikate.

Enterprise CA Security Model

Enterprise CA bezbednosni model, kreiran da bude globalan u forest-u, je kontrolisan putem DACL-ova na Active Directory objektima. DACL kontrolišu sledeće:

- Ko u organizaciji može da se enroll-uje za sertifikat ?
- Za koje tipove sertifikata oni mogu da se enroll-uju ?
- Od kog Enterprise CA oni mogu da zahtevaju sertifikat ?

Enterprise CA imaju DACL koji definiše koji im korisnici mogu slati zahteve za izdavanjem sertifikata (enrollment requests). Templejti sertifikata u Active Directory imaju DACL koji definiše koji korisnici mogu da zahtevaju sertifikat korišćenjem templejta. Enterprise CA takođe imaju listu templejta koje može da koristi za procesiranje zahteva. Za korisnika koji hoće uspešno da zahteva sertifikat od strane Enterprise CA, tri kriterijuma moraju da budu zadovoljena:

- Korisničko grupno članstvo daje korisniku prava da koristi templejt koji je publikovan na Active Directory.
- Korisničko grupno članstvo daje korisniku pravo da koristi Enterprise CA.
- Enterprise CA je konfigurisan da izdaje sertifikate po templejtima koje je korisnik zahtevao.
- Enterprise CA takođe imaju DACL koji upravlja administracijom CA. Administrativni zadaci koji se izvršavaju na CA uključuju sledeće:
- Povlačenje sertifikata;
- Izmena default CRL publikacionog perioda;
- Izmena liste CRL distribucionih tačaka (CDP) koje su publikovane u sertifikatima od strane Enterprise CA. CDP predstavlja directory entry ili neki drugi distribucioni izvor za CRL;
- Izmena liste Authority Information Access (AIA) lokacija publikovanih u sertifikatima od strane Enterprise CA. AIA adrese su URL (uniform resource

20. The Encrypting File System. Predstavlja fajl sistem drajver koji ima za cilj šifrovanje fajl sistema, a raspoloživ je od Microsoft Windows 2000 OS. Tehnologija je transparentna, što znači da se šifrovanje podataka vrši nad postojećim NTFS fajl sistemom, u cilju zaštite poverljivih podataka od napadača koji imaju fizički pristup računaru.

locators) adrese koje jedinstveno identifikuju svaku lokaciju na Internetu a koje se nalaze u sertifikatima koje izdaje CA koje govore verifikatoru sertifikata sa kog mesta treba dobaviti CA sertifikat. AIA pristupni URL-ovi mogu biti HTTP, FTP, LDAP, ili FILE adrese;
- Uključivanje ili isključivanje publikacije sertifikata na Active Directory-jumu;
- Obnavljanje CA;
- Izmena DACL na Enterprise CA;
- Izmena liste templejta sertifikata koji se koriste od strane Enterprise CA;

Enterprise CA može publikovati korisničke sertifikate, CA sertifikate i CRL liste na Active Directory-ju. Korisnički sertifikati se publikuju u okviru User objekta u domain data directory particiji. Korisnički sertifikati su takođe replicirani na Windows globalni katalog da bi obezbedili pristup u celom forest-u. CA sertifikati su publikovani na CertificationAuthority objektu a CRL liste su publikovane u okviru CRLDistributionPoint objekta u Active Directory-jumu. Da bi se osiguralo kreiranje lanca sertifikata u okviru datog CA i raspoloživost informacija o statusu povučenosti bez obzira na domensku strukturu, ovi objekti su publikovani u configuration data directory particiji, čiji je sadržaj repliciran u celom forest-u. CDP i AIA pokazivači u sertifikatima su konstruisani tako da rade nezavisno od domena čiji domen kontroler pripada forest-u.

U Windows mreži, tri mehanizma postoje, po kojima se CA sertifikati distribuiraju do Windows računara:

- Enterprise root certificate store. Enterprise root Certificate store je lociran na Active Directory-jumu. Kada domen administrator instalira Windows root CA (bilo enterprise ili stand-alone) u forest, instalacioni process takođe ažurira enterprise root Certificate store sa novim sertifikatom. Kada se računar u organizaciji startuje (boots up), sadržaj enterprise root Certificate store se download-uje i posledično osvežava svakih 8 sati. Ovaj jednostavni mehanizam distribuira root sertifikate do svih računara u forest-u;
- Windows grupna polisa. Može se koristiti obeležja Windows grupne polise za distribuciju bilo kog CA sertifikata grupama računara u okviru forest-a. Ako eksterni CA ne treba da bude poverljiv za čitavu organizaciju već samo za jedan skup korisnika ili računara u forest-u, može se koristiti grupna polisa da se primeni željeno setovanje na datu grupu uključenih računara;
- Distribucija sertifikata klijentima. Kada se klijent enroll-uje za dobijanje sertifikata od Windows CA korišćenjem Web klijenta, kompletan lanac sertifikata (uključujući root sertifikat) se download-uje klijentu kao odgovor od CA na zahtev za dobijanje sertifikata.

Da bi se iskoristile sve prednosti MS Enterprise CA koje je uspostavljeno za potrebe internih korisnika u jednoj organizaciji, neophodno je dobro osmisliti i projektovati koji će se sve templejti koristiti u okviru datog PKI sistema. Kao jedan od templejta koji obezbeđuje dosta korisnih funkcionalnosti, predlaže se korišćenje Smart Card User templejta za izdavanje sertifikata internim korisnicima u organizaciji u MS Enterprise CA koji ima sledeće karakteristike (neke od njih su zajedničke za sve templejte koji se koriste u okviru MS Enterprise CA):

- Ekstenzija Key Usage sadrži sledeće vrednosti: „Digital Signature“ i „Key Encipherement“;
- Ekstenzija SMIME Capabilities je uključene u sertifikat;
- Uključena je ekstenzija Certificate Template Name sa vrednošću „Smartcard User“;
- U sertifikat su uključene ekstenzije AIA i CDP ekstenzije;
- U sertifikat je uključena ekstenzija Enhanced Key Usage sa sledećim vrednostima:
  - Secure Email (1.3.6.1.5.5.7.3.4)
  - Client Authentication (1.3.6.1.5.5.7.3.2)
  - Smart Card Logon (1.3.6.1.4.1.311.20.2.2)
- U ekstenziji Subject Alternative Name upisano je sledeće: „Principal Name = domenski username“ i „RFC822 Name = email adresa“.

Interni korisnici date organizacije koji imaju smart karticu na kojoj je generisan asimetrični par ključeva (privatni i javni), pri čemu privatni ključ nikada ne može da napusti karticu, koji na svojim radnim stanicama imaju instalirane čitače smart kartica i odgovarajući middleware za datu smart karticu, kao i koji imaju izdate sertifikate od strane MS Enterprise CA u datoj organizaciji i to

po Smart Card User templejtu, mogu koristiti, bez potrebe za bilo kakvim dodatnim instaliranjem programa, standardne funkcionalnosti ukratko opisane u nastavku.

Kvalitet ovog rešenja je što se podizanjem MS Enterprise CA i izdavanjem sertifikata po Smart Card User templejtu na smart karticama za interne korisnike omogućava jednostavno korišćenje bezbednosnih mehanizama primenom standardnih programa i funkcionalnosti, kao što su:

- Windows logon standardna Windows (2000 i 2003) funkcionalnost;
- Zaštićeni e-mail sistem primenom standardnih e-mail klijenata kao što su: MS Outlook i MS Outlook Express;
- Zaštita na transportnom nivou primenom standardnog SSL protokola i klijentske autentikacije.

KLIJENTSKA SSL AUTENTIKACIJA

Imajući sertifikat sa gore navedenim karakteristikama, a posebno sa navedenom vrednošću (Client Authentication) u Enhanced Key Usage ekstenziji, interni korisnici mogu koristiti svoj sertifikat i privatni ključ na smart kartici za realizaciju klijentskog autentikacionog protokola u okviru SSL protokola zaštite. Pri tome, korisnik se može autentikovati WEB serveru ili nekom web servisu a za autentikaciju može koristiti ili sam sertifikat ili thumbprint svog sertifikata. U tom smislu, u slučaju klijentske autentikacije na neki web servis sa kojim komunikacija podrazumeva prethodno uspostavljenu SSL sesiju sa uključenom klijentskom autentikacijom, digitalni sertifikat korisnika treba da bude iskopiran na direktorijum gde se nalazi softver koji služi za eventualni poziv web servisa, ili se autentikacija sertifikata korisnika koji može da pristupi vrši na bazi thumprint-a samog korisničkog sertifikata. Šta će se koristiti za autentikaciju zavisi od konfiguracionog fajla u kome se nalazi zapisan način pozivanja datog web servisa.

ZAŠTIĆENI E-MAIL SERVIS

Primenom procedura i sistema definisanih u ovom dokumentu, kao i primenom smart kartica i gore navedenog tipa sertifikata, interni korisnik je u mogućnosti da, bez ikakvog dodatnog instaliranja softvera, koristi standardne S/MIME kompatibilne email klijente kao što su MS Outlok i MS Outlook Express za razmenu digitalno potpisanih i šifrovanih mail poruka. Zaštićeni email servis se omogućava odgovarajućim parametrima koji su uključeni u sertifikat i to:

- Uključenje ekstenzija: AIA, CDP i SMIME Capabilities;
- Uključenje email adrese u Subject strukturu korisnika, i to u polje pod oznakom „E“;
- Uključenje email adrese u ekstenziju Subject Alternative Name (ovo je alterantiva prethodnoj tački);
- Uključenje vrednosti „Secure Email“ u Enhanced Key Usage ekstenziju.

