



UNIVERZITET SINGIDUNUM
DEPARTMAN ZA POSLEDIPLOMSKE STUDIJE

MASTER STUDIJE

STUDIJSKI PROGRAM: INTERNET TEHNOLOGIJE I POSLOVNI SISTEMI

MASTER RAD

PRELAZAK SWIFT MREŽE NA INFRASTRUKTURU SA JAVNIM KLJUČEM

Mentor:

Prof. dr Mladen Veinović

Student:

Vladimir Stakić 66/2006

Beograd, 2008.

PRELAZAK SWIFT MREŽE NA INFRASTRUKTURU SA JAVNIM KLJUČEM

Sažetak

E-bankarstvo je proizvod i upotreba velikog broja tehnoloških i naučnih rešenja. SWIFT mreža je primer uspešnog proizvoda koji to potvrđuje. Bez adekvatne zaštite u svim segmentima procesa jedne transakcije ideja svetske finansijske mreže SWIFT ne bi nikad zaživela i trajala već 35 godina. SWIFT mreža je danas, krajem 2008. godine, ušla u završnu fazu prelaska na infrastrukturu sa javnim ključem, a već početkom sledeće godine planirano je potpuno gašenje sistema rada preko bilateralne razmene ključeva. Jedna ovako složena promena tražila je precizno planiranje i striktnu implementaciju.

TRANSITION OF THE SWIFT NETWORK TO THE PUBLIC KEY INFRASTRUCTURE

Abstract

E-banking is the product and utilization of numerous technological and scientific solutions. SWIFTNet is an example of the good product that verifies the above statement. Without an adequate protection in all process segments of one transaction, an idea of SWIFT, as the world financial network, would never become reality and last for 35 years already. Today, at the end of 2008, SWIFTNet have entered in the final phase of the transition to the public key infrastructure, and at the beginning of the next year the old bilateral key exchange system is scheduled for complete shutdown. Behind this highly complex transition is precise scheduling and strict implementation.

SADRŽAJ

1. Uvodna razmatranja	1
2. Pregled literature	3
2.1. Kratak istorijat protokola i Interneta.	3
2.2. TCP/IP skup protokola	4
2.2.1. Uvod	4
2.2.2. Slojevi	4
2.2.3. Internet protokol (IP).	5
2.2.4. Protokol za kontrolu prenosa (TCP)	6
2.3. HTTP i Web	6
2.3.1. HTTP	6
2.3.2. Web	8
2.3.2.1. Pretraživači.	8
2.3.2.2. Razlozi za popularnost Weba.	8
2.3.2.3. Mreža (Web) računara	9
2.3.2.4. Trendovi u budućnosti	9
2.4. SSL protokoli.	10
2.5. Savremene računarske mreže	12
2.5.1. Istorijat koncepta	12
2.5.2. Vrste mreža	12
2.5.2.1. PAN	12
2.5.2.2. LAN	13
2.5.2.3. CAN	13
2.5.2.4. MAN	13
2.5.2.5. WAN	13
2.5.2.6. Internetwork	14
2.5.2.7. Intranet	14
2.5.2.8. Extranet	14
2.5.3. Moderne mreže	14
2.5.3.1. Ethernet (IEEE 802.3).	15
2.5.3.2. WI-FI (802.11x).	16
2.5.3.3. Bluetooth (802.15.1)	16

2.6. E-poslovanje i Internet	16
2.6.1. Istorijat i definisanje e-poslovanja	17
2.6.2. Podela prema tipu učesnika na tržištu.	18
2.6.3. E-bankarstvo	20
2.7. SWIFT	21
2.7.1. Primer u praksi	23
2.8. Zaštita u računarskim mrežama	24
2.8.1. Kriptografija	25
2.8.1.1. Osnovni termini i definicije.	25
2.8.1.2. Simetrični kriptografski algoritmi	26
2.8.1.3. Asimetrična kriptografija (sa javnim ključem)	28
2.8.1.4. Izbor algoritma	30
2.9. Upravljanje ključevima	30
2.9.1. Definicija	30
2.9.2. Funkcije upravljanja ključevima.	31
2.9.2.1. Generisanje ključa.	31
2.9.2.2. Distribucija.	31
2.9.2.3. Instalacija	31
2.9.2.4. Čuvanje.	31
2.9.2.5. Promena	32
2.9.2.6. Kontrola	32
2.9.2.7. Odbacivanje	32
2.9.3. Moderno upravljanje ključevima	32
2.9.4. Principi upravljanja ključem.	33
2.10. Infrastruktura sa javnim ključevima (PKI)	34
2.10.1. Pojam PKI	34
2.10.2. Sastav PKI	35
2.11. PKI SMART kartice.	36
2.11.1. SMART kartice	36
2.11.1.1. Memorija	36
2.11.1.2. Procesor	37
2.11.1.3. Vrste kartica	37
2.11.1.4. Upotreba SMART kartica	38
2.11.2. PKI i SMART kartice	39
2.12. Inteligentna obrada podataka.	39
2.12.1. Poreklo	40
2.12.2. Poslovna primena.	40
2.13. Zaštita u E-bankarstvu	41
2.13.1. Upotrebljiva sigurnost	41

3. Analiza starog i novog sistema SWIFTNet-a.....43

3.1. Stari sistemi – BKE, MAC i SCR	43
3.2. Opis SWIFTNet PKI	43
3.2.1. Uvod.....	43
3.2.2. Vrednosti za klijente.....	44
3.2.2.1. Uopšteno	44
3.2.2.2. Poverenje	44
3.2.2.3. Garancije	45
3.2.3. Rigorozan PKI.	46
3.2.4. Osobine i funkcije.	47
3.2.4.1. PKI komponenta za klijente.	47
3.2.4.2. Komponente PKI SWIFT-a	48
3.2.4.3. Ključevi.	49
3.2.4.4. Digitalni sertifikati	50
3.2.5. Sertifikaciono telo.....	51
3.2.5.1. Registracija.....	51
3.2.5.2. Ko dobija sertifikaciju.....	51
3.2.5.3. Priprema za sertifikaciju.....	52
3.2.5.4. Sertifikacija.....	52
3.2.5.5. Priprema za povraćaj	52
3.2.5.6. Povraćaj	52
3.2.5.7. Opoziv.....	52
3.2.5.8. Onemogućavanje.....	52
3.2.5.9. Oflajn zahtevi.....	53
3.2.6. Glosar.....	53
3.3. Poređenje starog i novog sistema.....	55
3.3.1. Šta je promenjeno?.....	55
3.3.1.1. Nova aplikacija	56
3.3.1.2. Zaštita sigurnosnog ključa.....	56
3.3.2. Faze prelaska na novi sistem.....	56
3.3.3. Prednosti prelaska na novi sistem	58

4. Zaključna razmatranja 59

5. Literatura 61

Popis slika i tabela

Slike

Slika 1. – Vremenska linija bitnih događaja vezanih za Internet	3
Slika 2. – Slojevi TCP/IP skupa protokola – četvoroslojni model	5
Slika 3. – Položaj bezbednosnog sloja u odnosu na ostale protokole.....	10
Slika 4. – Prosti oblici e-poslovanja	19
Slika 5. – Sistem plaćanja RTGS (SWIFT kao WAN).....	24
Slika 6. – Šifrovanje i dešifrovanje sa ograničenim algoritmima	26
Slika 7. – Šifrovanje i dešifrovanje sa ključem.....	26
Slika 8. – Rad šifre niza.	27
Slika 9. – SWIFT portfolio komunikacionih servisa	45
Slika 10. – Interakcija klijenta sa SWIFTNet PKI serverima.....	48
Slika 11. – Sertifikaciono telo	52
Slika 12. – Paralelni prikaz rada BKE (ranije) i PKI (danas).....	56
Slika 13. – Vremenska linija i prekretnice za klijente SWIFTNet-a	57

Tabele

Tabela 1. – Glosar termina korišćenih za opis SWIFTNet PKI.....	54
---	----

1. Uvodna razmatranja

Internet je doneo veliku promenu u našem svetu. Razvojem tehnologije i nauke stvoreni su neki izuzetno komplikovani sistemi kao što je to svetska mreža SWIFT. Mreža je tokom svog višedecenijskog poslovanja doživela veliki broj promena i prilagođavanja novim i boljim standardima radi podizanja funkcionalnosti i sigurnosti poslovanja. Sve te promene su se rukovodile potrebom da se održi visok nivo sigurnosti u svetskom okruženju, da se smanje troškovi poslovanja, da se pojednostavi rad sistema za krajnje korisnike, kao i da se obezbedi višegodišnja sigurnost u radu.

Jasno je da sistemi, bilo da su oni veliki ili mali, imaju potrebu stalnog poboljšavanja i praćenja najnovijih svetskih tokova. Bilo kakav propust u nekim od njih bi doveo do velikih finansijskih gubitaka samog sistema i, u nekim slučajevima, i klijenata tog sistema. Na primer, sistemski propust u svetskoj mreži SWIFT mogao bi da ima nesagledive posledice za svetsku ekonomiju i finansije.

Iz navedenog razmatranja problem istraživanja ove studije može da se formuliše na sledeći način:

Prepoznati i oceniti faktore koji su sastavni delovi velikog svetskog sistema i način na koji je moguće poboljšavati sistem bez prekidanja njegovog funkcionisanja.

Na osnovu prethodnog razmatranja problema, stvorena su tri pitanja za istraživanje.

Pitanja:

1. Šta je promenjeno prilikom prelaska sa starog na novi sistem rada SWIFTNet-a?
2. Kako je izvršena promena sa starog na novi sistem rada u sistemu veličine SWIFTNet-a?
3. Koje su stvarne prednosti prelaska na novi sistem rada?

Polje istraživanja navedenih pitanja je široko i stoga postoji nekoliko ograničenja kako bi istraživanje moglo da se ostvari.

Prvo, svaki od naslova u pregledu literature se koristi ili je vezan za rad SWIFT sistema, i time dostojan da bude nezavisni istraživački rad. Pošto obimnost svake teme

prevazilazi raspoloživi prostor i resurse, akcenat je stavljen na PKI, dok će se ostale teme pojavljivati isključivo u kontekstu njihove implementacije.

Drugo, usled obimnosti svake teme ponaosob, analiza je ograničena samo na informacije koje su ekstremno bitne za cilj istraživanja.

Treće, jedna od specifičnosti SWIFT mreže je ograničena količina elektronskih i papiroloških podataka koja se može naći o funkcionisanja bilo kog njenog segmenta. Ovo jeste ograničenje za istraživanje, ali je i jedna od bitnih karakteristika SWIFT-a, jednog od najsigurnijih svetskih sistema sa višedecenijskom tradicijom u radu.

Istraživanje je bazirano na materijalu ograničenog karaktera, pretežno u formi prezentacija koje su prikazivane na kongresima i seminarima pod okriljem organizacije SWIFT. Takođe, dragocene informacije su pribavljene u konsultacijama sa stručnjacima iz oblasti međunarodnog platnog prometa koji su specijalizovani za aspekt elektronskog poslovanja preko SWIFT mreže.

Ovaj rad je podeljen u četiri poglavlja. U prvom poglavlju predstavljena je pozadina izabranog područja istraživanja zajedno sa razmatranjem problema i pitanjima za istraživanje. U drugom poglavlju, biće predstavljeno istraživanje literature i prethodna istraživanja koja su povezana sa temom. U trećem poglavlju su dati opis podataka istraživanja, razmatranja i rezultati. Četvrto poglavlje je posvećeno završnom razmatranju i zaključku.

2. Pregled literature

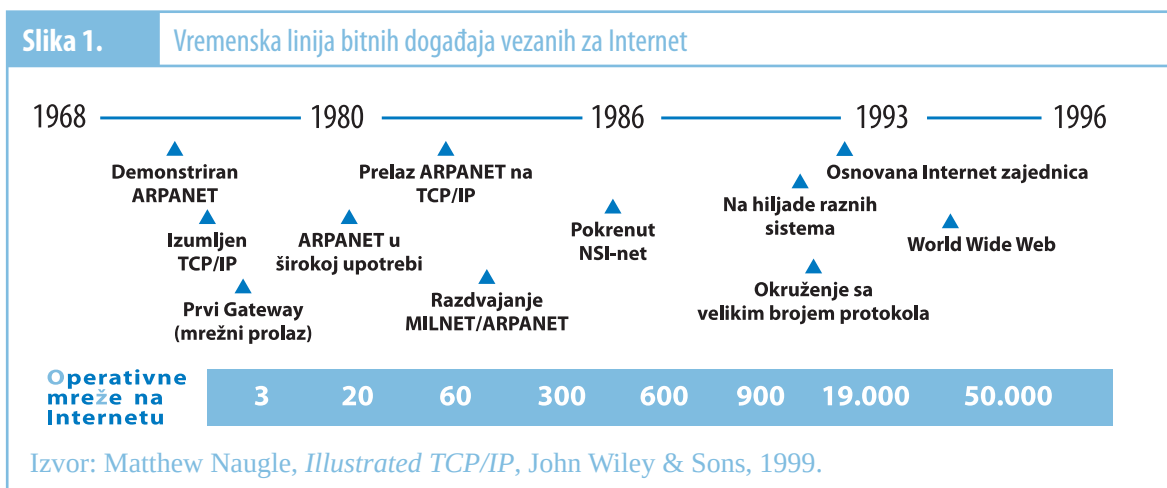
2.1. Kratak istorijat protokola i Interneta

Komunikacioni protokol je skup standarda, definisan da omogući računarima međusobno povezivanje radi razmene informacija sa što manjim brojem grešaka. Opšteprihvaćeni protokol za standardizaciju računarskih komunikacija je sedmoslojni skup hardverskih i softverskih preporuka, poznat pod imenom OSI (ISO/OSI¹) model.²

Razvoj računarske tehnike i razvoj protokola uslovio je pojavu Interneta. Internet je nastao od decentralizovane mreže, poznate pod nazivom ARPANET, koju je 1969. godine stvorilo Ministarstvo odbrane SAD radi osiguravanja komunikacija u slučaju atomskog napada. Kasnije se sa ARPANET-a prešlo na skup TCP/IP protokola za međusobnu komunikaciju.

Glavni oslonac Interneta čini okosnica sastavljena od komunikacionih linija za prenos podataka velikim brzinama između značajnih čvorova i glavnih računara. Jedan (ili više) čvorova Interneta može da se isključi bez ugrožavanja Interneta kao celine ili ugrožavanja komunikacija na Internetu, jer ga ne kontroliše samo jedna mreža ili računar. To je inače i bio osnovni cilj prilikom stvaranja ARPANET-a.

Naredna slika ilustruje važnije događaje u razvoju protokola i Interneta.



¹ Referentni model Međunarodne organizacije za standardizaciju/međupovezivanje otvorenih sistema (eng. *International Organization for Standardization/Open System Interconnection*), koji deli komunikaciju između računara u sedam protokolskih slojeva.

² Microsoft, *Računarski rečnik*, Prevod petog izdanja, CET, Beograd, 2003.

2.2. TCP/IP skup protokola

2.2.1. Uvod

„Skup pravila koja omogućavaju različitim vrstama računara i računarskih mreža na Internetu da međusobno komuniciraju“³

Internet i WWW su bazirani na TCP/IP. Termin „TCP/IP“ se ne odnosi samo na TCP i IP, već takođe obuhvata druge protokole, aplikacije i čak mrežne medije. Ovi protokoli obuhvataju UDP, ARP i ICMP. Ove aplikacije obuhvataju Telnet, FTP, Secure Shell, NFS, Web pretraživače i servere, a mnoge stavke zajedno se nazivaju Web servisi.⁴

TCP/IP skup protokola omogućava računarima svih veličina (namena), različitih proizvođača širom sveta, sa različitim operativnim sistemima (različitih generacija), da komuniciraju. To je njegova ključna karakteristika. TCP/IP je pravi otvoreni sistem, u smislu da su definicija protokola i njegove brojne implementacije besplatno javno dostupne. Tehnička dokumentacija za TCP/IP je poznata pod nazivom RFC. RFC dokumenta definišu funkcije procesiranja ovog protokola. Ona se izdaju pod kontrolom Odbora za arhitekturu Interneta. Izvori, od kojih se mogu dobiti ova dokumenta su APNIC za Aziju, RIPE za Evropu i INTERNIC za SAD.

2.2.2. Slojevi

Za objašnjavanje funkcionisanja TCP/IP skupa protokola koriste se različiti modeli. Zajedničko za sve njih je da su bazirani na prikazu rada skupa protokola preko slojeva – nivoa na kojem pojedinačni protokoli rade. Standardno se koristi sedmoslojni OSI prikaz. Radi isticanja gornjih slojeva protokola koji su predmet ovog rada, korišćen je četvoroslojni model.

Elementi četvoroslojnog modela su:

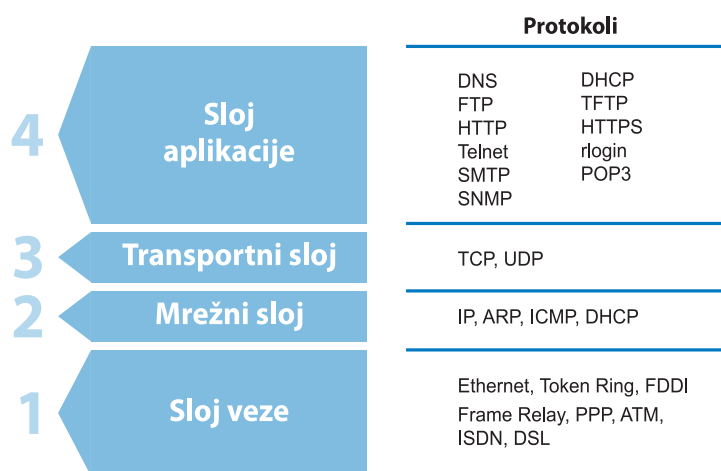
- Sloj veze – On je sastavljen od LAN i WAN tehnologije. Standardno, LAN je ograničen na specifično područje, obično na kancelariju. S druge strane, bilo koja mreža koja koristi rutere i javne mrežne veze potpada pod WAN. On se sastoji od drajvera za uređaj u operativnom sistemu i odgovarajuće mrežne kartice u računaru. Ove dve komponente pokrivaju hardversku, fizičku vezu računara sa mrežnim kablom.
- Mrežni sloj – Osnovna namena mrežnog sloja je utvrđivanje najbolje putanje i usmeravanje paketa za slanje. U ovom sloju se nalazi IP (Internet protokol). On predstavlja usko grlo pešćanog sata jer se iznad njega nalaze višestruki protokoli višeg sloja, dok se istovremeno ispod njega nalaze višestruki protokoli nižeg sloja.

³ Microsoft, *Encarta Encyclopedia Deluxe 2004*.

⁴ *The Internet Encyclopedia*, Vol.3, John Wiley & Sons, New Jersey, 2004., str. 424.

- **Transportni sloj** – Ovaj sloj obezbeđuje tok podataka između dva računara na mreži i obezbeđuje odgovarajuću uslugu za aplikativni sloj koji je iznad njega. U TCP/IP skupu protokola, na ovom sloju su dva potpuno različita protokola: TCP (Transmission Control Protocol) i UDP (User Datagram Protocol).
- **Sloj Aplikacije** – Ovaj sloj je zadužen je za detalje karakteristične za konkretnu aplikaciju. Primeri u okviru TCP/IP skupa za ovaj nivo su: HTTP, FTP, SMTP, SNMP, itd.

Slika 2. Slojevi TCP/IP skupa protokola – četvoroslojni model



Izvor: Matthew Naugle, *Illustrated TCP/IP*, John Wiley & Sons, 1999.

2.2.3. Internet protokol (IP)

IP⁵ isporučuje niz bajtova od matičnog računara A do odredišnog računara B, čak i kada su računari na različitim mrežama, ili na značajnoj geografskoj udaljenosti. Gornji sloj daje niz bajtova i odredište za IP sloj. IP sloj formira IP datagram od date sekvence. IP datagram se sastoji od IP zaglavlja, nakon kojih slede podaci transportnog sloja.

Softver IP sloja utvrđuje putanje koje paketi moraju da pređu od tačke A, preko različitih posredničkih čvorova da bi na kraju stigli do tačke B. Svaki paket putuje nezavisno čak i kada matični računar A želi da pošalje nekoliko paketa do tačke B – isporuka svakog paketa se pravi nezavisno od prethodnih. Putanje kojim prolazi svaki paket mogu da se promene. IP sloj je projektovan s namerom da se ne bavi sa garantovanom isporukom (npr., paketi mogu da budu izgubljeni ili duplirani), već umesto toga on je sistem za „najbolji pokušaj“.

Operativni sistem, prilikom podizanja, dodeljuje jedinstvenu 32-bitni numeričku identifikaciju poznatu kao njegovu IP adresu za svaku NIC koja se nalazi u matičnom sistemu. Ne

⁵ RFC 791.

postoji čvrsta veza između Ethernet adrese i IP adrese. IP adresa se dobija bilo preuzimanjem iz konfiguracionog fajla ili preko DHCP. IP adrese se pažljivo kontrolišu širom sveta. IANA⁶ dodeljuje takozvane javne IP adrese organizacijama i pojedincima na zahtev.

2.2.4. Protokol za kontrolu prenosa (TCP)

TCP⁷ nudi klijentskom procesu vezu sa serverskim procesom. Ovu vezu potrebno je uspostavljati prema potrebi. Nakon što je ova veza uspostavljena, TCP protokol garantuje ispravnu (prema sadržaju i redosledu) isporuku podataka. TCP šalje svoj sadržaj poruke preko IP sloja i može da otkrije i da se oporavi od grešaka. TCP, međutim, ne garantuje brzinu isporuke, čak i kada nudi kontrolu zakrčenosti.

Brojeve portova koristi transportni sloj za mnogostruku komunikaciju između nekoliko parova procesa. Svakoj poruci, ovaj sloj dodaje adrese koje se zovu brojevi portova. Stoga, veza je jedinstveno identifikovana sa četiri broja: izvorne i odredišne IP adrese, i izvornog i odredišnog broja porta. IP adrese obezbeđuje IP sloj.

TCP zahteva da svaki segment uključuje potvrdu prethodno primljenog segmenta u suprotnom smeru. TCP je klizni nadzorni protokol koji ima vremensku kontrolu i ponovna slanja. Ako pošiljalac ne primi potvrdu unutar perioda vremenske kontrole, on ponovo šalje segment. Potvrde su nakačene na podatke odgovora.

TCP poruke, nazvane segmenti, se šalju kao jedan ili više IP datagrama. TCP zaglavlje dolazi nakon IP zaglavlja. Ono obezbeđuje informacije specifične za TCP protokol.

2.3. HTTP i Web

2.3.1. HTTP

HTTP⁸ je jezgro World Wide Web-a. Web pretraživači na korisničkim računarima i Web serveri negde na Internetu međusobno komuniciraju preko HTTP-a koristeći TCP obično na portu 80.

HTTPS⁹ je nastao uvođenjem metoda šifrovanja (kao što je to SSL) radi kodiranja brojeva kreditnih kartica i drugih informacija. Njegova osnovna namena je da se osujete potencijalni kradljivci ovih informacija.

⁶ www.iana.org

⁷ RFC 793, RFC 3168

⁸ RFC 2616, 1999

⁹ RFC 2660, 1999

Web pretraživač prikazuje fajl markerskog teksta sa ugrađenim komandama praćenih sintaksičkim zahtevima HTML-a. Postoji nekoliko načina za prizivanje ovih komandi. Najrasprostranjeniji je klik na miša. Većina linkova na klik, prikazanih preko Web pretraživača, su takozvani linkovi koji sadrže URL sa vidljivim delom teksta ili grafike.

Zahtev i odgovor se prave shodno HTTP formatu poruke, koja je niz linija teksta. Prva linija identifikuje poruku kao zahtev ili odgovor. Linije u nastavku su poznate kao linije zaglavlja sve do dolaska do prazne linije. Nakon prazne linije nalaze se linije koje čine “telo entiteta.” Linije zaglavlja imaju levu stranu koja označava različite parametre odvojene od desne strane koja obezbeđuje vrednosti sa dvotačkom.

Linija za zahtev ima tri komponente:

- metod (može biti GET, POST ili HEAD),
- URL, i
- verziju HTTP (bilo 1.0 ili 1.1)

Linija za odgovor takođe ima tri komponente:

- HTTP - verzija,
- statusni kod (kao čuveni 404)
- i frazu (kao što su Not Found, OK ili Bad Request).