Pored parametara uključenih u sam sertifikat, neophodno je podesiti mail nalog na datom računaru da odgovara e-mail adresi koja je postavljena u E polje Subject strukture, kao i u Subject Alternative Name. Pored toga, u mail klijentima je neophodno podesiti bezbednosne parametre i omogućiti funkcije digitalnog potpisivanja i šifrovanja (posebne ikone za ove funkcije u okviru mail klijenata) putem tehnologije digitalne envelope. Uz to je neophodno izabrati sertifikat korisnika iz Personal Store-a date radne stanice za potrebe digitalnog potpisivanja i raspakovanja digitalne envelope. Potrebno je izabrati sertifikat koji je izdat od strane Enterprise CA i koji se automatski ili manuelno instalira na radnu stanicu sa smart kartice.

Nakon ovih podešavanja, interni korisnici mogu razmenjivati digitalno potpisane poruke između sebe. Po dobijanju prve digitalno potpisane poruke, sertifikat potpisnika se automatski dodaje u vaše kontakte. U tom smislu, nakon prve razmene digitalno potpisanih poruka, moguće je da se naredne poruke i šifruju korišćenjem javnog ključa namenjenog primaoca koji se nalazi u sertifikatu, u odgovarajućem kontaktu za tog primaoca.

Moguće je izvršiti šifrovanje i prilikom slanja prve poruke ukoliko je mail server integrisan sa Active Directory-jem (na primer ukoliko se koristi MS Exchange server). U tom slučaju je potrebno javni ključ namenjenog primaoca potražiti na Active Directory-ju i izvršiti traženo šifrovanje.

WINDOWS LOGON

Kao što je već rečeno, jedna od ključnih, uglavnom unikatnih, karakteristika MS Enterprise CA je mogućnost izdavanja sertifikata za potrebe bezbednog logovanja na domen putem smart kartica. Za realizaciju ove funkcije je neophodno:

- Uključiti ekstenzije AIA i CDP u sertifikate;

- Ubaciti vrednost „Smart Card Logon“ u Enhanced Key Usage ekstenziju;
- Ubaciti domenski username datog korisnika u „Principal Name (PN)“ u okviru Subject Alternative Name ekstenzije.

Nakon ovoga, korisnik se loguje na mrežu korišćenjem svoje smart kartice i ukucavanjem PIN koda kojim se omogućava pristup smart kartici.

ZAKLJUČAK

U ovom radu je opisan projekat uspostave internog PKI sistema Organizacije na bazi MS Certificate Services. Predlog je, da se ovaj sistem bazira na hijerarhijskoj PKI infrastrukturi u kojoj bi postojao jedan offline Root CA Organizacije i jedan online MS Enterprise CA (Organizacije Subordinate Enterprise CA) za izdavanje sertifikata internim korisnicima računarske mreže Organizacije. Takođe poželjno bi bilo uspostaviti takav sistem da se sertifikati internim korisnicima Organizacije izdaju na smart karticama i da omogućavaju sledeće funkcije:

- Zaštićeni Windows logon na domen Organizacije;
- Zaštićeni e-mail servis putem nekog od standardnih e-mail klijenata, MS Outlook i MS Outlook Express;
- Zaštitu na transportnom nivou putem standardnog SSL protokola i klijentske autentikacije na bazi smart kartica.

Realizacijom ovog predloga, detaljno analiziranog u okviru izloženog rada, ostvaruje se interni PKI sistem koji omogućuje jaku dvo-faktorsku autentikaciju internih korisnika (Windows logon), kao i korišćenje zaštićene interne komunikacije primenom bezbednosne nadgradnje standardnih programskih paketa (S/MIME kod mail klijenata i SSL kod WEB aplikacija). U tom smislu, za realizaciju ovog projekta je potrebno nabaviti smart kartice, odgovarajući middleware za date smart kartice, kao i odgovarajuće čitače smart kartica za interne korisnike. Dodatni softverski paketi i programi nisu potrebni.

PRILOG 1: KVALIFIKOVANI ELEKTRONSKI POTPIS

Elektronski potpis predstavlja tehnologiju koja u sistemima elektronskog poslovanja omogućava:

- provera autentičnosti potpisnika,
- zaštita integriteta podataka koji se prenose i
- neporecivost elektronskog potpisivanja date poruke ili dokumenta.

Dakle, analogno svojeručnom potpisu u standardnom poslovanju koristi se elektronski potpis u elektronskom poslovanju. Štaviše, elektronski potpis ima i dodatnu osobinu da štiti integritet elektronsko potpisane poruke što svojeručni potpis ne obezbeđuje. Što se tiče pravnih aspekata elektronskog potpisa, Direktiva Evropske Unije 1999/93/ES o elektronskim potpisima (usvojena 13. decembra 1999. a formalno stupila na snagu 19.01.2000. godine) predstavlja pravno utemeljenje elektronskog potpisa i na osnovu nje su doneti Zakoni o elektronskom potpisu u svim zemljama Evropske Unije, kao i u većini ostalih zemalja Evrope.

U nastavku teksta ćemo se posvetiti temi šta je to elektronski potpis, čemu služi i koji uslovi treba da se ispune da bi elektronski potpis bio ekvivalentan svojeručnom potpisu.

ZAKONSKE ODREDBE

U Zakonu o elektronskom potpisu navedene su sledeće definicije:

- "Elektronski potpis" – skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
- "Kvalifikovani elektronski potpis" - elektronski potpis kojim se pouzdano garantuje identitet potpisnika, integritet elektronskih dokumenata, i onemogućava naknadno poricanje odgovornosti za njihov sadržaj, i koji ispunjava uslove utvrđene Zakonom o elektronskom potpisu;

Takođe, prema tekstu Zakona, kvalifikovani elektronski potpis, mora da zadovolji sledeće uslove:

- isključivo je povezan sa potpisnikom;
- nedvosmisleno identifikuje potpisnika;
- nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika;
- direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka;
- formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa (SSCD);
- proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Kvalifikovani elektronski potpis, koji zadovoljava prethodno navedene uslove, u odnosu na podatke u elektronskom obliku ima isto pravno dejstvo i dokaznu snagu kao i svojeručni potpis, odnosno svojeručni potpis i pečat, u odnosu na podatke u papirnom obliku.

Primenom kvalifikovanog elektronskog potpisa pouzdano se realizuju sledeće funkcije:

- Provera autentičnosti potpisnika,
- Zaštita integriteta sadržaja poruke koja je potpisana,
- Neporecivost potpisivanja poruke.

Kao što je i navedeno, jedan od uslova da se formira kvalifikovani elektronski potpis je da se koriste sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD – Secure Signature Creation Device), koja moraju da obezbede:

- da se podaci za formiranje kvalifikovanog elektronskog potpisa mogu pojaviti samo jednom i da je obezbeđena njihova poverljivost;
- da se iz podataka za proveru kvalifikovanog elektronskog potpisa, ne mogu u razumno vreme i trenutno dostupnim sredstvima, dobiti podaci za formiranje kvalifikovanog elektronskog potpisa;
- da kvalifikovani elektronski potpis bude zaštićen od falsifikovanja, upotrebom trenutno dostupne tehnologije;
- da podaci za formiranje kvalifikovanog elektronskog potpisa budu pouzdano zaštićeni od neovlašćenog korišćenja.

Sredstva za formiranje kvalifikovanog elektronskog potpisa, prilikom formiranja potpisa, ne smeju promeniti podatke koji se potpisuju ili onemogućiti potpisniku uvid u te podatke pre procesa formiranja kvalifikovanog elektronskog potpisa. Sredstva za formiranje kvalifikovanog elektronskog potpisa moraju dodatno da ispune i sledeće uslove, i to:

- da se podaci za formiranje kvalifikovanog elektronskog potpisa generišu u samom sredstvu za formiranje kvalifikovanog elektronskog potpisa i da ga nikad ne napuštaju,
- da se kvalifikovani elektronski potpis formira u samom sredstvu za formiranje kvalifikovanog elektronskog potpisa,
- da se obezbedi korišćenje sredstva za formiranje kvalifikovanog elektronskog potpisa isključivo od strane potpisnika uz prethodno realizovanu pouzdanu proceduru autentikacije,
- sredstvo mora biti takvo da je potpisnik u mogućnosti da ga koristi u različitim aplikacijama i informatičko - tehnološkim okruženjima.

Pored sredstava za formiranje kvalifikovanog elektronskog potpisa, za konkretno kreiranje kvalifikovanog potpisa neophodno je primeniti i bezbednu aplikaciju za formiranje potpisa (SSCA – Secure Signature Creation Application) koja se koristi zajedno i neodvojivo sa SSCD. Ova aplikacija u sebi sadrži i bezbednu aplikaciju za verifikaciju potpisa (SSVA – Secure Signature Verification Application). Ove aplikacije, koje se još nazivaju i „komponente aplikacije potpisa“, moraju da zadovolje sledeće zahteve:

- dodela podataka procesu formiranja ili verifikacije kvalifikovanog elektronskog potpisa,
- verifikacija kvalifikovanog elektronskog potpisa i validacija kvalifikovanih elektronskih sertifikata, kao i prikaz rezultata.
- Tehničke komponente sertifikacionih tela treba da budu softverski i hardverski proizvodi koji:
- kreiraju podatke za formiranje kvalifikovanog elektronskog potpisa i prenose ih u SSCD ili ih generišu direktno na SSCD,
- drže raspoloživim kvalifikovane sertifikate za verifikaciju i, ako je potrebno, za dobavljanje od strane zainteresovanih strana.