Na primer, URL <http://www.singidunum.ac.rs/sadrzaj> naznačava pretraživaču da treba da koristi HTTP protokol da preuzme stranu, s tim da se ta strana nalazi na računaru „singidunum.ac.yu“ i da se ta strana zove „sadrzaj“. Pored toga, „ac“ označava skraćenicu za akademsku mrežu, a „rs“ označava aktivni domen za Srbiju. Da je umesto „ac.rs“ stajalo „com“, onda bi to označavalo da sajt postoji iz komercijalnih razloga ili radi ostvarivanja profita. Postoje i druge skraćenice, kao što su „edu“ za WEB sajtove koje su postavile obrazovne institucije, „org“ koji označava neprofitne organizacije, itd.

Web serveri koji zahtevaju autentifikaciju korisnika šalju zaglavlje „WWW Authenticate“. Web klijent, u tom slučaju, zahteva upis korisničkog imena i lozinke, i šalje ovu informaciju u svakoj od narednih poruka zahteva serveru.

Kolačići¹⁰ upotpunjuju sesiju sa HTTP zahtevima i odgovorima. Oni se smeštaju na klijentski sistem. Kada se korisnik vrati na isto mesto na Web-u, pretraživač vraća kopiju kolačića na server. Podaci kolačića se koriste za identifikaciju korisnika, da saopšte serveru da pošalje namensku verziju Web stranice, za podnošenje informacija o obračunu korisnika i za druge administrativne namene.

¹⁰ RFC 2965

2.3.2. Web

World Wide Web, skraćeno Web, je skup međusobno povezanih hipertekstualnih dokumenata koji se nalaze na HTTP serverima po čitavom svetu. Web dokumenti poznati i kao Web strane, napisani su u HTML jeziku, identifikuju se preko URL-a, prenose se sa čvora na čvor do krajnjeg korisnika pod kontrolom HTTP protokola. Web je razvio Timothy Berners-Lee 1989. godine za Evropski savet za nuklearna istraživanja.

Prednost hiperteksta je da u hipertekstualnom dokumentu, ako se žele dodatne informacije o određenoj pomenutoj temi, obično je dovoljno „kliknuti na nju“ da bi se pročitali dodatni detalji. U stvari, dokumenti mogu i često su povezani sa drugim dokumentima od potpuno različitih autora - poput fusnota, ali se referentni dokument dobija trenutno.

2.3.2.1. Pretraživači

Za pritup Web-u potreban je program koji se zove pretraživač. Pretraživač čita dokumenta i može da prihvata dokumenta iz drugih izvora. Provajderi informacija postavljaju hipermedijalne servere sa kojih pretraživači mogu da uzmu dokumenta. Hipermedija je superskup hiperteksta – to je bilo koji medijum sa pointerima na drugi medijum. To znači da pretraživači možda neće prikazati tekstualni fajl, ali mogu da prikažu ilustracije, puste zvuk ili animacije.

Pretraživači, pored navedenog, mogu da pristupe fajlovima preko FTP, NNTP, gopher-a i drugih. Povrh svega, ako server ima mogućnosti pretrage, pretraživači će dozvoliti pretrage dokumenata i baza podataka.

2.3.2.2. Razlozi za popularnost Weba

Web je počeo da bude popularan izvor nakon 1993. godine, kada je prvi široko rasprostranjeni pretraživač omogućio pristup različitim informacijama na Internetu. Vremenom je sadržaj ponude na mreži proširen, pa je ceo sistem iz zabave ubrzo prerastao u potrebu. Dodatni razlog za veliku popularnost Weba je multimedijalni sadržaj. Mogućnost da korisnici (preko pretraživača i drugih specijalizovanih aplikacija) čitaju tekstove, gledaju slike, posmatraju animacije, slušaju muziku i čak, u novije vreme, da istražuju interaktivna virtuelna okruženja uvela je Web u sastavni deo života desetina miliona ljudi širom sveta.

Samo mali procenat informacija na Webu je ograničen pretplatnicima ili drugim ovlašćenim korisnicima. Većina Web strana su raspoložive svakome, pod uslovom da ta osoba ima pristup računaru koji može da se poveže na Internet.

Web je postao i velika tržnica za mnoge kompanije koje prodaju proizvode i usluge, kao i veliki forum za ljude koji razmenjuju mišljenja i informacije.

2.3.2.3. Mreža (Web) računara

Kompletnu komunikaciju na Webu nose skupovi računara, koji su međusobno povezani preko računarske mreže. Web tehnologija može da se koristi širom intranet-a (mreže unutar kompanije ili organizacije) ili širom globalnog Interneta¹¹.

Kao i sva ostala komunikacija između računara, računari koji su uključeni na Web koriste dva tipa softvera: klijent i server (poznatiji i pod nazivom klijent/server arhitektura). Da bi stavili na raspolaganje informaciju, računar pokreće serverski program. Za preuzimanje i prikazivanje informacije sa servera, računar pokreće klijentski program. Klijent kontaktira server da zahteva informaciju, server odgovara tako što šalje kopiju zahtevane informacije. Da bi informacija imala bilo kakvo značenje, klijentski i serverski programi moraju da postupaju po komunikacionom protokolu, skupu pravila koji definiše formu i značenje svake moguće poruke. Upravo iz ovog razloga je razvoj protokola omogućio razvoj Web-a.

U principu svaki računar može da radi kao klijent ili server. U praksi, međutim, veliki, moćni računari se obično biraju da pokreću serverski softver, a mali stoni računari (npr. PC) su dovoljni da pokreću klijentski softver. Moćni računari su izabrani za serverski softver zato što moraju da budu u mogućnosti da barataju zahtevima za informacijama miliona osoba, a da pritom to rade dovoljno brzo da te osobe ne iskuse dugo čekanje. PC računar, s druge strane, koristi jedna osoba da otvori Web sajt. Nakon što korisnik pošalje zahtev, on čeka da se tražena informacija prikaže. Stoga, klijentski programi koji rade na pojedinačnom računaru, barataju samo sa jednom aktivnošću u trenutku. Server, međutim, mora da istovremeno barata zahtevima velikog broja klijenata (nekada su u pitanju i milioni zahteva).

2.3.2.4. Trendovi u budućnosti

Količina informacija na Webu nastavlja brzo da raste, kao i broj korisnika širom sveta i količina onlajn poslovanja. U mnogim poslovima, Web je zamenio tradicionalno naručivanje kataloga. Pored toga, ljudi nastavljaju da proširuju i poboljšavaju Web tehnologiju. Nekoliko istraživačkih inicijativa su na putu da stvore nove metode koje pretražuju Web zarad informacija, nove metode za ograničavanje pristupa intelektualnoj svojini i nove tehnologije koje će dozvoliti emitovanje Web-a nalik klasičnoj televiziji.

Iako većina Web strana koristi HTML jezik, predložene su nove ekstenzije i alternativne tehnologije. Na primer, XML je postao popularan za B2B komunikaciju. Za razliku od HTML, gde je unapred definisano značenje tagova, XML omogućava kompanijama da ga koriste da definišu sopstvene tagove. Na primer, izdavač i knjižara mogu da definišu sopstvene tagove za informacije o autorima, naslovima i drugim informacijama koje su im

¹¹ Microsoft, *Encarta Encyclopedia Deluxe 2004*.

potrebne za poslovnu komunikaciju. Takođe, proizvođač automobila i prodavac mogu da definišu jedinstvene tagove koji označavaju marku, boju, opremu vozila. XML definicije imaju značenje isključivo obuhvaćenim stranama. Stoga, softver proizvođača automobila neće razumeti tag za autora kod izdavača, i obrnuto.

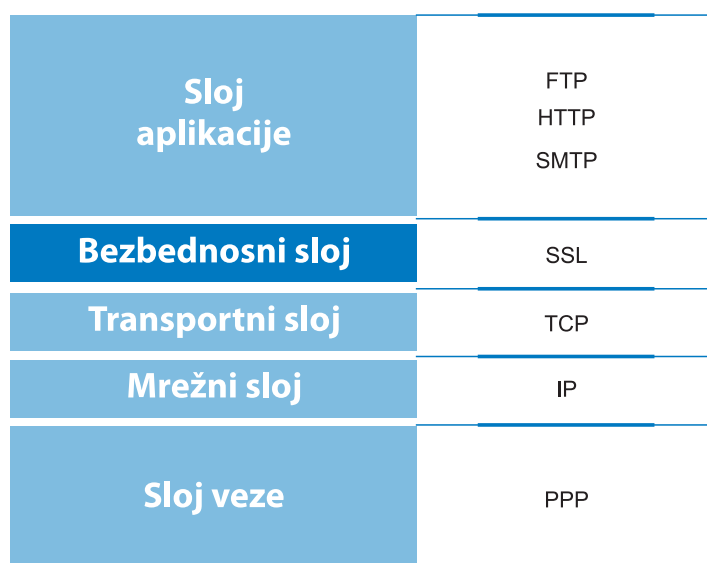
Javljaju se takođe i druge forme, kao što je to WML. On je projektovan za korišćenje sa malim bežičnim uređajima, kao što su mobilni telefoni sa mogućnošću prikazivanja Web sadržaja. Još jedna tehnologija, za koju se očekuje da će dobiti na važnosti, je CDN ili preslikavanje (eng. *mirroring*). On se sastoji od višestrukih sajtova širom sveta koji sadrže identičnu informaciju. Kada korisnik zahteva stranu, CDN preusmerava zahtev najbližoj kopiji. Sa korisničkog aspekta, rezultat korišćenja CDN je brži odgovor.

2.4. SSL protokoli

SSL protokol je razvila kompanija Netscape Communication Corporation 1995. godine, za slanje privatnih dokumenata preko Interneta, dok je S-HTTP projektovan da šalje pojedinačne poruke i takođe koristi metod šifrovanja.

Osnovna ideja koja stoji iza primene SSL protokola je ubacivanje novog sloja između komunikacionog softvera HTTP i TCP, koji će šifrovati podatke na način gde je dešifrovanje moguće samo kod autorizovnog primača. Na primer, kada klijent pošalje šifrovane podatke na server, taj server jedini poseduje ključ za dešifrovanje podataka. Da bi ovaj sistem funkcionisao, i klijent i server moraju da imaju uključen SSL, tj. moraju da imaju SSL između aplikacije i transportnog sloja u svojim mrežnim softverima.

Slika 3. Položaj bezbednosnog sloja u odnosu na ostale protokole



Rezultat korišćenja ovog protokola je sprečavanje prisluškivanja, modifikovanja, lažnog predstavljanja (falsifikovanja) i poricanja. Prisluškivanje se sprečava simetričnim šifarskim sistemima (standardno se koristi RC4 algoritam u SSL-u). Ostale tri karakteristike se postižu asimetričnim šifarskim sistemima (uz primenu digitalnih sertifikata).

Digitalni sertifikat je obezbeđenje da softver koji se prenosi sa Interneta dolazi iz izvora sa dobrom reputacijom. Digitalni sertifikat obezbeđuje informacije o softveru – na primer o identitetu autora i datumu kada je softver registrovan kod ovlašćenog izdavaoca sertifikata (CA), ali takođe predstavlja i meru obezbeđenja od poigravanja sa datom informacijom.¹²

SSL je slojeviti protokol. Može se reći da se on sastoji iz dva sloja protokola. Na donjem nivou SSL Record Protocol je postavljen preko nekog pouzdanog transportnog protokola kao što je to TCP. SSL Record Protocol se takođe koristi da enkapsulira različite protokole višeg nivoa. Ovaj način razmene poruka je projektovan da olakša sledeće radnje:

- Autentifikuje server klijentu.
- Omogući da klijent i server izaberu kriptografske algoritme, ili šifarske ključeve, koje podržavaju obe strane.
- Opciono da autentifikuju klijenta serveru.
- Koriste tehnike šifrovanja preko javnog ključa za razmenu tajnih informacija.
- Naprave šifrovanu SSL konekciju.