U smislu gore navedenog, proizvodi za kvalifikovane elektronske potpise predstavljaju:

- sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD),
- bezbedna aplikacija za formiranje i verifikaciju kvalifikovanog elektronskog potpisa (SSCA i SSVA),
- tehničke komponente sertifikacionih tela.
- Najpopularnije aplikacije u kojima se koristi elektronski potpis su:
- Zaštićeni E-mail servis,
- Zaštićene WEB transakcije,
- Bezbedna plaćanja putem Interneta,
- Formiranje VPN (IPSec) mreža,
- Bezbedno upravljanje dokumentacijom, itd.

Najznačajnija polja primene elektronskog potpisa su:

- Elektronsko poslovanje (e-business),
- Elektronska trgovina (e-commerce),
- Elektronsko bankarstvo,
- Elektronska uprava (e-govemment),
- Elektronsko zdravstvo (e-healthcare),
- Platni sistemi na bazi čip kartica (EMV), itd.

Dakle, za primenu kvalifikovanog elektronskog potpisa neophodno je istovremeno posedovati dva osnovna elementa:

- sredstvo za formiranje kvalifikovanog elektronskog potpisa (SSCD) i
- kvalifikovani elektronski sertifikat potpisnika.

Ako bilo koji od ovih elemenata nedostaje, potpis ne zadovoljava uslove da bude kvalifikovani već je to "samo" elektronski potpis. Drugim rečima, iako elektronski potpis može prema Zakonu biti bilo šta što je "logički povezano sa elektronskim dokumentom i što služi za identifikaciju potpisnika" (na primer skenirani svojeručni potpis na kraju dokumenta i sl.), elektronskim potpisom se smatra i potpis koji je izvršen sredstvom za formiranje kvalifikovanog elektronskog potpisa a potpisnik nema kvalifikovani sertifikat. Takođe, potpisnik koji ima kvalifikovani sertifikat a potpisivanje ne vrši primenom sredstva za formiranje kvalifikovanog potpisa ne može da formira kvalifikovani elektronski potpis koji je pravno izjednačen sa svojeručnim potpisom.

Na primer, u našoj zemlji je od 06.01.2003. uvedeno elektronsko bankarstvo između pravnih liCA i skoro svih naših banaka u kome se koriste smart kartice za elektronsko potpisivanje finansijskih transakcija. Ti potpisi predstavljaju "samo" elektronske potpise jer korisnici nemaju kvalifikovane sertifikate a smart kartice koje se koriste nisu verifikovane kao sredstva za formiranje kvalifikovanog potpisa u našoj zemlji. Po svemu sudeći, na osnovu svetske prakse, u domenu elektronskog bankarstva neće ni biti obavezno da se koristi kvalifikovani elektronski potpis jer se to smatra zatvorenom grupom korisnika (gde postoji eksplicitni ugovor između komitenta i banke).

Na osnovu svetskih i evropskih analiza, prava i najšira primena kvalifikovanog elektronskog potpisa se očekuje u domenu elektronske uprave kada će građani elektronski poslovati sa javnom upravom, tj. slati elektronske zahteve javnoj upravi (npr. zahtev za izdavanje elektronskog izvoda iz matične knjige, elektronska prijava poreza, itd.). Ovi zahtevi moraju biti potpisani kvalifikovanim elektronskim potpisom građana. U tom smislu, tekući projekat uvođenja ličnih karata u Srbiji kao elektronskih identifikacionih dokumenata u obliku smart kartice predstavlja pravu podršku za pomenuti sistem. Naime, očekuje se da će pomenuta elektronska lična karta, odmah po uvođenju, biti verifikovana kao sredstvo za formiranje kvalifikovanog elektronskog potpisa.

TEHNOLOŠKI ASPEKTI

Kriptografski algoritmi koji se primenjuju u sistemima zaštite Internet/Intranet računarskih mreža dele se u dve velike grupe:

- Simetrični kriptografski algoritmi,
- Asimetrični kriptografski algoritmi.

Podela je izvedena na osnovu karakteristika kriptografskih ključeva za šifrovanje i dešifrovanje. Naime, kod simetričnih kriptografskih sistema ključevi za šifrovanje i dešifrovanje su identični (tajni ključ - secret key) dok su kod asimetričnih sistema ključevi za šifrovanje i dešifrovanje različiti (javni i privatni ključ - public and private key). Primenom simetričnih kriptografskih algoritama se, kao i u tradicionalnim sistemima zaštite, ostvaruje funkcija zaštite tajnosti u savremenim informacionim sistemima. Sa druge strane, primenom asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa ostvaruju se već pomenute, bezbednosne funkcije u savremenim računarskim mrežama:

- Bezbedna provera autentičnosti strane koja je poslala digitalno potpisanu poruku,
- Zaštita integriteta podataka u poruci koja je poslata,
- Neporecivost potpisnika za sadržaj date poruke.

Kvalifikovani elektronski potpis se na ovom stepenu tehnološkog razvoja formira na bazi primene asimetričnih kriptografskih algoritama i tehnologije digitalnog potpisa. Kvalifikovani elektronski potpis se formira u skladu sa preporukom PKCS#l (Public Keu Cryptographic Standard), a dužina modulusa u asimetričnom kriptografskom algoritmu mora biti minimalno 1024 bita. PKCS#l standard opisuje metode šifrovanja i dešifrovanja podataka korišćenjem RSA asimetričnog algoritma i najčešće se koristi za konstrukciju digitalnog koverta i digitalnog potpisa.

U slučaju digitalnog koverta, sadržaj poruke se prvo šifruje određenim simetričnim algoritmom (kao što su DES, 3-DES, RC2, IDEA, AES, ili neki namenski privatni algoritmi). Zatim se tajni ključ primenjenog simetričnog algoritma koji je upotrebljen za šifrovanje date poruke šifruje RSA algoritmom upotrebom asimetričnog javnog ključa korisnika kome je data poruka namenjena (RSA public key operacija). Tako šifrovan sadržaj

poruke i šifrovani simetrični tajni ključ kojim je ta poruka šifrovana zajedno predstavljaju digitalni koverat. Primenom tehnologije digitalnog koverta postiže se da samo namenjeni primalac poruke može dešifrovati poslatu poruku jer samo on poseduje svoj asimetrični privatni ključ na bazi koga se, uz primenu asimetričnog kriptografskog algoritma, prvo dešifruje simetrični tajni ključ na osnovu koga se, uz primenu sada simetričnog kriptografskog algoritma, dešifruje data poruka.

U slučaju digitalnog potpisa, sadržaj koji treba da se potpiše prvo ce redukuje u otisak poruke (message digest) primenom nekog od metoda za kreiranje otiska poruke, message-digest algoritma (kao što su na primer MD5, SHA-l, RIPEMD-160, SHA-256, SHA-512, ili neki drugi algoritmi), a zatim se dobijeni otisak poruke šifruje primenom, na primer, RSA algoritma koristeći privatni ključ potpisnika poruke (RSA private key operacija). Šifrovani otisak poruke predstavlja digitalni potpis date poruke i postaje njen pridruženi deo. Kada ovakva poruka stigne do primaoca kome je namenjena izvršava se postupak verifikacije digitalnog potpisa. Ovaj postupak se sastoji od dešifrovanja otiska dobijene poruke primenom RSA algoritma uz upotrebu javnog ključa pošiljaoca (potpisnika) poruke. Po dešifrovanju digitalnog potpisa primalac poruke izvrši isti message digest postupak nad dobijenom porukom. Ako je dobijeni otisak poruke identičan sa dešifrovanom vrednošću otiska, verifikacija je uspela, u protivnom verifikacija je negativna i poruka se odbacuje kao nevalidna.

Kvalifikovani elektronski potpis se formira primenom jednog od standardizovanih asimetričnih kriptografskih algoritama iz sledeće grupe, i to:

- RSA (Rivest Shamir Adleman),
- DSA (Digital Signature Algorithm) ili
- ECDSA (Elliptic Curve Digital Signature Algorithm).

Pri formiranju kvalifikovanog elektronskog potpisa primenjuju se i hash funkcije za dobijanje otisaka poruke fiksne veličine (128 ili 160 bita). Hash funkcije realizuju se primenom standardizovanih hash algoritama iz sledeće grupe, i to:

- MD5 (Message Digest) - rezultuje u hash vrednostima veličine 128 bita ili
- SHA-1 (Secure Hash Algorithm) - rezultuje u hash vrednostima veličine 160 bita.

Pri tome treba istaći da su se u poslednje vreme pojavili teorijski naučni radovi koji ukazuju na veoma velike slabosti trenutno korišćenih hash funkcija, kao što su MD5 i SHA-1. U tom smislu, očekuje se da će se uskoro standardizovati nova hash funkcija koja će se koristiti u PKI sistemima i koja neće imati uočene slabosti kao aktuelno korišćenje hash funkcije (kandidati su RIPEMD-160, SHA-256, SHA-512, itd.).