Mnogi faktori utiču na stepen sigurnosti SSL protokola. Na primer, dužina ili kompleksnost ključa zajedno sa složenošću algoritma koji se koristi za šifrovanje podataka, obično ukazuju na efektivnost šifrovanja. Na primer, DES, koji je razvijen 1976. godine od strane IBM-a, koristi 56-bitova u svom ključu da promeni segmente poruke od po osam karaktera u 64-bitne segmente kodiranog teksta. NIST je 1997. godine je organizovao razvoj novog sistema šifrovanja, nazvanog AES. AES postepeno menja DES, pošto koristi jači algoritam i baziran je na 128-bitnoj enkripciji za razliku od 64-bitnog standarda koji koristi DES. Takođe, Švajcarski federalni institut za tehnologiju razvio je 90-tih godina prošlog veka standard IDEA. Banke u SAD i nekoliko zemalja u Evropi koriste standard IDEA za mnoge od svojih transakcija.

¹² Microsoft, *Računarski rečnik*, Prevod petog izdanja, CET, Beograd, 2003.

2.5. Savremene računarske mreže

„Grupa računara i pratećih uređaja povezanih komunikacionom opremom.”¹³

U proteklih 40 godina računarske mreže su dramatično način na koji radimo, na koji se igramo i na koji komuniciramo. Sada imamo raspoložive informacije i ličnu komunikaciju na način na koji se nikad nije verovalo da će biti moguć, a to sve dodirnom prsta. Tehnologija je evoluirala i integrisala se u svaku oblast naših života. Većina ljudi nije čak ni svesna u kojoj se meri njihov stil života oslanja na računarske mreže. Televizija, mobilni i fiksni telefoni, Internet, itd. koji dopiru do naših domova, ne bi mogli da egzistiraju bez računarskih mreža.

2.5.1. Istorijat koncepta

Oxford American Dictionary u osnovi definiše reč mrežu kao „Skup ukrštenih horizontalnih i vertikalnih linija; Grupa međusobno povezanih ljudi ili stvari”¹⁴.

Kao jedan od najjednostavnijih koncepata koje je čovek razvio, mreža je infrastruktura koja omogućava efikasno povezivanje više tačaka. Ovaj termin nije iskovan pojavom računara, već pre nastankom vremena. Neki od poznatih primera mreža pre digitalne ere su međusobno povezani kanali za navodnjavanje, ukršteni sistemi puteva (autoputeva) i komunalna infrastruktura. Uprkos tome što se ovi sistemi obično ne nazivaju mrežama, svi ovi sistemi mogu da se definišu kao mreže i odlični su primeri koncepta koji nije nov, ali je iznenada naša nove primene u proteklih četiri do šest decenija.

2.5.2. Vrste mreža

2.5.2.1. PAN

PAN je računarska mreža koja se koristi za komunikaciju između kompjuterskih uređaja koji su međusobno blizu. Domet PAN je obično nekoliko metara. PAN može da se koristi za komunikaciju između personalnih uređaja ili za povezivanje za viši nivo mreže i Interneta.

PAN može da se poveže USB ili FireWire kablovima. Wireless PAN (WPAN) može da se napravi preko mrežnih tehnologija kao što su IrDA i Bluetooth.

Bluetooth PAN se takođe naziva piconet (*piconet*) i sastoji se od 8 aktivnih uređaja između kojih je postavljen odnos *master-slave*. Veliki broj uređaja može da se poveže u

¹³ Microsoft, *Računarski rečnik*, Prevod petog izdanja, CET, Beograd, 2003.

¹⁴ „An arrangement of intersecting horizontal and vertical lines; A group of interconnected people or things”

režimu mirovanja. Prvi Bluetooth uređaj je *master*, a svi ostali drugi uređaji su *slave* koji komuniciraju sa *masterom*. Pikonet standardno ima domet od 10 metara, iako je moguće postignuti i domet od 100 metara u idealnim uslovima.

2.5.2.2. LAN

LAN je računarska mreža koja je ograničena na relativno malo fizičko područje kao što su prostorija, jedna zgrada, brod ili avion. LAN se ponekad naziva mreža jedne lokacije.

Definišuće karakteristike LAN mreža, nasuprot WAN mrežama, su obično veća brzina protoka podataka, manje geografsko područje i velika potreba za iznajmljenim telekomunikacionim linijama.

2.5.2.3. CAN

CAN je računarska mreža koja je sačinjena od međusobnog povezivanja lokalnih računarskih mreža (LAN), a ograničena je na jednu geografsku lokaciju (privatnu lokaciju) kao što su industrijski kompleks ili univerzitet. CAN mreža je veća od LAN mreže ali manja od WAN mreže.

2.5.2.4. MAN

MAN je gradska računarska mreža velike brzine koja može da obuhvata jednu računarsku mrežu ili više lokalnih računarskih mreža i telekomunikacionu opremu, kao što su mikrotalasne i satelitske relejne stanice. Manja je od regionalne računarske mreže, ali obično radi na većoj brzini.

MAN mreža pokriva područje od 5 do 50 km. U njenoj izgradnji učestvuju ISP-ovi koji pružaju usluge korisnicima. U segmentu bežične mreže brzina je preko 1Mbps, dok je u žičanoj mreži reda veličine 100 ili 1.000Mbps.

2.5.2.5. WAN

WAN je regionalna računarska mreža koja povezuje geografski udaljena područja. Neformalno, WAN je mreža koja koristi rutere i komunikacionu vezu.¹⁵ Razlika WAN u odnosu na PAN, LAN i CAN je što pokriva široka područja.

Najveći i najpoznatiji primer WAN mreže je Internet.

WAN se koristi da međusobno poveže LAN i druge vrste mreža tako da korisnici i računari sa jedne lokacije mogu da komuniciraju sa korisnicima i računarima sa druge

¹⁵ Groth, David, Skandier, Toby, *Network+ Study guide, Fourth Edition*, Sybex, Inc., 2005.

lokacije. Veliki broj WAN mreža su napravljene za određenu organizaciju i privatnog su karaktera. Druge mreže, koje su oformili ISP-jevi, omogućavaju povezivanje sa LAN mreža organizacije na Internet. WAN se često pravi korišćenjem iznajmljenih linija, kao skuplje rešenje, i na jeftinije načina korišćenjem metoda komutacije kola (npr. dialup konekcija) ili komutacije paketa (npr. PVC ili SVC).

2.5.2.6. Internetwork

Mreža koju čine povezivanje dve ili više posebnih računarskih mreža ili segmenata mreža preko zajedničke tehnologije rutiranja. Rezultat tog povezivanja se naziva *internetwork*, često skraćivan na internet.

Najpoznatiji primer *internetworkinga* je Internet, mreže mreža baziranih na mnogim hardverskim tehnologijama, ali unificiranih preko standarda za *internetwork* protokol, pod imenom grupa internet protokola (TCP/IP). Mrežni elementi korišćeni za povezivanje pojedinačnih mreža su poznati kao ruteri.

2.5.2.7. Intranet

Intranet je privatna kompjuterska mreža koja koristi Internet protokole i mrežno povezivanje radi bezbedne razmene bilo kog informacionog ili operativnog sistema organizacije među njenim zaposlenima. Dobio je ime po tome što često koristi Internet (Web strane, FTP lokacije, e-pošta, ...) koji je dostupan samo unutar kompanije ili organizacije.

Internet može da se prihvati kao privatna verzija Interneta ili kao privatna nadogradnja Interneta ograničena na organizaciju. Intranet organizacije ne mora da pruža pristup Internetu. Kada je taj pristup dozvoljen, on se obično vrši preko mrežnog *gatewaya* sa podignutim *firewallom* koji štiti intranet od neovlašćenog pristupa spolja.

2.5.2.8. Extranet

Ekstranet je proširenje institucionalnog intraneta koje koristi tehnologiju WWW da olakša komunikaciju sa dobavljačima i klijentima korporacije. U kratkim crtama, ekstranet može da se razume kao intranet koji je mapiran na javni Internet ili neki drugi sistem prenosa koji nije pristupačan široj javnosti, ali kojom upravljaju više od jednog administratora kompanije.

2.5.3. Moderne mreže

U nastavku rada su opisani najrašireniji mrežni standardi.

2.5.3.1. Ethernet (IEEE 802.3)

Ethernet¹⁶ se koristi za povezivanje kompjutera i u malim kućnim i u velikim poslovnim situacijama i danas je to najrasprostranjeniji standard za računarske mreže. On često omogućava pristup internetu sa drugih standarda komunikacije na računare u domu ili na poslu. Oprema za ethernet je relativno malih dimenzija, pristupačna i može da nosi podatke velikim brzinama.

Originalna specifikacija je navodila osnovni opseg brzina od 10mbps¹⁷, dok novije tehnologije su donele brzine koje se danas kreću između 100mbps i 1000mbps. Ethernet se retko koristi van lokalnih mreža (u domovima i poslu) usled problema sa opsegom (daljinom). Instalacije za ethernet standardno mogu da rade do maksimalno par stotina metara. To ostavlja prostora drugim mrežnim infrastrukturalama da povežu računare na većim razdaljinama. Ethernet obično formira sistem koji se naziva LAN. Standard je razvila kompanija Xerox, odsek PARC¹⁸, projekat koji je u osnovi osmislio i rukovodio Robert Metcalfe. 1976. godine Metcalfe i njegov tim je publikovao rad pod nazivom *Ethernet: Distributed Packet Switching For Local Computer Networks* u kojem je objavljena konceptualna specifikacija Ethernet standarda. Uz njega je nastao standard IEEE 802.3.

Ethernet standard demonstrira fleksibilnost podrškom višestrukih medijuma za prenos. Originalni medijum, poznat pod imenom 10BASE-2, koji je koristio BNC¹⁹ tip koaksijalnih povezivanja i koaksijalnog kabliranja. To je godinama bio standard koji je prebacivao podatke brzinom od 10mbps. 10BASE-2, međutim, je postao dosta nezgapan, zahtevajući veliko održavanje. Zahtevan je kompletan krug za propisan rad. To znači da jedan otkaz mesta povezivanja ili pucanje kabla u velikim mrežama prouzrokuje prestanak normalnog rada.

Početkom 90-tih pušten je noviji standard 10BASE-T. 10BASE-T koristi kabl sa upredenim paricama, koji je sličan bakarnim telefonskim žicama, ali se razlikuje po tome što nosi četiri upredene parice. On je trenutno najrašireniji standard na svetu, a radi na brzinama od 10mbps, ili kasnije 100mbps (100BASE-T). Krajem prošlog veka, nastao je i *Gigabit Ethernet*, koji omogućava brzine prenosa do 1000mbps preko istog kabla sa upredenim paricama. Standard Gigabit Ethernet takođe može da prenosi podatke preko optičkih kabla.

¹⁶ eng. *Ethernet*

¹⁷ *mbps* – skraćenica za megabita u sekundi. Odgovara grubo jedan milion bitova u sekundi.

¹⁸ PARC – Xerox-ov Palo Alto Research Center smešten u Palo Alto, Kalifornija.

¹⁹ BNC je konektor tipa RF koji se koristi za prekidanje koaksijalnog kabla. Konektor je nazvan po svom „Bajonetskom” mehanizmu završavanja i njegova dva izumitelja „Neill” i „Concelman”.

2.5.3.2. Wi-Fi (802.11x)

Wi-Fi je standard razvijen da obavlja skoro istu ulogu kao i ethernet, jedino bez ožičenja. Prenosom preko vazduha, Wi-Fi omogućava da tačke budu bilo gde u radijusu od 100 do 300 metara od Wi-Fi rutera imaju stalnu, bezbednu konekciju LAN-a. Wi-Fi je počeo sa brzinama od samo 11mbps u obliku IEEE 802.11b, ali danas može da dostigne brzine između 54mbps i 108mbps.

Prvi Wi-Fi standard razvilo je Vic Hayes 1991. godine iz kompanije AT&T. U osnovi on je projektovan da obezbedi bežičnu komunikaciju za naplatne sisteme u maloprodajnim objektima i radio je na brzinama od 1 ili 2mbps. Krajem prošlog veka IEEE je ratifikovao specifikaciju 802.11b, koja omogućava bežično povezivanje nalik ethernetu između tačaka u opsegu brzine od 1 i 11mbps. Promenljiva brzina omogućava hardveru na tačkama da se prebace na niže brzine prenosa podataka kada se odaljavaju od pristupnog mesta²⁰ radi održavanja konekcije na većim razdaljinama. 2003. i 2004. godine pojavio se noviji standard IEEE 802.11g baziran na Wi-Fi specifikaciji. 802.11g obezbeđuje brzine između 11 i 54mbps, dok pritom održava kompatibilnost sa starijim 802.11b standardom. 2005. godine, pojavio se i noviji standard 802.11n. Specifikacija 802.11n omogućava brzine 108 do 540mbps dok pritom održava punu podršku za standarde 802.11b/g.

2.5.3.3. Bluetooth (802.15.1)

Bluetooth, IEEE 802.15.1, je standard za bežičnu mrežu malog opsega. Prvobitnu ga je razvio Ericsson Corporation. Bluetooth je projektovan da zauzme specijalni segment tržišta, a ne da bude univerzalna, široko rasprostranjena tehnologija visokih performansi. Bluetooth se skoro uvek koristi u "ad-hoc" vrsti mreža. U ovoj mreži bez rutera, tačke su odgovorne za automatsko međusobno obavljanje komunikacije. Obično se primenjuje u mobilnim telefonima, PC i PDA sinhronizaciji i u drugim situacijama u kojima mali uređaji zahtevaju malu snagu, kratak opseg. Bluetooth je postao standardan u većini današnjih malih prenosivih uređaja.

2.6. E-poslovanje i Internet

„Informacija je kamen temeljac e-poslovanja“²¹

Internet omogućava poslovnom okruženju da efikasnije koristi informacije (npr. omogućavanje zaposlenima, poslovnim parterima, dobavljačima i klijentima da pristupe poslovnim informacijama koje su im potrebne i kada su im potrebne. Web može da se koristi za

²⁰ Pristupna tačka; Obično za ruter ili svič bežične mreže.

²¹ Heimann, J., *Oracle9I for eBusiness: Security for your eBusiness Applications*, USA, 2001. str. 1

pravljenje elektronskih narudžbina. Ove vrste narudžbina se brže popunjavaju, a moguće greške se lakše uočavaju i ispravljaju nego kod običnih popunjenih rukom koje se dobijaju putem telefona ili faksa.

2.6.1. Istorijat i definisanje e-poslovanja

EDI predstavlja skup standarda za kontrolu prenosa poslovnih dokumenata, kao što su porudžbine i fakture, između računara. Cilj EDI-ja je izbegavanje rada sa papirom i skraćivanje vremena za odgovor. Da bi EDI bio efikasan, korisnici moraju unapred da se dogovore o određenim standardima za formatiranje i razmenu informacija, kao što je to protokol X.400 (standard CCITT serije).

Elektronska trgovina, B2C ili e-trgovina se odnose na onlajn prodaju. Elektronsko poslovanje ili e-poslovanje, s druge strane, odnosi se na više od čiste onlajn prodaje.

E-poslovanje koristi Internet tehnologije – kao što su obična e-pošta, onlajn bankarska rešenja, web sajтови i sofisticiranije aplikacije kao što su menadžment rešenja za klijente bazirana na web-u – radi obezbeđivanja boljeg korisničkog servisa, uobličavanja poslovnih procesa, povećanja prodaje i smanjenja troškova. Stoga, svaki vlasnik posla koji koristi Internet da razvije ili unapredi svoj posao koristi e-poslovanje.

Izraz elektronsko poslovanje prvi put je upotrebila američka kompanija IBM 1996. godine, da bi se označilo poslovanje uz značajnu primenu savremene, elektronske tehnologije.

Pod e-poslovanjem (e-business) podrazumevamo obavljanje poslovnih procesa uz primenu informacionih tehnologija i telekomunikacija. To omogućava slanje velikog broja informacija na velike daljine u kratkom vremenskom periodu. Preduzeća, koja u svom poslovanju koriste elektronsku tehnologiju, ostvaruju značajne uštede u troškovima poslovanja, efikasnije obavljaju zadatke i, samim tim, budu konkurentniji na tržištu.

Upotreba elektronskog poslovanja omogućava konkurentnije poslovanje i povećava šansu opstanka na tržištu, omogućava unutrašnju i spoljnu integraciju preduzeća. E-poslovanje omogućava i spoljnu integraciju tj. integraciju sa poslovnim partnerima, vladinim agencijama i slično, koja ubrzava, pojednostavljuje i pojeftinjuje međusobne transakcije. Najveći problem je pitanje bezbednosti rada tj. zaštita podataka od neovlašćenog pristupa i promena, i zaštita kreditnih kartica prilikom kupovine preko mreže i sl. To je problem koji zahteva veće tehničke i organizacione inovacije, kako bi se u što većoj meri sprečile zloupotrebe. Ljudski faktor je takođe veoma važan. Potrebno je sve više stručnjaka koji vladaju novom tehnologijom, a neophodno je i uvežbavanje korisnika unutar organizacije za što efikasnijim korišćenjem tih tehnologija. Kao i kod svih novih tehnologija postoji otpor uvođenju tehnologija, na kojima se zasniva elektronsko poslovanje.

Da bi se elektronsko poslovanje moglo razvijati, potrebno je ispuniti neke tehnološke pretpostavke. Pre svega je potrebno raspolagati informatičkom magistralom tj. infrastrukturom zadovoljavajućeg kapaciteta. Da bi se osigurala kompatibilnost uređaja i metoda koje se koriste u elektronskom poslovanju, potrebno je standardizovati sve aspekte rada mreže, od standarda video distribucije do protokola za rad u mreži i pružanja mrežnih usluga, kompresije različitih oblika multimedijalnih dokumenata i sl.

Među najvažnijim razlozima za optimistička predviđanja brzog razvoja e-poslovanja su:

- Izvanredno brz tehnološki razvoj;
- Razvoj novih servisa i poslovnih modela;
- Razvoj nacionalnih i međunarodnih standarda i vodiča za e-poslovanje.

Elektronsko poslovanje predstavlja poslovnu transformaciju zasnovanu na:

- udruživanju preduzeća (integracija),
- procesu saradnje (kolaboracija), i
- globalnom mrežnom povezivanju korišćenjem Interneta kao medija.

Među najvažnijim procesima e-poslovanja se ističu:

- prikupljanje podataka i informacija
- marketing (4P – marketing miks): promocija, podrška kupcima, uvođenje novog proizvoda,...
- onlajn prodaja (proizvoda i usluga)
- komunikacija

Najpopularniji kanal elektronskog poslovanja jeste Internet.

2.6.2. Podela prema tipu učesnika na tržištu

Postoje dva osnovna modela e-poslovanja:

- B2C (*Business to Consumer*) – Oblik poslovanja na Internetu koji pruža direktan interfejs između preduzeća i potrošača. Potrošači naručuju proizvode i servise elektronskim putem od preduzeća. Internet pruža različite mogućnosti marketinškog nastupa preduzeća i omogućava masovni pristup potrošača proizvodima i servisima elektronskim putem.
- B2B – Business to Business – Podrazumeva elektronsko poslovanje koje se odvija između preduzeća (od otkrivanja/pronalaženja odgovarajuće robe, pregovora,

naručivanja, ispostavljanja faktura, plaćanja, distribucije dokumentacije, a nekad čak i konkretne robe ili usluge, podrške, itd.).

Slika 4. prikazuje sve proste oblike e-poslovanja.

Slika 4.

Prosti oblici e-poslovanja

	Business	Consumer	Government
Business (poslovni sistemi)	B2B koordinacija	B2C informacije	B2G informacije
Consumer (potrošači)	C2B nabavke	C2C e-trgovina	C2G e-trgovina
Government (vlade zemalja)	G2B poreske obaveze	G2C komparacija cena	G2G aukcijska tržišta

Postoje i složeniji oblici e-poslovanja koji su kombinacija prethodno opisanih, a to su:

- B2B2C (*Business to Business to Consumer*) i
- C2B2C (*Consumer to Business to Consumer*).

Razvoj informacione i telekomunikacione tehnologije stvorio je uslove za globalizaciju poslovanja. Glavni cilj je postao da se bez obzira na geografske distance što brže i efikasnije povežu klijenti i tokovi informacija. U uslovima vrlo jake konkurencije gde postepeno nestaju razlike između banaka, investicionih banaka, brokerskih firmi i osiguravajućih kompanija, finansijske organizacije su pod stalnim pritiskom da zadrže korisnike svojih usluga, smanje troškove, upravljaju rizikom i koriste tehnologiju kao izvor konkurentske prednosti.

Model globalne organizacije i jake konkurencije zahteva novu koncepciju pristupa banaka u njihovom poslovanju, o čemu svedoče sve veća ulaganja u specijalizovanu i prema klijentu orijentisanu tehnologiju. Internet je jedna od tih tehnologija. Banke su prvobitno imale odbojnost prema inovacijama koje donosi poslovanje na Internetu, ali su tokom vremena uvidele da to nije prolazni fenomen nego sve više deo poslovne stvarnosti sa još većom perspektivom u budućnosti. Vremenom je nastao termin e-bankarstvo.

2.6.3. E-bankarstvo

Danas postoji preko 1000 svetskih banaka koje nude klijentima mogućnost obavljanja bankarskih transakcija direktno iz kuće, posredstvom Interneta.

Elektronsko bankarstvo predstavlja elektronske sisteme za transfer novca, zapisa i dokumenata bez papira baziranog na integraciji računarske i komunikacione tehnologije. U polazištu elektronskog bankarstva je EFT (eng. *Electronic Funds Transfer*) odnosno transfer sredstava iz dela finansijskih aktiva u okviru jednog ili više transaktora, elektronskim putem. Taj prenos novca i zapisa bez papira obavlja se uz korišćenje odgovarajućih programskih paketa i aplikacija.

Da bih nastavio izlaganje problematike o elektronskom bankarstvu navodim neku od definicija pojma e-bankarstva.

*“Elektronsko bankarstvo (Electronic Banking) termin je kojim se u informatici naziva korišćenje računara u bankarskim poslovima”.*²²

Elektronsko bankarstvo (eng. *E-banking*) je vid bankarskog poslovanja korišćenjem računarskih mreža i telekomunikacionih medija. Ono se ne može zvati Internet bankarstvo jer mreže koje se koriste ne moraju biti deo Interneta niti bazirane na Internet tehnologiji. Sve rasprostranjenija implementacija e-bankarstva podrazumeva rad preko Interneta uz intenzivno korišćenje Web tehnologije. Krajnji cilj je da istovremeno, i bankarski službenici sve svoje poslove obavljaju preko pretraživača, kao i da korisnik bankarskih usluga sve transakcije obavlja preko svog ličnog računara ili mobilnog telefona, standardnim Web pretraživačem (eng. *Web browser*).

Elektronsko bankarstvo, kao specifičan deo elektronskog poslovanja, ima sledeće prednosti u odnosu na klasično poslovanje:

- Smanjenje troškova transakcija;
- Brži obrt sredstava;
- Siguran i bezbedan platni promet;
- Ušteda vremena;
- Mogućnost obavljanja transakcija sa radnog mesta;
- Stalni uvid u stanje na računu i promet.

²² Stankić, R., Marinčić, D., *Računarstvo i informatika*, ZUNS, Beograd, 2003.

Primarni cilj uvođenja sistema elektronskih plaćanja bio je rešavanje problema sistema plaćanja zasnovanih na papiru, korišćenjem potencijalnih prednosti primene informacione tehnologije. Praksa je kasnije pokazala da ovi procesi znače mnogo više od zamene papirnih dokumenata i njihovog fizičkog prenosa elektronskim putem, odnosno da efikasno i ekonomično korišćenje ove tehnologije zahteva reinženjering poslovnih procesa i međusobnih odnosa učesnika.

2.7. SWIFT

SWIFT je svetsko udruženje za interbankarske finansijske telekomunikacije. Osnovan je 1973. godine, sa ciljem da postavi standard u automatskom transferu podataka između banaka, a od 1987. godine je proširen delokrug i na transfer podataka između finansijskih, nebankarskih organizacija: investicione institucije, brokerske i dilerske kompanije, klirinške organizacije, berza itd. Danas je SWIFT svetski lider u transferu podataka banaka i ostalih finansijskih organizacija.

SWIFT je sinonim za WAN mrežu. Ova mreža ima dve centrale koje se nalaze u Americi i Holandiji. Centri za podršku postoje na tri kontinenta i oni su na raspolaganju korisnicima 24 časa dnevno. Pored toga SWIFT mreža ima svoja regionalna predstavništva u svim većim zemljama u svetu. Početkom 2008. godine to je značilo 8.468 korisnika SWIFT-a iz 208 zemalja i obim od ukupno 3,501,000,000 razmenjenih poruka u 2007. godini. Visoki stepen sigurnosti u SWIFT mreži utiče i na proces ulaska novih korisnika u mrežu.