Kvalifikovani elektronski potpis formira se u skladu sa skupom tehničkih pravila za formiranje kvalifikovanog elektronskog potpisa koji moraju poštovati kako potpisnik tako i korisnik koji proverava kvalifikovani elektronski potpis. Pravila propisuje Nadležni organ (kao Root CA), u skladu sa Zakonom o elektronskom potpisu i odgovarajućim podzakonskim aktima. Pravila su unapred definisana za sve ovlašćene učesnike u sistemu ili je informacija o korišćenim Pravilima uključena u elektronska dokumenta koja se razmenjuju i koja su potpisana kvalifikovanim elektronskim potpisom.

Potpisana elektronska dokumenta se razmenjuju u formi dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikovanom elektronskom sertifikatu potpisnika kako bi primalac elektronskog dokumenta mogao proveriti kvalifikovani elektronski potpis na bazi usaglašene tehnologije i postupaka.

PRILOG 2: ZAKON O ELEKTRONSKOM POTPISU

Zakon o elektronskom potpisu u Srbiji (u nastavku: Zakon) je izglasan u Narodnoj Skupštini Republike Srbije dana 14.12.2004. i publikovan u Službenom Glasniku Republike Srbije br. 135 od 21.12.2004.

Osnovna uloga Zakona se svodi na dve najvažnije stvari:

1. Da propiše uslove pod kojima je elektronski potpis pravno ekvivalentan svojeručnom potpisu,
2. Da propiše uslove koje moraju da ispune Sertifikaciona tela koja izdaju kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.

Tamo gde se elektronski potpis i kvalifikovani elektronski potpis ne zahtevaju posebno odgovarajućim Zakonom, njihova upotreba treba da bude

na dobrovoljnoj osnovi. Publikovanjem Zakona o elektronskom potpisu, kao sistemskog zakona, omogućuje se pokretanje procesa ažuriranja svih relevantnih zakona koji imaju veze sa elektronskim poslovanjem. U tim zakonima, kao najmanje što treba uraditi, treba svuda gde piše svojeručni potpis dodati i „ili kvalifikovani elektronski potpis u skladu sa Zakonom o elektronskom potpisu".

Zakonske odredbe mogu zahtevati usklađenost sa određenim dodatnim uslovima za korišćenje kvalifikovanog elektronskog potpisa za aktivnosti državne uprave. Pomenuti uslovi treba da budu objektivni, proporcionalni, nediskriminatorni i treba da se odnose samo na specifične karakteristike relevantnih aplikacija.

U članu 45. Zakona se navodi da Nadležni organ donosi podzakonska akta za sprovođenje ovog Zakona. U tom smislu, pripremljena su četiri podzakonska akta koja su predviđena u Zakonu, i to:

- Pravilnik o vođenju evidencije sertifikacionih tela,
- Pravilnik o Registru sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate u Republici Srbiji,
- Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa,
- Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata.

Ova četiri podzakonska akta su publikovana u Službenom glasniku Republike Srbije br. 48 od 7. juna 2005. godine. Nakon publikovanja podzakonskih akata, neophodno je realizovati aktivnosti na uspostavi nadležnog Nacionalnog tela u cilju obezbeđenja neophodne infrastrukutre za implementaciju Zakona, a samim tim i Evropske Direktive o elektronskim potpisima. U pomenutim podzakonskim aktima, navedeno je da će se data akta primenjivati od 1. jula 2006. što praktično znači da je to datum predviđenog početka implementacije Zakona o elektronskom potpisu i podzakonskih akata.

Kao što je već rečeno, Zakon o elektronskom potpisu u Srbiji je izglasan u Narodnoj Skupštini Republike Srbije dana 14.12.2004. i publikovan u Službenom Glasniku Republike Srbije br. 135 od 21.12.2004. Time je završena priča koja je započela još u avgustu 2000. godine kada je radna grupa pod okriljem tadašnjeg Saveznog zavoda za informatiku započela izradu Predloga Zakona o elektronskom poslovanju i elektronskom potpisu. Predlagač tog Zakona je trebalo da bude Savezno Ministarstvo pravde ali iz mnogih poznatih i nepoznatih razloga taj Zakon nije nikada usvojen na saveznom nivou. Zatim je krajem 2002. godine organizovana radna grupa od strane Ministarstva za nauku, tehnologije i razvoj Republike Srbije za izradu Predloga Zakona o elektronskom potpisu. Ovaj predlog je izrađen početkom 2003. godine i prosleđen Ministarstvu a zatim Vladi i Skupštini ali nije stigao da bude izglasan pre nego što je vlada pala i skupština raspuštena.

Nakon formiranja nove Vlade početkom 2004. godine svi predlozi Zakona koji su se našli u proceduri prethodne Skupštine vraćeni su nadležnim Ministarstvima na eventualnu doradu. To se desilo i sa predlogom Zakona o elektronskom potpisu koji je vraćen tada Ministarstvu za nauku i zaštitu životne sredine koje je angažovalo istu radnu grupu za eventualnu reviziju Zakona. To je iskorišćeno da se izradi predlog u koga su ugrađene neophodne izmene u skladu sa najnovijim zaključcima i trendovima u tom domenu u Evropskoj zajednici. Tako modifikovan predlog je vraćen Ministarstvu i kompletna procedura je ponovo primenjena i, kao što je ranije istaknuto, uspešno završena tek krajem prošle godine. Na taj način, sudbina Zakona o elektronskom potpisu je na određeni način pratila dobro poznata politička previranja u našoj zemlji.

U međuvremenu, nekoliko država u okolini (Makedonija, Republika Srpska, Crna Gora) usvojilo je Zakone o elektronskom potpisu koji su se manje ili više bazirali na nekim našim prethodnim verzijama Zakona.

Kao što je ranije već rečeno, osnovna uloga Zakona o elektronskom potpisu se svodi na dve najvažnije stvari:

- da propiše uslove pod kojima je elektronski potpis pravno ekvivalentan
- svojeručnom potpisu i
- da propiše uslove koje moraju da ispune Sertifikaciona tela koja izdaju
- kvalifikovane sertifikate za verifikaciju kvalifikovanih elektronskih potpisa.

Zakon o elektronskom potpisu primenljiv je na pravna i fizička lica jer se sertifikati izdaju kako fizičkim licima tako i fizičkim licima koji su pravni zastupnici pravnih lica.

U daljem tekstu je dat osvrt na odredbe Zakona, posebno ističući karakteristične i veoma važne odredbe, a posebno imajući u vidu odredbe koje se odnose na specificiranje određenih poslova Nadležnog tela.

Zakon se sastoji od sledećih 7 poglavlja:

1. Osnovne odredbe,
2. Elektronski potpis i kvalifikovani elektronski potpis,
3. Elektronski sertifikati i sertifikaciona tela,
4. Prava, obaveze i odgovornosti korisnika i sertifikacionih tela,
5. Nadzor,
6. Kaznene odredbe,
7. Prelazne i završne odredbe.

OSNOVNE ODREDBE

U prvom poglavlju, Članovi 1.-5. Zakona, daju se osnovne odrednice Zakona (Član 1.), definicije pojedinih izraza (Član 2.), kao i odrednice vezane za elektronske dokumente (Članovi 3.-5.).

Posebno treba istaći da se Članovima od 3. do 5. ustanovljava pravna validnost i punovažnost elektronske dokumentacije. Dakle, iako se primenom elektronskih dokumenata ipak ne mogu realizovati sve vrste poslova i pravnih radnji (izuzeci su navedeni u Članu 3), sva dokumentacija koju treba čuvati može se čuvati i u elektronskom obliku pri čemu elektronski dokumenti moraju biti elektronski potpisani. Dakle, pomenute odredbe predstavljaju osnovne odredbe kojima se prepoznaje elektronski dokument u našem pravnom sistemu i kao takve, svakako mogu predstavljati osnovu za primenu u različitim oblastima.

Međutim, sa druge strane, Zakon predstavlja osnovu za uspostavljanje elektronskog potpisa, elektronskog dokumenta i elektronskog sertifikata u našem pravnom sistemu i, kao sistemski zakon, treba da podstakne donošenje novih i ažuriranje postojećih zakona u cilju primene elektronskog potpisa i elektronskog dokumenta. Među takvim novih zakonima bi bili i Zakon o elektronskoj upravi, Zakon o elektronskom dokumentu, Zakon o elektronskoj arhivi, Zakon o nadležnom telu za vremensku overu (Time-Stamping Authority), itd. koji bi delimično ili potpuno imali uporište u Zakonu o elektronskom potpisu.

ELEKTRONSKI POTPIS I KVALIFIKOVANI ELEKTRONSKI POTPIS

U drugom poglavlju, članovi 6.-11. Zakona, utvrđuju se osnovne odrednice Zakona vezane za primenu elektronskog potpisa i kvalifikovanog elektronskog potpisa. U članu 6. se, u skladu sa Evropskom direktivom, utvrđuje da elektronskom potpisu ne može da se ukine pravno dejstvo samo zato što je u elektronskom obliku. To pravo se ograničava u datom članu na sve one poslove i postupke koji ne zahtevaju primenu svojeručnog potpisa. U članu 7. se posebno ističu uslovi koje je neophodno da zadovolji elektronski potpis da bi bio kvalifikovani elektronski potpis. Kao što je već ranije rečeno, osnovna dva uslova za kreiranje kvalifikovanog potpisa su:

- Kreiranje kvalifikovanog elektronskog potpisa pomoću sredstva za kreiranje kvalifikovanog elektronskog potpisa (SSCD - Secure Signature Creation Device),
- Da potpisnik poseduje kvalifikovani elektronski sertifikat.