Proces je definisan, a njegovim završavanjem se garantuje visoka obučenost i osposobljenost kadrova novog korisnika i sigurnost starih korisnika. Dati proces uključivanja novog korisnika u SWIFT mrežu se ranije odvijao u sledećim fazama:

Prva faza (trajala oko 8 nedelja):

- Prijavljivanje za uključanje u SWIFT mrežu i pripremanje projektnog tima;
- Popunjavanje i slanje prijavnih dokumenata;
- Naručivanje svih potrebnih sredstava.

Druga faza (trajala oko 18 nedelja):

- Popunjavanje i vraćanje implementacionih formulara u službu za naručivanje;
- Instaliranje SWIFT opreme i softvera i njihovo testiranje;
- Obuka korisnika.

Treća faza (trajala oko 4 nedelje):

- Provera i testiranje kadrova po završenoj obuci;
- Razmena bilateralnih ključeva.

Ulaskom novog korisnika u SWIFT mrežu on je postajao punopravan član korisnik mreže. Svakih tri meseca su starim članovima SWIFT mreže slati fajlovi koji sadrže podatke o svim novim članovima mreže. Danas, uvođenjem PKI, izbegnuta je potreba za tim. Takav način organizovanja i vođenja mreže ju je učinio najboljom i najsigurnijom mrežom ove vrste u svetu i skoro sav promet u međunarodnom bankarstvu i finansijama se odvija preko nje.

Pristup korisnika na SWIFT mrežu je ostvarivan uobičajeno na izložen način povezivanja u klijent/server arhitekturi, pri čemu su se mogle koristiti iznajmljene linije i X.25 protokol. Danas je sve olakšano mogućnošću korišćenja standardnih Internet konekcija. Sada je širi izbor konekcija, a kao protokol se kroisti X.500.

Ono što je bilo i dalje je obavezno pri korišćenju SWIFT-a je:

- Standardizovana struktura dokumenata
- Kriptografija, odnosno šifriranje poruke

Svaki korisnički server, preko koga se pristupa SWIFT mreži bio je opremljen čitačem kartica SCC i ICC koje su obezbeđivale identifikaciju korisnika, a svi PC i korisničkoj LAN mreži su imali instalirane klijent-SWIFT aplikacije. Danas su u upotrebi Hardverski sigurnosni moduli (HSM).

Ranije su postojale korisničke kartice za pristup mreži na tri nivoa (tri vrste):

1. Korisničke kartice koje su služile za prijavljivanje korisnika na mreži;
2. Administratorske kartice koje su koristili administratori mreže za pristup;
3. Kartice korišćene za razmenu bilateralnih ključeva.

Veliku popularnost SWIFT-a, kao WAN mreže koja obezbeđuje implementaciju Internet tehnologija u svet finansijsko bankarskih usluga ima svoje polazište u sledećim mogućnostima (24 časa/dnevno, 7 dana u nedelji):

- Sve vrste transfera sredstava korisnika (klijenata)
- Sve vrste transfera banaka
- Prenos poruke (između svih članica)
- Menjački poslovi
- Depoziti i zajmovi

- Mogućnost pozajmice depozita i sredstava
- Plaćanje kamata
- Izvodi i potvrde stanja računa
- Postavljanje pitanja (upita) i dobijanje odgovora
- Korišćenje Internet servisa.

Svaka standardizovana SWIFT poruka sastoji se iz tri dela:

1. Naslov (prijavni i korisnički deo)
2. Tekst
3. Završetak

Tekst poruke je strogo struktuiran i za svaku se poruku tačno zna koja polja poruke moraju biti popunjena, a koja mogu ostati prazna.

Konstantno širenje međunarodne trgovine i finansija, rast važnosti tržišta kapitala i razmene informacija, znanja i dokumenata u čitavom tom finansijskom kompleksu, postavio je pred SWIFT visoke zahteve zaštite. Ta zaštita postiže se sledećim mehanizmima:

- Kontrola pristupa
- Zaštita tajnosti i integriteta informacije
- Provera identiteta pošiljaoca i primaoca uz korišćenje svih elemenata kriptografije
- Šifriranje
- Ključevi (javni i tajni)
- Dešifrovanje

2.7.1. Primer u praksi

U dosadašnjim izlaganjima, pored ostalog, pokrivene su sledeće oblasti:

- Internet protokoli i Internet sa osvrtom na TCP/IP skup protokola
- Računarske mreže
- E-poslovanje sa osvrtom na e-bankarstvo

Na primeru plaćanja RTGS unutar SWIFT mreže moguće je prikazati kako ove tri i još nekoliko drugih oblasti funkcioniše unutar jednog sistema.

Slika 5. Sistem plaćanja RTGS (SWIFT kao WAN)

Vidljiva je izuzetna složenost jedne ozbiljne WAN mreže. Sledećih nekoliko elementa unutar SWIFT mreže su značajni za predmet istraživanja:

- TCP/IP skup protokola – TCP/IP skup protokola ima funkciju povezivanja WEB klijenta na Internet. Način funkcionisanja ovog skupa pravila omogućava da se veliki broj računara poveže u Internet mrežu.
- Internet – Vidljivo je korišćenje Interneta preko kojeg je u određenim unapred predviđenim uslugama SWIFT sistema, moguće prići VPN-u ili SWIFT mreži.
- VPN – VPN se u ovom slučaju koristi da preko Interneta odvoji saobraćaj od drugih korisnika preko vrste mreže sa jakim sigurnosnim osobinama.

2.8. Zaštita u računarskim mrežama

Bezbednost IKT²³ sistema je objektivna mera/ocena stanja rizika IKT sistema ili stanja sigurnog, pouzdanog i neometanog funkcionisanja sistema u odnosu na sam sistem i njegovo okruženje.²⁴

U nastavku je izdvojeno i opisano nekoliko ključnih oblasti vezanih za e-bankarstvo.

23 Informaciono komunikacioni sistem – skr. IKT

²⁴ Milosavljević, M., Grubor, G., *Osnovi bezbednosti i zaštite informacionih sistema*, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Beograd, 2006.

2.8.1. Kriptografija

Kriptografija je grana kriptologije koja za predmet ima sintezu postupaka za obezbeđivanje tajnosti informacija, tzv. kripto-zaštitu informacija.²⁵

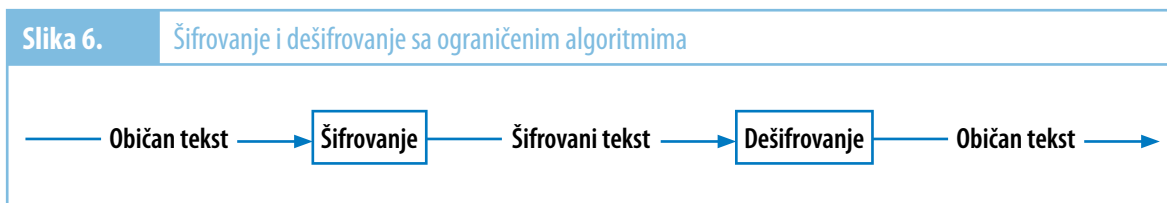
2.8.1.1. Osnovni termini i definicije

Poruka u svojoj originalnoj formi se naziva običan tekst (eng. *plaintext* ili *cleartext*). Proces zaštite te poruke skrivanjem njenog sadržaja naziva se šifrovanje (eng. *encryption* ili *enciphering*). Šifrovana poruka se naziva šifrovani tekst (eng. *ciphertext*), a postupak prebacivanja šifrovanog teksta nazad u običan tekst se naziva dešifrovanje (eng. *decryption* ili *deciphering*).

Osobe koje se bave kriptografijom zovu se kriptografi. Veština i nauka razbijanja šifrovanih poruka naziva se kriptanaliza, kojom se bave kriptanalitičari.

Kôd ili kriptografski algoritam je matematička funkcija ili formula koja se koristi za konvertovanje običnog teksta u šifrovani i nazad. Uobičajeno, za šifrovanje i dešifrovanje koristi se par algoritama koji se nazivaju ograničeni algoritmi.

Na slici 1. prikazan je šematski tok ograničenih algoritama.



Glavni problem kod ograničenih algoritama je da ne mogu da ga koriste menjajuće grupe. Svaki put kada neko napusti grupu, algoritam mora da se promeni. Da bi se zadržala tajna, svaka grupa mora da napravi sopstvene algoritme i softvere za njihovo korišćenje.

Ova ograničenja se prevazilaze korišćenjem promenljive poznate kao ključ ili kriptopromenljiva. Opseg mogućih vrednosti za ključ se zove prostor ključa. Dok svaka grupa koristi sopstveni ključ, zajednički i dobro poznati algoritam može da deli bilo koji broj grupa.

Neki algoritmi će koristiti različite ključeve za šifrovanje i dešifrovanje. Slika 2. ilustruje da je ključ ulazni podatak za algoritam.

²⁵ Ikkal, J., *An Introduction to Cryptography*, Information Security Management Handbook, 6th Edition, Auerbach Publications, 2007.

Slika 7. Šifrovanje i dešifrovanje sa ključem



Treba imati u vidu da bezbednost svih takvih algoritama zavisi od ključa a ne od samog algoritma. Stručnjaci za bezbednost informacija naglašavaju da bilo koji algoritam koji nije prethodno razmatran, analiziran i izdržao napade (npr. *zero restriction*) treba smatrati nebezbednim i odbaciti ga.

2.8.1.2. Simetrični kriptografski algoritmi

Algoritmi koji koriste isti ključ za šifrovanje i dešifrovanje zovu se simetrični kriptografski algoritmi. Postoje dve osnovne vrste ovih algoritama: šifra niza i šifra bloka.

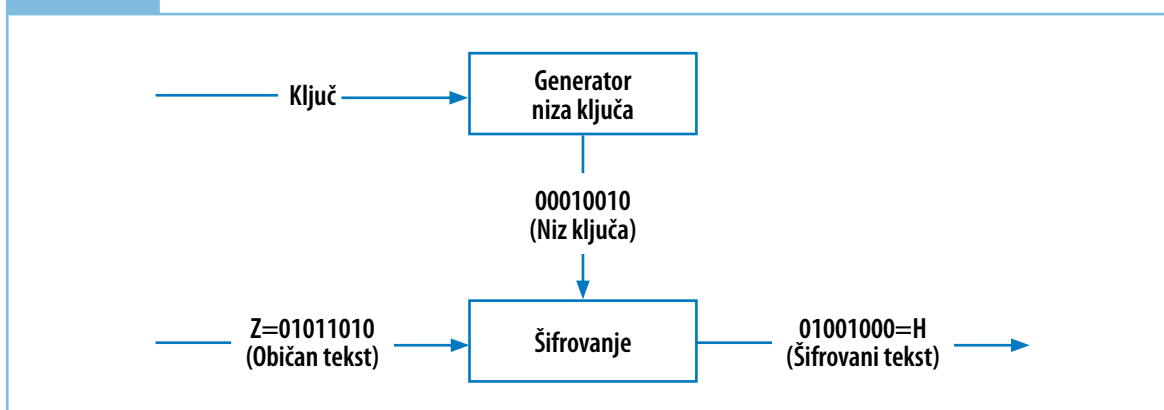
Šifra niza

Kod šifre niza, algoritam uzima poruku u nizu i radi na pojedinačnim elementima podataka (karakterima, bitovima ili bajtovima).

Standardno, generator slučajnih brojeva koristi se za pravljenje niza karaktera koji se nazivaju niz ključa. Niz ključa se zatim kombinuje sa čistim tekstom preko XOR (isključujuće-ILI) za pravljenje šifrovanog teksta.

Slika 3. ilustruje ovu operaciju šifrovanja slova Z, čija je ASCII vrednost predstavljena binarno kao 01011010. Treba imati u vidu da operacija XOR uključuje binarne cifre, samo 0 XOR 1 daje 1, svi ostali XOR za rezultat imaju 0.

Slika 8. Rad šifre niza



Šifra bloka

Šifra bloka zahteva akumuliranje neke količine podataka ili višestrukih elemenata podataka pre otpočinjanja šifrovanja. Šifrovanje i dešifrovanje se dešava na nekom broju podataka, za razliku od šifre niza koja radi nezavisno na svakom karakteru ili bitu.

DES

DES je star skoro 30 godina, a iz razloga njegove široke implementacije i korišćenja, on će verovatno da koegzistira uz AES još nekoliko godina. Uprkos početnoj zabrinutosti u vezi uloge NSA u postavljanju standarda, DES je pobudio veliko interesovanje za kriptografiju. Prodavci i korisnici su podjednako želeli da prihvate prvi standard za šifrovanje koji je odobrila vlada. DES je simetrična šifra bloka koja radi u blokovima od 64 bita u trenutku, sa 64-bitnim običnim tekstom koji daje 64-bitni šifrovani tekst. Ako podatak nije deljiv sa 64 bita, onda se on popunjava do kraja.

Trostruki DES je DES koji se izvršava tri puta, obično sa dva 56-bitna ključa. U najpopularnijoj formi, prvi ključ se koristi za DES šifrovanje poruke. Drugi ključ se koristi za DES dešifrovanje te ist šifrovane poruke. Iz razloga što on nije pravi ključ, pokušano dešifrovanje samo dodatno skrembluje podatke. Rezultujući šifrovani tekst se zatim ponovo šifrue prvim ključem čime se dobija konačni šifrovani tekst. Ponekad se koriste tri ključa za ovu operaciju.

AES

1997. godine NIST je objavio zahtev za ponudu radi izbora algoritma šifrovanja simetričnim ključem koji će se koristiti za zaštitu osetljivih (neklasifikovanih) saveznih informacija. Nakon testiranja 15 izabranih kandidata NIST je izabrao algoritam Rijndael kao AES standard. Rijndael je šifra bloka koja može da procesira blokove dužine 128, 192 i 256 bita korišćenjem ključeva dužine 128, 192 i 256 bita. Moguće su svih devet kombinacija dužine bloka i ključa.²⁶ Uprkos tome, standard AES specifikuje samo dužinu blokova podataka od 128 bita sa ključevima dužine 128, 192 i 256 bita.

Ovaj algoritam uključuje početnu logičku operaciju XOR stanja i zaokruženi ključ, devet krugova transformacije i krug koji se izvršava na kraju sa izostavljanjem jednog koraka.

* * *

Dobro poznato i često korišćeno šifrovanje je šifra niza raspoloživa uz algoritam PKZIP. Na nesreću, postoji takođe dobro poznat napad koji uključuje običan tekst nasuprot njemu – ako znate deo običnog teksta, moguće je dešifrovati fajl.

²⁶ Sajt za razvoj algoritma Rijndael: <http://www.esat.kuleuven.ac.be/wrijmen/rijndael/>

U 1975. godini teoretisano je da bi namenski razbijač DES koštao oko 20 miliona dolara. 1998. napravljen je jedan za 220.000 dolara. Sa razvojem snage računanja, vreme i novac potrebni za razbijanje zaštite DES je još dodatno smanjeno. Uprkos tome što se on i dalje koristi, ako je moguće, daleko je bolje koristi AES ili trostruki DES.

2.8.1.3. Asimetrična kriptografija (sa javnim ključem)

Asimetričnost je termin koji se koristi u kriptografskim sistemima gde se jedan ključ koristi za šifrovanje, dok se drugi koristi za dešifrovanje.

U osnova ovog koncepta, koji je pronađen 1976. godine, je jako jednostavna. Postoji par ključeva tako da ako se jedan koristi za šifrovanje, drugi može da se koristi za dešifrovanje. Pored toga davanje jednog ključa ne znači lako otkrivanje drugog. To je osnova asimetrične kriptografije, često zvane kao kriptografija sa javnim ključem.

Postoji puno raspoloživih algoritama, ali većina njih su ili nesigurni ili prave šifrovani tekst koji je veći od običnog teksta. Od algoritama koji su i sigurni i efikasni, samo tri mogu da se koriste i za šifrovanje i digitalni potpis. Na žalost, ovi algoritmi su često sporiji i do hiljadu puta u odnosu na simetrično šifrovanje ključem. Kao rezultat, popularni su hibridni kriptografski sistemi.

RSA

RSA je dobio ime po svojim pronalazačima (Rivest, Shamir, Adleman). RSA se oslanja na teškoću rastavljanja velikih prostih brojeva na faktore. Ako dođe do iznenadnog skoka u kompjuterskoj tehnologiji ili matematici koja menja to, sigurnost takvih šema šifrovanja biće razbijena.

Kriptosistemi eliptične krive (ECC)

Rešavanje RSA se oslanja na težak matematički problem: rastavljanje veoma velikih brojeva. Postoji još jedan težak matematički problem: logaritmovanje. Na primer, moguće je lako podići 7 na 4-ti stepen i dobiti 2401; ali ako se da samo 2401, sprovođenje postupka unazad i dobijanje 7^4 je teže (skoro jednako teško kao sprovođenje rastavljanje velikih brojeva na faktore).

Teškoća sprovođenja izolovanih logaritmovanja preko eliptične krive (koju ne treba mešati sa elipsom) je još teža, a za istu veličinu ključa, ona predstavlja teži izazov od RSA (ili predstavlja istu teškoću/sigurnost sa manjom veličinom ključa). Postoji implementacija ECC koja koristi problem rastavljanja na faktore, ali ova varijanta ne predstavlja praktičnu prednost u odnosu na RSA.

Suština je da eliptična kriva ima interesantnu osobinu: moguće je definisati tačku na krivoj kao zbor dve druge tačke na krivoj.

SSL

SSL obezbeđuje šifrovanje između pretraživača i Web servera.

SSL funkcioniše na osnovi sertifikata i provere autentičnosti.

Ako je sertifikat legitiman, pretraživač će uradi sledeće:

- Generisati slučajni ključ za simetrično šifrovanje
- Šifrovati ovaj simetrični ključ sa javnim ključem servera
- Šifrovati URL koji želi sa simetričnim ključem
- Poslati šifrovani ključ i šifrovani URL na server

Server će uraditi sledeće:

- Dešifrovati simetrični ključ sa svojim privatnim ključem
- Dešifrovati URL sa simetričnim ključem
- Procesirati URL
- Šifrovati odgovor sa simetričnim ključem
- Poslati šifrovani odgovor nazad do pretraživača

U ovom slučaju, iako je šifrovanje dvosmerno, provera autentičnosti je samo jednostrana: identitet servera je dokazan klijentu, ali ne i obratno. međusobna provera autentičnosti je takođe moguća i sprovodi se u nekim slučajevima. U određenom scenariju visokog nivoa sigurnosti, banka može da izda sertifikat pojedincima, i nijednom pretraživaču neće biti dozvoljeno da se poveže bez tih pojedinačnih sertifikata koji identifikuju korisnike serveru banke.

Šta se događa kada pretraživač koji može da vrši samo 40-bitno šifrovanje (stariji zakoni u SAD su zabranjivali izvoz pretraživača sa 128-bitnim šifrovanjem) dođe na sajt koji ima mogućnost 128-bitnog? Tipično, sajt će se spustiti na 40-bitno šifrovanje.

Treba imati u vidu da osnovni sertifikati ugrađeni u pretraživače ponekad ističu; poslednji veliki slučajeve vrste je bio VeriSign 1999. godine. U tom trenutku, prvenstveno finansijske institucije su insistirale da njihovi korisnici nadgrade svoje pretraživače.

Na kraju, treba pomenuti i postojanje drugog protokola nazvanog Secure HTTP koji pruža sličnu funkcionalnost ali se veoma retko koristi.

2.8.1.4. Izbor algoritma

Koji algoritam šifrovanja, sa kojom veličinom ključa, treba da izabere profesionalac za zaštitu informacija?

Pravi odgovor je: zavisi od nekoliko faktora; šta se šifruje, protiv koga nam je potrebna zaštita i koliko dugo treba da traje ta zaštita?

Ako je to podatak sa berze, bilo koja šema šifrovanja koja može da izdrži do 20 minuta je dovoljna; za 20 minuta, ista informacija biće na brojnim servisima besplatnim servisima za berzanske kvote.

Ako je to lozinka za Web sajt lista Politika? Bitna je pretpostavka ne koristiti istu lozinku za vaš nalog e-pošte, SSL je dovoljno sposoban za taj server.

Transakcije preko kreditne kartice, bankovnog računa i medicinskih kartona zahtevaju najjače moguće šifrovanje, i u prenosu i u čuvanju.

2.9. Upravljanje ključevima

Najmanje cenjen izum (od ukupno pet) koji karakteriše modernu kriptografiju je automatsko upravljanje ključem. Ovaj moćan mehanizam nam omogućava da se prevaziđu strogost i disciplina koja vodi do neizbežnog kompromitovanja kripto-sistema. Omogućavanjem da se ključevi često i sigurno menjaju, ovaj sistem prevazilazi fundamentalna ograničenja algoritama koji koristimo. On omogućava da se kompenzuju ljudska ograničenja kao što su to nemogućnost pamćenja ili prepisivanja dugačkih slučajnih brojeva.²⁷

2.9.1. Definicija

Upravljanje ključevima može da se definiše kao generisanje, beleženje, transkripcija, distribuiranje, instalacija, čuvanje, zamena, raspoređivanje i kontrola kriptografskih ključeva. Praksa sugeriše da svaki od navedenih koraka predstavlja mogućnost za kompromitovanje kriptografskog sistema. Takođe, ona sugeriše da su napadi na ključeve i upravljanje ključevima verovatniji i efikasniji od napada na algoritme.

²⁷ Murray, W.H., *Principles and Applications of Cryptographic Key Management*, Information Security Management Handbook, 6th Edition, Auerbach Publications, 2007.

Upravljanje ključevima mora da bude rigorozno i disciplinovano. Praksa govori da je jako teško postići.

2.9.2. Funkcije upravljanja ključevima

U nastavku su detaljnije opisane funkcije koje detaljnije definišu upravljanje ključevima.

2.9.2.1. Generisanje ključa

Generisanje ključa je izbor broja koji će se koristiti za prilagođavanje mehanizma šifrovanja prema određenoj upotrebi. Upotreba može da bude par pošiljaoca i primača, domen, aplikacija, uređaj ili objekat podataka. Ključ se bira tako da ga nije moguće predvideti i da njegovo poznavanje ne procuri u toku procesa generisanja.

Neophodno je ali ne i dovoljno da se ključevi biraju nasumično. Pored nasumičnog biranja ključeva, da izabrani ključ ne bude obelodanjen u trenutku njegovog izbora. Iako ključ može da se sigurno sačuva nakon njegovog generisanja, on može da bude ranjiv na otkrivanje u trenutku njegovog generisanja kada se on može pojaviti u jasnoj formi. Alternativno, informacija koja se koristi prilikom generisanja ključa može da se zabeleži u trenutku kada se sakuplja, time čineći da ključ bude predvidljiviji u odnosu na veličinu prostora ključa.

2.9.2.2. Distribucija

Distribucija ključa je proces dobijanja ključa sa tačke njegovog generisanja do tačke njegove nameravane upotrebe. Ovaj problem je teži u algoritmima sa simetričnim ključem, gde je neophodno zaštititi ključ od otkrivanja u toku procesa. ovaj korak mora da se izvrši na kanalu odvojenom od onog kojim dolazi saobraćaj.

2.9.2.3. Instalacija

Instalacija ključa je proces dobijanja ključa za čuvanje u uređaju ili za proces koji će ga koristiti. Tradicionalno, ovaj korak je uključivao neke manuelne operacije. Takva operacija može rezultovati u curenju informacija o ključu, greškama u njenoj transkripciji ili ona može da bude toliko nezgrapna da odvrati od njenog korišćenja.

2.9.2.4. Čuvanje

Ključ može da se zaštiti integritetom samog mehanizma za čuvanje. Na primer, mehanizam može da bude projektovan da nakon što je ključ instaliran, on se ne može videti van same mašine za šifrovanje. Zaista, neki specijalni uređaji za čuvane ključa su konstruisani na samouništenje kada se na njih primeni sila koja može da otkrije ključ ili ako postoji dokaz da se čačka uređaj ključa.

Kao alternativa, ključ može da se čuva u šifrovanoj formi tako da poznavanje sačuvane forme ne otkriva informaciju o ponašanju uređaja pod ključem.