Članovi 8. i 9. Zakona ukazuju na osnovne uslove koje moraju da obezbede sredstva za kreiranje i sredstva za proveru kvalifikovanog elektronskog potpisa, respektivno. Ovi članovi takođe odgovaraju Aneksima 3 i 4 Evropske Direktive o elektronskim potpisima, respektivno.

Član 10. je jedan od ključnih članova Zakona jer utvrđuje pravnu ekvivalentnost između kvalifikovanog elektronskog potpisa (i njegovo dejstvo na podatke u elektronskom obliku) i svojeručnog potpisa, odnosno svojeručnog potpisa i pečata (i njihovo dejstvo na podatke u papirnom obliku). Posebno se ističe odrednica Zakona o pravnoj ekvivalentnosti kvalifikovanog elektronskog potpisa i svojeručnog potpisa i pečata jer je to delimično i osnova za donošenje Zakona o nadležnom telu za vremensku overu (Time-Stamping Authority).

Član 11. utvrđuje da Nadležni organ (Ministarstvo za nauku i zaštitu životne sredine, u daljem tekstu: Ministarstvo) propisuje tehničko-tehnološke postupke za formiranje kvalifikovanog elektronskog potpisa, kao i bliže uslove koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa. Ovaj član Zakona je stoga osnova za izradu odgovarajućeg podzakonskog akta.

ELEKTRONSKI SERTIFIKATI I SERTIFIKACIONA TELA

Ovo poglavlje je posvećeno drugim važnim pojmovima i tehnologijama koji se uvode ovim Zakonom, pored elektronskog potpisa, a to su: elektronski sertifikati i sertifikaciona tela koja ih izdaju. U tom smislu, osnovne definicije elektronskog sertifikata i sertifikacionog tela su, zbog celine izlaganja, ponovljene u članu 12. Zakona.

Član 13. Zakona ukazuje da sertifikacionim telima nije potrebna posebna dozvola za izdavanje elektronskih sertifikata, a član 14. utvrđuje da Nad-

ležni organ vodi evidenciju sertifikacionih tela. Prema članu 15. Zakona, sertifikaciono telo je dužno da Nadležnom organu prijavi početak obavljanja usluga izdavanja elektronskih sertifikata najmanje 15 dana pre početka rada. U članu 16. Zakona se utvrđuje način vođenja evidencije sertifikacionih tela koja izdaju elektronske sertifikate i taj član je osnova za izradu odgovarajućeg podzakonskog akta.

Član 17. Zakona je takođe jedan od ključnih članova Zakona jer ukazuje na to koji podaci moraju da se sadrže u kvalifikovanom elektronskom sertifikatu. Ovaj član se, u tom smislu, bazira na Aneksu 1 Evropske direktive.

Član 18. Zakona je još jedan od ključnih članova Zakona jer se u njemu definišu kriterijumi koje moraju da ispune sertifikaciona tela koja izdaju kvalifikovane elektronske sertifikate. Ovaj član se bazira na Aneksu 2 Evropske direktive. Na kraju pomenutog člana se navodi da će Nadležni organ propisati bliže uslove i način provere ispunjenosti uslova iz datog člana i to predstavlja osnovu za izradu odgovarajućeg podzakonskog akta. Proces provere ispunjenosti uslova iz člana 18. Zakona predstavlja proceduru akreditacije sertifikacionih tela od strane Nadležnog organa.

U članu 19. Zakona se navodi da Nadležni organ vodi Registar sertifikacionih tela za koja se utvrdi da ispunjavaju uslove iz člana 18. Zakona (tj. za akreditovana sertifikaciona tela). Ovaj član predstavlja osnovu za izradu odgovarajućeg podzakonskog akta.

U članu 20. Zakona, takođe ključni član, navodi se da sertifikaciono telo mora ispunjavati sve uslove iz člana 18. Zakona da bi bilo upisano u Registar sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate. Drugim rečima, prema našem Zakonu o elektronskom potpisu utvrđuje se ovim članom obavezna akreditacija za sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate. Ovo je na neki način odstupanje od određenih navoda iz Evropske direktive kojima se propisuje takozvana "dobrovoljna" akreditacija sertifikacionih tela. Međutim, u našem Zakonu su korišćena rešenja koja su slična regulativi i legislativi onih zemalja Evropske unije (kao na primer Nemačka) koje su čvrsto uspostavile nacionalnu PKI infrastrukturu i kod kojih ima najviše akreditovanih sertifikacionih tela i odobrenih sredstava za formiranje kvalifikovanih elektronskih potpisa (SSCD).

Odredbama člana 21. Zakona se dozvoljava da se organu državne uprave može poveriti izdavanje kvalifikovanih elektronskih sertifikata u skladu sa posebnim propisima koji se odnose na organe državne uprave. Smisao ovog člana je da se može formirati i PKI infrastruktura za izdavanje kvalifikovanih sertifikata u okviru državne uprave u skladu sa posebnim propisima i da odgovarajuće sertifikaciono telo ne mora da se akredituje kod Nadležnog organa da bi bilo upisano u Registar iz člana 19. zakona. Međutim, podrazumeva se da dato sertifikaciono telo ispunjava sve uslove za sertifikaciono telo koje izdaje kvalifikovane sertifikate, navedene u članu 18. Zakona.

Član 22. Zakona ukazuje na to da evidencija iz člana 16. kao i Registar iz člana 19. Zakona moraju biti javno dostupni svim zainteresovanim stranama.

PRAVA, OBAVEZE I ODGOVORNOSTI KORISNIKA I SERTIFIKACIONIH TELA

Četvrto poglavlje Zakona je posvećeno osnovnim pravima, obavezama i odgovornostima kako korisnika kojima se izdaju tako i sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate. U tom smislu, prvih 5 članova (članovi 23.-27.) u ovom poglavlju se odnose na korisnika i na njegova prava i obaveze:

- Da može da mu se izda sertifikat na njegov zahtev o čemu sklapa poseban ugovor sa sertifikacionim telom (član 23.),
- Da može sam da bira sertifikaciono telo izuzev u slučajevima koji su definisani posebnim propisima (član 23.),
- Da može istovremeno koristiti usluge više sertifikacionih tela (član 23.),
- Da se kvalifikovani elektronski sertifikat izdaje svakom korisniku na njegov zahtev na bazi nesumnjivo utvrđenog identiteta i ostalih Zakonom utvrđenih podataka (član 24.),
- Da je korisnik dužan da čuva podatke i sredstva za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe (član 25.),
- Da je korisnik dužan da odmah dostavi sertifikacionom telu sve informacije o promenama podataka koji se nalaze u korisnikovom sertifikatu (član 26.),
- Da je korisnik dužan da odmah zatraži opoziv svog sertifikata u svim slučajevima gubitka ili oštećenja sredstava za formiranje kvalifikovanog elektronskog potpisa (član 26.),
- Da korisnik odgovara za sve nepravil-

nosti koje su nastale neispunjavanjem obaveza iz članova 25. i 26., osim ako ne dokaže da oštećeno lice nije preduzelo sve Zakonom propisane radnje za proveru elektronskog potpisa i elektronskog sertifikata (član 27.).

Sledećih 5 članova Zakona (članovi 28.-32.) se odnose na sertifikaciono telo i na njegova prava i obaveze:

- Da obezbedi ispunjenje osnovnih dužnosti kao sertifikaciono telo (član28.),
- Da informiše korisnike o svim važnim aspektima upotrebe
- kvalifikovanog elektronskog sertifikata (član 29.),
- Da izvrši sve neophodne aktivnosti u vezi funkcije opoziva
- kvalifikovanih elektronskih sertifikata (član 30.),
- Da čuva kompletnu dokumentaciju o kvalifikovanim elektronskim
- sertifikatima 10 godina nakon prestanka njihove važnosti (član 31.),
- Da izvrši sve neophodne aktivnosti u vezi sa prestankom obavljanja delatnosti (član 32.).

U članu 33. se navodi obaveza Nadležnog organa da propiše najniži iznos osiguranja od rizika za moguće štete nastale vršenjem usluga izdavanja sertifikata, dok je član 34. Zakona posvećen utvrđivanju uslova pod kojima je sertifikaciono telo odgovorno i uslova kada nije odgovorno za moguću štetu licima koja su se pouzdala u kvalifikovani elektronski sertifikat izdat od strane datog sertifikacionog tela.

Član 35. Zakona je posvećen uslovima pod kojima su inostrani elektronski i kvalifikovani elektronski sertifikati ravnopravni sa domaćim sertifikatima.

NADZOR

Peto poglavlje Zakona (članovi 36. do 41.) posvećeno je inspekcijskom nadzoru sertifikacionih tela (koja su upisana u evidenciju i u Registar) koje vrši Nadležni organ. U tom smislu, u članu 36. se navode te osnovne obaveze Nadležnog organa. Opseg posla pomenutog inspekcijskog nadzora je naveden u članu 37. dok je član 38. Zakona posvećen navođenju prava i dužnosti koja imaju ovlašćena lica Nadležnog organa u vršenju inspekcijskog nadzora.

U članu 39. Zakona se navodi šta sve može ovlašćeno lice Nadležnog organa da propiše svojim rešenjem, kao jednu vrstu opomene, ukoliko se utvrdi neadekvatan i protivzakonit rad sertifikacionog tela, dok se u članu 40. Zakona navodi da Nadležni organ donosi rešenje o brisanju datog sertifikacionog tela iz Registra sertifikacionih tela koja izdaju kvalifikovane sertifikate ukoliko ono prestane da ispunjava uslove iz člana 18. ovog Zakona.

Član 41. Zakona je posvećen dužnostima sertifikacionog tela koje u cilju sprovođenja inspekcijskog nadzora moraju da omoguće pristup u poslovne prostorije i podatke o poslovanju i celokupnu poslovnu dokumentaciju, uvid u računarsku opremu i informacionu infrastrukturu, itd. ovlašćenim predstavnicima Ministarstva nadležnim za inspektorske poslove.

KAZNENE ODREDBE

Članovi 42. do 44. Zakona predstavljaju kaznene odredbe za različite slučajeve nepoštovanja Zakona i određenih njegovih odredbi definisanih u pojedinim članovima. U tom smislu, član 42. se odnosi na prekršaje korisnika i stoga su definisane kazne za sledeće grupe korisnika:

- Korisnik – pravno lice,
- Korisnik – preduzetnik,
- Odgovorno lice u pravnom licu,
- Korisnik – fizičko lice.

Član 43. Zakona odnosi se na kazne predviđene za sertifikaciono telo, kao i za odgovorno lice sertifikacionog tela.

Član 44. Zakona odnosi se na kazne za prekršaje u domenu čuvanja podataka i sredstava za proveru elektronskog potpisa onoliko vremena koliko je propisano da se čuvaju sama elektronska dokumenta i te kazne se odnose na korisnike pravna lica, preduzetnike, kao i na odgovorna lica u pravnom licu.

PRELAZNE I ZAVRŠNE ODREDBE

Ovo poglavlje sastoji se od dva člana (članovi 45. i 46.) i odnosi se na utvrđivanje da će Nadležni organ doneti podzakonska akta za sprovođenje ovog Zakona u roku od 3 meseca od datuma stupanja na snagu Zakona (član 45.), kao i da Zakon stupa na snagu osmog dana od dana njegovog objavljivanja u Službenom glasniku Republike Srbije.

PRILOG 3: PODZAKONSKA AKTA

U ovom poglavlju su razmatrana četiri podzakonska akta Zakona o elektronskom potpisu koja bliže uređuju pitanja:

- vođenja evidencije sertifikacionih tela,
- uspostave Registra sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate,
- tehničko-tehnoloških uslova za formiranje kvalifikovanog elektronskog potpisa,
- kriterijuma koje treba da ispuni sertifikaciono telo da bi izdavalo kvalifikovane elektronske sertifikate.

Podzakonska akta su publikovana u Službenom glasniku Republike Srbije br. 48 od 7. juna 2005. godine. Zakon daje opšte odredbe i nije zavistan od tehničko-tehnoloških aspekata realizacije elektronskog potpisa i elektronskih sertifikata. U tom smislu, podzakonska akta, koja se mogu lakše menjati u skladu sa razvojem odgovarajućih tehnoloških rešenja jer ih donosi nadležni Ministar a ne Narodna skupština, bliže određuju sva tehnička pitanja vezana za Zakon o elektronskom potpisu i imaju uporište u odgovarajućim članovima Zakona.

U podzakonskim aktima je precizirano da je Nadležni organ, naveden u Zakonu o elektronskom potpisu, u stvari Ministarstvo za nauku i zaštitu životne sredine (u nastavku Ministarstvo) koje je nadležno za informaciono društvo (član 11. Zakona) i, shodno tome, podzakonska akta je potpisao Ministar za nauku i zaštitu životne sredine.

PRAVILNIK O EVIDENCIJI SERTIFIKACIONIH TELA

Ovim pravilnikom propisuje se sadržaj i način vođenja evidencije sertifikacionih tela koja obavljaju usluge izdavanja elektronskih sertifikata na teritoriji Republike Srbije, način podnošenja prijave za upis u evidenciju, obrazac prijave za upis u evidenciju, potrebna dokumentacija uz prijavu, promena podataka i obrazac prijave za upis promene. Ovaj pravilnik je predviđen u članu 16. stav 2, Zakona, a odnosi se i na na član 15. Zakona po kome je sertifikaciono telo dužno da nadležnom organu prijavi početak obavljanja usluga izdavanja elektronskih sertifikata, najmanje 15 dana pre početka rada.

Član 14. Zakona definiše obavezu Nadležnog organa da vodi evidenciju sertifikacionih tela. Evidencija se vodi u papirnom i elektronskom obliku. Evidencija u elektronskom obliku je javno dostupna putem Web sajta Ministarstva.

PRAVILNIK O REGISTRU SERTIFIKACIONIH TELA ZA IZDAVANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA U REPUBLICI SRBIJI

Ovim Pravilnikom propisuje se sadržaj i način vođenja registra sertifikacionih tela koja izdaju kvalifikovane elektronske sertifikate u Republici Srbiji (u daljem tekstu: Registar), način podnošenja zahteva za upis u Registar, potrebna dokumentacija koja se prilaže uz zahtev, obrazac zahteva, kao i način objavljivanja podataka iz Registra. Ovaj pravilnik je predviđen članom 19. stav 2 Zakona. Registar vodi Ministarstvo u papirnom i elektronskom obliku. Registar u elektronskom obliku je potpisan kvalifikovanim elektronskim potpisom Ministarstva. Registar u elektronskom obliku je javno dostupan na Internet strani Ministarstva.

PRAVILNIK O TEHNIČKO-TEHNOLOŠKIM POSTUPCIMA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA I KRITERIJUMIMA KOJE TREBA DA ISPUNE SREDSTVA ZA FORMIRANJE KVALIFIKOVANOG ELEKTRONSKOG POTPISA

Ovim pravilnikom propisuju se tehničko-tehnološki postupci za formiranje kvalifikovanog elektronskog potpisa, kriterijumi koje treba da ispune sredstva za formiranje i proveru kvalifikovanog elektronskog potpisa, kao i način razmene potpisanih elektronskih dokumenata, postupak formiranja i provere kvalifikovanih elektronskih sertifikata i druga tehnička pitanja od značaja za sprovođenje Zakona. U ovom pravilniku su navedeni i odgovarajući međunarodni standardi i preporuke sa kojima moraju da budu u skladu postupci za formiranje kvalifikovanog elektronskog potpisa, kao i kriterijumi koje treba da ispunjavaju sredstva za formiranje i proveru kvalifikovanog elektronskog potpisa. Ovaj pravilnik je predviđen članom 11. Zakona u kome se navodi da Ministarstvo, kao Nadležni organ, propisuje tehničko-tehnološke postupke za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

U ovom pravilniku je naveden skup tehničkih pravila koja opisuju način formiranja kvalifikovanog elektronskog potpisa u skladu sa trenutnim tehnološkim, algoritamskim i standardizacionim aktivnostima. Kvalifikovani elektronski potpis se formira u skladu sa preporukom PKCS#1, a dužina modulusa u asimetričnom kriptografskom algoritmu mora biti minimalno 1024 bita. Takođe, kvalifikovani elektronski potpis se formira primenom jednog od standardizovanih asimetričnih kriptografskih algoritama iz sledeće grupe: RSA, DSA ili ECDSA. Pri formiranju kvalifikovanog elektronskog potpisa primenjuju se i hash funkcije za dobijanje otisaka poruke fiksne veličine (128 ili 160 bita). Hash funkcije se realizuju primenom standardizovanih hash algoritama: MD5 (Message Digest) -rezultuje u hash vrednostima veličine 128 bita ili SHA-1 (Secure Hash Algorithm) -rezultuje u hash vrednostima veličine 160 bita.

Takođe je veoma bitno istaći da je u pravilniku navedeno (član 7. pravilnika) da sredstvo za formiranje kvalifikovanog elektronskog potpisa mora imati takva svojstva koja omogućavaju naknadnu ugradnju novih algoritama u skladu sa daljim razvojem kriptografskih tehnika i standarda. To se posebno odnosi na navedene standardne hash funkcije za koje se već sada zna da imaju kriptografske slabosti. To se odnosi na SHA-1 algoritam a pogotovo na MD5. U tom smislu, u svetu se već razmatra šire uvođenje i postepena standardizacija kvalitetnijih hash algoritama, kao što su: RIPEMD-160, SHA-256, SHA-512 i drugi. Međutim, za sada u svetu i dalje preovlađuju navedeni hash algoritmi: MD5 i SHA-1.

Kvalifikovani elektronski potpis formira se u skladu sa skupom tehničkih pravila za formiranje kvalifikovanog elektronskog potpisa koji moraju poštovati kako potpisnik tako i korisnik koji proverava kvalifikovani elektronski potpis. Pravila propisuje nadležno Sertifikaciono telo u skladu sa Zakonom o elektronskom potpisu i ovim Pravilnikom. Pravila su unapred definisana za sve ovlašćene učesnike u sistemu ili je informacija o korišćenim Pravilima uključena u elektronska dokumenta koja se razmenjuju i koja su potpisana kvalifikovanim elektronskim potpisom.

Potpisana elektronska dokumenta se razmenjuju u formi dokumenata u kojima su ugrađeni osnovni podaci o postupku, algoritmu i kvalifikovanom elektronskom sertifikatu potpisnika kako bi primalac elektronskog dokumenta mogao proveriti kvalifikovani elektronski potpis na bazi usaglašene tehnologije i postupaka. Forma elektronskog dokumenta koji je potpisan kvalifikovanim elektronskim potpisom mora da je usklađena na primer sa PKCS#7 preporukom.

Dalje, u pravilniku se navodi da kvalifikovani elektronski sertifikat mora imati strukturu definisanu preporukom ITU-T X.509v3 i da bude u skladu sa profilom kvalifikovanog sertifikata koji je definisan u standardnim dokumentima navedenim u pravilniku. Takođe, navodi se i da postupak provere kvalifikovanog elektronskog potpisa obuhvata i postupak provere kvalifikovanog elektronskog sertifikata sa naznačenim koracima od kojih se sastoji pomenuti postupak.

U daljem tekstu pravilnika se navode dodatni kriterijumi koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa, kao i standardi i preporuke sa kojima treba da budu u skladu sredstva za formiranje i proveru kvalifikovanog elektronskog potpisa. Najvažniji dodatni kriterijumi, između ostalih, koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa (SSCD) su:

- da se podaci za formiranje kvalifikovanog elektronskog potpisa generišu
- u samom SSCD i da ga nikad ne napuštaju,
- da se kvalifikovani elektronski potpis formira u samom sredstvu za formiranje kvalifikovanih elektronskih potpisa (SSCD).
-

Programska oprema i postupci primenom kojih se vrši provera kvalifikovanog elektronskog potpisa moraju u potpunosti onemogućiti dobijanje podataka za izradu kvalifikovanog elektronskog potpisa pomoću podataka za njegovu proveru.

PRAVILNIK O BLIŽIM USLOVIMA ZA IZDAVANJE KVALIFIKOVANIH ELEKTRONSKIH SERTIFIKATA

Ovim Pravilnikom propisuju se kriterijumi koje moraju da ispune sertifikaciona tela koja izdaju kvalifikovane elektronske sertifikate, kao i način provere njihove ispunjenosti. Proveru ispunjenosti kriterijuma za izdavanje kvalifikovanih elektronskih sertifikata vrši Ministarstvo neposredno, odnosno drugi subjekat kome je Ministarstvo poverilo navedene poslove. Izdavanje kvalifikovanih elektronskih sertifikata u smislu Zakona i ovog pravilnika, podrazumeva formiranje i dodeljivanje kvalifikovanih elektronskih sertifikata korisnicima, odnosno pružanje usluga sertifikacije. Ovaj pravilnik je predviđen članom 18. stav 2 Zakona.

U Zakonu su date sledeće definicije:

- Elektronski sertifikat – elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;

- Kvalifikovani elektronski sertifikat - elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene Zakonom;
- Sertifikaciono telo - pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama Zakona.

Kvalifikovani elektronski sertifikat je izdat od strane Sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata, mora da bude usklađen sa preporukom ITU-T H.509, i mora da sadrži sledeće podatke:

- oznaku da se radi o kvalifikovanom sertifikatu,
- skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat,
- skup podataka koji jedinstveno identifikuju potpisnika,
- podatke za proveru elektronskog potpisa (javni ključ asimetričnog algoritma) koji odgovaraju podacima za formiranje kvalifikovanog elektronskog potpisa koji su pod kontrolom potpisnika,
- podatke o početku i kraju važenja elektronskog sertifikata,
- identifikacioni broj izdatog elektronskog sertifikata,
- eventualna ograničenja vezana za upotrebu sertifikata,
- kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat.

Kvalifikovani elektronski sertifikat mora da je usklađen sa preporukom ITU-T H.509 i dokumentima: ETSI ESI TS 101 862 "Qualified Certificate Profile" i RFC 3739 "Intemet H.509 Public Keu Infrastructure: Qualified Certificates Profile".

Dakle, da bi ce formirao kvalifikovani elektronski potpis neophodno je da potpisnik ima kvalifikovani elektronski sertifikat koga izdaje sertifikaciono telo koje ispunjava određene uslove definisane u Direktivi Evropske Unije o elektronskim potpisisma 1999/93/ES od 19.01.2000. godine i u Zakonu. Drugim rečima, CA koje izdaje kvalifikovane elektronske sertifikate treba da ispuni uslove za izdavanje kvalifikovanih sertifikata u skladu sa Direktivom Evropske unije o elektronskim potpisima (Aneks 2 Direktive) i domaćim Zakonom o elektronskom potpisu (član 18. Zakona).

U skladu sa kriterijumima navedenim u Direktivi (Aneks 2), u članu 18. Zakona su definisani odgovarajući domaći kriterijumi koje treba da ispune sertifikaciona tela u cilju izdavanja kvalifikovanih elektronskih sertifikata, koje navodimo u nastavku.

Dakle, prema Zakonu Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata mora ispunjavati sledeće uslove:

1. sposobnost za pouzdano obavljanje usluga izdavanja elektronskih sertifikata;
2. bezbedno i ažurno vođenje registra korisnika kao i sprovođenje bezbednog i trenutnog opoziva elektronskog sertifikata;
3. obezbeđivanje tačnog utvrđivanja datuma i vremena izdavanja ili opoziva elektronskog sertifikata;
4. da izvršava proveru identiteta i, ako je potrebno, drugih dodatnih obeležja licu kojem se izdaje sertifikat, na pouzdan način i u skladu sa propisima;
5. da ima zaposlena lica sa specijalističkim znanjima, iskustvom i stručnim kvalifikacijama potrebnim za vršenje usluge izdavanja elektronskih sertifikata, a naročito u odnosu na: upravljačke sposobnosti, stručnost u primeni tehnologija elektronskog potpisa i odgovarajućih sigurnosnih procedura i bezbednu primenu odgovarajućih administrativnih i upravljačkih postupaka koji su usaglašeni sa priznatim standardima;
6. da koristi pouzdane sisteme i proizvode koji su zaštićeni od neovlašćenih izmena i koji obezbeđuju tehničku i kriptografsku sigurnost procesa;
7. da preduzima mere protiv falsifikovanja elektronskih sertifikata, a u slučajevima u kojima generiše podatke za formiranje elektronskog potpisa da garantuje tajnost procesa formiranja tih podataka;
8. da obezbedi finansijske resurse za osiguranje od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata;
9. da obezbedi čuvanje svih relevantnih informacija koje se odnose na elektronske sertifikate u propisanom vremenskom periodu i to u izvornom obliku;
10. da ne čuva i ne kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu;
11. da obezbedi sisteme za fizičku zaštitu uređaja, opreme i podataka, i sigurnosna rešenja za zaštitu od neovlašćenog pristupa;
12. da informiše lica koja traže izdavanje

kvalifikovanog elektronskog sertifikata o tačnim uslovima izdavanja i korišćenja tog sertifikata, uključujući bilo koja ograničenja u korišćenju, kao i o postupcima za rešavanje sporova. Takve informacije, koje mogu biti dostavljene elektronski, moraju biti napisane i pripremljene u razumljivom obliku na srpskom jeziku. Odgovarajući delovi tih informacija moraju biti raspoloživi na zahtev trećim licima koja koriste elektronski sertifikat;

13. da koristi pouzdan sistem upravljanja elektronskim sertifikatima u obliku koji omogućava njihovu proveru kako bi:

- unos i promene radila samo ovlašćena lica;
- mogla biti proverena autentičnost informacija iz sertifikata;
- elektronski sertifikati bili javno raspoloživi za pretraživanje samo u onim slučajevima za koje je vlasnik sertifikata dao saglasnost;
- bilo koja tehnička promena koja bi mogla da naruši bezbednosne zahteve bila poznata sertifikacionom telu.

U tekstu pravilnika je svaki od 13 kriterijuma detaljnije razrađen a na kraju su navedene i procedure provere ispunjenosti datih kriterijuma. Naime, sertifikaciono telo pred Ministarstvom vrši demonstraciju kompletnog poslovanja u smislu ispunjenja navedenih 13 kriterijuma i drugih aktivnosti usaglašenih sa Zakonom, ovim pravilnikom, kao i Opštim i Posebnim pravilima rada sertifikacionog tela.

Samo one kompanije koje mogu da dokažu da poseduju neophodnu pouzdanost i specijalističko znanje mogu da rade kao sertifikaciona tela koja izdaju kvalifikovane sertifikate. Oni takođe moraju da pokažu da poseduju osiguranje za nadoknadu eventualnih šteta nastalih njihovom krivicom. Kompanija koja je kandidat za sertifikaciono telo koje izdaje kvalifikovane sertifikate posedovaće neophodnu pouzdanost poslovanja ukoliko može garantovati da će se kao sertifikaciono telo pridržavati svih odgovarajućih zakonskih regulativa koje propisuju poslovanje sertifikacionih tela. Neophodno specijalističko znanje će biti raspoloživo ukoliko osobe koje rade u sertifikacionom telu poseduju to znanje, iskustvo i veštine koje se zahtevaju za njihov posao. Ostali uslovi za rad sertifikacionog tela će biti zadovoljeni ukoliko su mere za ispunjenje bzbednosnih zahteva iz Zakona o elektronskom potpisu i odgovarajućeg podzakonskog akta odgovarajuće, ako su predstavljene na odgovarajući način u Internim pravilima rada i dostavljene Nadležnom organu na verifikaciju, kao i ako su potpuno implementirane u praksi. Potrebno je obezbediti da su ovi uslovi ispunjeni tokom čitavog operativnog rada sertifikacionog tela. Ako se iz bilo kojih okolnosti ukazujue da nije moguće više ispunjavati sve zahtevane uslove, mora se o tome odmah bez kašnjenja obavestiti Nadležni organ.

LITERATURA

[1] Milan Marković, „Uspostava nacionalne PKI infrastrukture za primenu kvalifikovanog elektronskog potpisa u Srbiji“, Smart e-Government 2005, Beograd, 18.-19.10.2005. Pozivni rad.
[2] Simon Singh, “The Code book: Secret History of Codes and Code breaking”, Fourth Estate, 1999.
[3] D. Kahn, “The Codebreakers: The comprehensive History of Secret communication from Ancient Times to the Internet”, Scribner, Revised edition, 1996.
[4] W. F. Friedman, “The Index of Coincidence and Its Application on Cryptography”, Riverbank Publication No. 22, Riverbank Labs. 1920. Reprinted by Aegan Park Press 1987.
[5] C.E.Shannon, “Communication Theory of Secrecy Systems”, Bell system Technical Journal, v.28, n. 4, 1949, pp. 656-715.
[6]J.L.Smith, “The Design of Lucifer, A cryptographic device for data communication”, IBM research report RC3326, 1971.
[7] Federal Information Processing Standards, “Data Encryption standard (DES)”, Publication 46-3, Okt 1999.
[8] Federal Information Processing Standards, “Advanced Encryption standard (AES)”, Publication 197, Nov 2001.
[9] W. Diffie, M. Hellman, “New Directions in Cryptography”, IEEE Transactions on information theory, Nov 1976, pp. 644-654.
[10] R.L. Rivest, A. Shamir, L.M. Adleman, “A method for Obtaining digital signatures and Public-Key Cryptosystems”, Communications of the ACM, v. 21, n. 2, Feb 1978, pp.120-126.
[11] A. Menezes, P. van Oorschot, S. Vanstone, “Handbook of Applied Cryptography”, CRC press, 1996.
[12] B. Schneier: “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2nd Edition, John Wiley & Sons, 1996.
[13] “An Introduction to Cryptography”, Network Associates Inc., studeni 1998. http://www.cs.ust.hk/~choy/comp364/Spr02/PGP-introCrypto.pdf
[14] “Cryptography A-Z”, SSH Communication Security, 2003. http://www.ssh.com/support/cryptography/index.html
[15] EFF, „Cracking DES: Secrets of Encryption research, Wiretap Politics and Chip Design“, O’Reilly and Associates, 1998.
[16] T. ElGamal, “A Public-Key Cryptosystem and a Signature Scheme Base on Discrete Logarithms”, Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, 1985, pp. 10-18.
[17] V.S. Miller, “Use of Elliptic Curves in Cryptography”, Advances in Cryptology: Proceedings of CRYPTO 85, Springer-Verlag, 1986, pp. 417-426.
[18] N. Koblitz, “Elliptic Curve Cryptosystems”, Mathematics of Computation, v.48, n. 177, 1987, pp.203-209.
[19] “Factorization of RSA-576”, RSA Security, RSA Laboratories, http://www.rsasecurity.com/rsalabs/challenges/factoring/rsa576.html.
[20] Franke J. , “RSA576”, Privately circulated email reposted to prime numbers Yahoo! Group, Dec 2003.
[21] Wikipedia, http://en.wikipedia.org/wiki/Million_instructions_per_second
[22] S. Gilheany, “Evolution of Intel Microprocessors: 1971 to 2007”, Berghell Associates, LLC http://www.berghell.com/whitepapers.htm
[23] M. Gardner, “A new Kind of Cipher that would take millions of years to break”, Scientific American, v. 237, n. 8, Aug 1977, pp. 120-124
[24] G. Moore, “Craming more components onto integrated circuits”, Electronic, Volume 38, Number 8, April 1965.
[25] V. Welch et al, “X.509 Proxy Certificates for dynamic delegation”, 3rd annual PKI RandD Workshop, 2004.
[26] E.Persson, “Digital Identity Service in Sweden”, in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
[27] T.Denny, “Secure Transactions over Open Networks”, in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
[28] M.Marković, Z.Savić, Ž.Obrenović, A.Nikolić, “A PC cryptographic coprocessor based on TI signal processor and smart card system”, Proc. of CMS2001 (Communication and Multimedia Security), May 21-22, Darmstadt, Germany.
[29] P.VanEecke, “Legal status of non-qualified, qualified and enhanced electronic signatures in the

Member States", EEMA Workshop "The Legal Impact of the Electronic Signature Directive on Business", Novembar 29/30, 2001, Brussels, Belgium
[30] P.VanEecke, "The European Legal Framework on Electronic Signatures", in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
[31] J.Dumortier, "The implementation of e-Signature Directive in the Member States", EEMA Workshop "Putting e-Signatures into Practice," Novembar 25/26, 2002, Brussels, Belgium.
[32] S.Upton, "Presentation of a voluntary accreditation scheme for Certification service providers", EEMA Workshop "Putting e-Signatures into Practice," Novembar 25/26, 2002, Brussels, Belgium.
[33] C.Luyten, "A legally recognized platform for electronic invoicing", EEMA Workshop "Putting e-Signatures into Practice", Novembar 25/26, 2002, Brussels, Belgium.
[34] J.M.Eymeri, "The Electronic Identification of Citizens and Organizations in the European Union: State of Affairs", 37th Meeting of the Director-General of the Public Service of the Member States of the European Union, November 26/27, 2001, Bruges, Belgium.
[35] E.Persson, "Digital Identity Service in Sweden", in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002
[36] B.Goetz, A.Kraft, "eGovernment – two success stories for G2E & G2C in Germany", in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
[37] S.Klein, "Using electronic signatures for e-government services – the experiences of the city of Bremen" EEMA Workshop "Putting e-Signatures into Practice" Novembar 25/26, 2002, Brussels, Belgium
[38] F.Wynants, "The Co-Sourced PKI Solution – the Belgian e-ID Project", EEMA Workshop "PKI – Making it Work," May 6/7, 2003, Stockholm, Sweden
[39] Z.Savić, A.Nikolić, M.Marković, "Cryptographic Proxy Gateways in Securing TCP/IP Computer Networks", in Proc. of Information Security Solution Europe Conference, ISSE 2001, London, September 26-28, 2001
[40] Z.Savić, M.Marković, "Development of Secure WEB Financial Services in Serbia", accepted for Information Security Solution Europe Conference, ISSE 2003, Wienna, Austria, Occtober 7-9, 2003
[41] S.Kent, "A System Level Analyst of Biometric User Authentication", in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002
[42] R.Muller, "Biometrics and ISO standardisation", in Proc. of Information Security Solution Europe Conference, ISSE 2002, Paris, October 2-4, 2002.
[43] Milan Marković, „Data protection technics and cryptographic protocols in modern computer networks", Tutorial 13th International conference on Telecommunications, ICT 2006, Madeira Portugal, May 9-12, 2006.
[44] Randall K. Nichols, ICSA Guide to Cryptography, Computing McGraw-Hill, First edition, December 1999.
[45] A.K. Lenstra, E.R. Verheul: Selecting cryptographic key sizes, Journal of Cryptology 14 (2001), 255-293.
[46] Martin Kiaer, A Microsoft PKI Quick Guide, http://www.windowsecurity.com/articles/, May 09, 2007.
[47] R.C. Merkle, "Secure communication over insecure channels", Communications of the ACM, 21(4):294-299, 1978.
[48] Milan Marković, "Infrastruktura sistema sa tajnim i javnim ključevima", Zbornik radova VJINFO'2001, april 2001, Beograd.
[49] Bogdan Brkić, "Infrastruktura sistema sa javnim ključevima (PKI) za interne korisnike u lokalnoj računarskoj mreži", diplomski rad, ETF, Banja Luka.
[50] Saša Mrdović, "Izgradnja infrastrukture javnih ključeva (PKI)", magistarski rad, ETF, Sarajevo.
[51] Brian Komar with Microsoft PKI team, Microsoft Windows server 2003 PKI and Certificate Security, Microsoft Press A Division of Microsoft Corporation One Microsoft Way Redmond, Washington, 2004.

CIP - Каталогизација у публикацији
Народна библиотека Србије, Београд

004.056.55
004.738.5:339

КОРАЋ, Вања, 1976-
Infrastruktura sa javnim ključevima u funkciji zaštite informacionog toka i elektronskog poslovanja / Vanja Korać. - Beograd : Centar za nove tehologije Viminacium : Arheološki institut = Belgrade : Center for new technology Viminacium : Archaeological Institute, 2010 (Beograd : Digital Art). - 99 str. : ilustr. ; 28 cm. - (Arheologija i prirodne nauke. Posebna izdanja, ISSN 1820-6492 ; 5)

Tekst štampan dvostubačno. - Tiraž 500. - Napomene i bibliografske reference uz tekst. - Abstract. - Bibliografija: str. [102-103].

ISBN 978-86-87271-21-0 (CNTV)

a) Криптологија b) Електронско пословање - Заштита
COBISS.SR-ID 176732940