2.9.2.5. Promena

Promena ključa je prestanak korišćenja jednog ključa i početak primene drugog. To se određuje konvencijom ili protokolom. Standardno, vreme u kojem će najverovatnije procureti informacija o ključu je vreme zamene ključa. Stoga, postoji veličina stabilnosti ključa. S druge strane, što je duže ključ u upotrebi, veći deo saobraćaja koji je šifrovan njime, to je veća mogućnost da će biti otkriven i veći deo saobraćaja koji će biti kompromitovan. Stoga, postoji veličina za menjanje ključa.

2.9.2.6. Kontrola

Kontrola ključa je mogućnost upotrebe usmerenog ili zadržavajućeg uticaja preko njegovog sadržaja ili korišćenja. Jedna od zadataka kontrole ključa je osigurati da se ključ koji je namenjen za šifrovane ključeva ne može koristiti za podatke.

2.9.2.7. Odbacivanje

Ključevi moraju da se odbacuju na takav način da se zaštite od otkrivanja. Ranije je to bio veći problem nego što je to sada.

2.9.3. Moderno upravljanje ključevima

Moderno upravljanje ključevima je stvorio tima IBM-a 70tih godina prošlog veka. Moderno upravljanje ključevima je potpuno automatizovano; manuelni koraci se ne zahtevaju niti dozvoljavaju. Korisnici ne biraju, komuniciraju ili prepisuju ključeve. Ne samo da bi takvi koraci zahtevali da korisnik zna ključ i dozvoli mu da ga otkrije, slučajno ili namerno, oni bi takođe bili veoma podložni greškama.

Moderno upravljanje ključem dozvoljava česte promene ključa. Najočigledniji primer je ključ sesije. On se kreira u trenutku sesije, razmenjen pod ključem za šifrovanje ključa i automatski odbačen na kraju sesije.

Automatizovanje sistema menja balans. Ono dozvoljava česte promene sigurnosnog ključa koje podižu trošak napada za kriptanalitičare. Što se više ključeva koristi za datu količinu podataka, veća je cena napada (potrebno je naći više ključeva) i manja je mogućnost uspeha (manje podataka za svaki ključ). Kako se broj ključeva povećava, cena napada se približava beskonačnosti, a mogućnost uspeha se približava nuli. Trošak zamene ključeva linearno povećava troškove šifrovanja, a eksponencionalno povećava trošak napada.

Iz razloga što mnogi algoritmi koriste ključeve fiksne dužine, a pojedinac skoro uvek može da nađe ključ u upotrebi korišćenjem ograničenog seta ključeva, i iz razloga što pad cena i povećavanje brzine kompjutera uvek smanjuje trošak i vreme potrebno za takav napad, ograničena dužina ključa može da predstavlja ozbiljno ograničenje efektivnosti algoritma. U današnjem Internet svetu, u kojem se istovremeno koriste hiljade kompjutera za nalaženje jednog ključa, u najmanju ruku je shvatljivo da pojedinac može da nađe ključ za vreme njegovog veka upotrebe. Automatska promena ključa kompenzuje ovo ograničenje.

Međutim, moderno upravljanje ključem ima druge prednosti pored veće efikasnosti dužine ključa i kraćeg veka. Ono može da se koristi da osigura uključivanje većeg broja ljudi u osetljive zadatke. Na primer, glavni Visa ključ je sačuvan u San Francisku u kutiji koja se zove BBN SafeKeyper. On je stvoren unutar kutije i niko ne zna šta je to. Delotvorno korišćenje ključa zahteva posedovanje kutije i njena tri fizička ključa. Iz razloga shvatljivo je kutija može da se uništi, ona je eksportovala informacije o ključu. Pet poverenika dele ovu informaciju na takav način da bilo koja trojica, korišćenjem druge kutije SafeKeyper, mogu da rekonstruišu ključ.

Upravljanje ključem takođe može da se koristi za smanjenje rizika u vezi sa izgubljenim ili oštećenim ključevima. Uprkos tome što aplikacije za komunikaciju ne moraju da brinu o izgubljenim ključevima, u aplikacijama za šifrovanje fajlova, izgubljen ključ može da bude ekvivalentan gubitku podataka. Upravljanje ključevima može da pruži zaštitu protiv toga. Na primer, jedan od zaposlenih može da ima informaciju o jednom od ključeva drugog koji bi mu omogućili da ga povрати ako se bilo šta dogodi drugom zaposlenom. U tom slučaju on može sasvim sam da povрати ključ. Pošto kopija ključa prepolovljava njegovu sigurnost, implementacija koja se koristi može da omogućiti da se sigurnost kompenzuje preciziranjem koliko ljudi mora da učestvuje u procesu dobijanja ključa nazad.

Upravljanje ključem može da bude zasebna računarska aplikacija ili ona može da bude integrisana u druge aplikacije. IBM prodaje proizvod koji banke mogu da koriste za upravljanje ključevima preko banka i aplikacija.

Netscape Navigator i Lotus Notes imaju ugrađeno upravljanje ključem.

2.9.4. Principi upravljanja ključem

Brojni principi navode korišćenje i implementaciju upravljanja ključem. Oni su neophodni, ali možda nisu dovoljni za sigurnu implementaciju. To znači, čak i implementacije

nabrojane koje se drže ovih principa mogu da budu slabe, ali sve implementacije koje se njih ne drže su slabe.

Na prvom mestu, upravljanje ključem mora da bude potpuno automatizovano. Ne smeju da postoje bilo kakve manuelne operacije. Ovaj princip je neophodan i radi discipline i za tajnost ključeva.

Na drugom mestu, ni jedan ključ ne sme nikad da se pojavi u čistoj spoljašnjoj formi izvan kriptografskog uređaja. Ovaj princip je neophodan za tajnost ključeva. On takođe odoleva poznatim napadima običnog teksta nasuprot ključevima.

Ključevi moraju da se nasumično biraju iz kompletnog prostora ključa. Ako postoji bilo koji obrazac načina na koji se biraju ključevi, ovaj obrazac može da iskoristi napadač da smanji njegov posao. Ako se ključevi povuku na način da svi mogući ključevi nemaju jednaku mogućnost da se povuku, onda je posao napadača smanjen.

Na primer, ako se ključevi biraju tako da odgovaraju rečima prirodnog jezika, onda je potrebno tražiti samo ključeve koji odgovaraju takvom opsegu umesto kompletnog prostora ključa.

2.10. Infrastruktura sa javnim ključevima (PKI)

2.10.1. Pojam PKI

Infrastruktura sa javnim ključevima (eng. *Public Key Infrastructure*, PKI) predstavlja kombinaciju hardverskih i softverskih elemenata, ljudi, politika i procedura neophodnih za generisanje, skladištenje, upravljanje, distribuciju i opoziv digitalnih sertifikata. Njena osnovna uloga je uspostavljanje digitalnog identiteta (eng. digital IDs) subjekata u okviru mreže baziranog na digitalnim sertifikatima, čime se stvara pogodno okruženje za realizaciju drugih bezbednosnih servisa, prvenstveno onih kod kojih je od značaja autentičnost subjekata koji komuniciraju.

PKI se bazira na politici zaštite informacionog sistema u kome se primenjuje. Politika zaštite uspostavlja i definiše osnovne pravce i strategiju razvoja bezbednosti informacionog sistema organizacije, propisuje procedure i principe korišćenja kriptografskih mehanizama u sistemu (način upravljanja ključevima), propisuje neophodne nivoe kontrole koji odgovaraju nivoima rizika itd.

Drugačije rečeno, uspostavljanje PKI je osnovni preduslov za realizaciju sistema zaštite. Servisi PKI koriste se na svim nivoima zaštite računarskih resursa i mreža.

Primeri primena zasnovanih na infrastrukturi sa javnim ključevima (PKI) su:

- formiranje virtualne privatne mreže (eng. Virtual Private Network, VPN)
- formiranje pouzdanog sistema zaštite na transportnom nivou u računarskoj mreži
- zaštita E-mail servisa
- zaštita WEB transakcija
- bezbedna razmena dokumenata
- kontrola radnog vremena i pristupa određenim prostorijama.

2.10.2. Sastav PKI

PKI se sastoji iz sledećih komponenti:

- sertifikacionog tela (CA – eng. *Certification Authority*), koje izdaje digitalne sertifikate i reguliše način njihove upotrebe tokom perioda važnosti
- osnovnog dokumenta rada Politike sertifikacije (CP – eng. *Certificate Policy*), koja utvrđuje osnovne principe rada CA i ostalih komponenti PKI
- praktičnih pravila rada (CPS – eng. *Certificate Practice Statement*), predstavljenih dokumentom koji praktično opisuje rad CA i neophodan je u slučaju komercijalnog rada. CPS je detaljan dokument koji sadrži operacione procedure za realizaciju principa koji su navedeni u politici sertifikacije i predstavlja praktičnu podršku sistemu. On uključuje definicije kako je CA formiran, kako radi, kako se generišu digitalni sertifikati, kako se povlače, kako će ključevi biti generisani, registrovani i sertifikovani, gde će se čuvati i kako će biti raspoloživi korisnicima
- registracionih tela (RA – eng. *Registration Authority*), koji predstavljaju interfejs odn. mesta za podnošenje zahteva za izdavanje sertifikata
- komunikacionih sistema za razmenu podataka između registracionog i sertifikacionog autoriteta, distribuciju zahteva za izdavanje sertifikata i slanje digitalnih sertifikata.
- kriptografskih aplikacija za realizaciju funkcija PKI subjekata koji komuniciraju u mrežnom okruženju, na bazi izdatih digitalnih sertifikata
- krajnjih korisnika odn. subjekata koji komuniciraju.

2.11. PKI SMART kartice

2.11.1. SMART kartice

Smart kartice su fascinantna tvorevina tehnologije. One bukvalno drže ključ da bi povećale sigurnost. Jedan od mnogih izazova za sigurnost informacija je kontrolisanje pristupa resursima kao što su informacije, aplikacije, servisi ili sistemski uređaji. U današnje vreme, kombinacija korisničkog imena i lozinke su norma za autentifikaciju korisnika, ali ovaj pristup predstavlja fundamentalnu slabost u pogledu sigurnosti. Pošto poslovi stavljaju veće zahteve za pristup informacijama i raspoloživost rastućem broju različitih entiteta, kombinacija korisničkog imena i lozinke jednostavno ne može to da izdrži. Ne samo da smart kartice obezbeđuju mehanizam da osiguraju dugotrajnu skalarnost i funkcionalnost za kontrolisanje pristupa, već one takođe obezbeđuju servise za omogućavanje posla.

Radi boljeg razumevanja smart kartice kao celine, u nastavku je data analiza njenih sastavnih elemenata.

2.11.1.1. Memorija

Postoji nekoliko vrsta memorija koje mogu da se integrišu u smart karticu, kao što su to na primer:

- ROM (*read-only memory*) – ROM, ili još preciznije podatke sadržane unutar ROM-a, unapred određuje proizvođač i oni su nepromenljivi. On je previše ograničen za današnje zahteve.
- PROM (*programmable read-only memory*) – Ova vrsta memorije može da se modifikuje, ali zahteva primenu visokih napona da napravi topljive veze unutar IC.
- EPROM (*erasable programmable ROM*) – EPROM je dosta korišćen u ranijim smart karticama, ali arhitektura IC radi u režimu OTP (*one-time programmable*), i stoga ograničava servise koje nudi ICC.
- EEPROM (električno izbrisivi PROM) – EEPROM je IC izbora iz razloga što korisnicima nudi pristup i mogućnost da se ponovo upiše, u nekim slučajevima i do milion puta. Tipično, količina memorije je u opsegu od 8 do 256 KB.
- RAM (*random access memory*) – RAM nema mogućnost pamćenja podataka, i svi podaci su izgubljeni kada uređaj nije napajan.

2.11.1.2. Procesor

Memorija sama po sebi ne čini karticu “pametnom.” Prilikom implementacije IC, u čip se integriše mikrokontroler (ili CPU), koji efektivno upravlja podacima u memoriji. Logika kontrole je usadena u kontroler memorije i pruža različite servise, poslednji od njih je sigurnost. Stoga, jedan od najinteresantnijih aspekata smart kartica (i njihovog korišćenja u primenama u vezi sigurnosti) je zasnovan na činjenici da kontrole povezane sa podacima su suštinske za pravljenje IC.

Jednostavno rečeno, smart kartica ima procesor i nepromenljivu memoriju, što joj omogućava da bude pametna koliko i sigurna. Navedene su neke od osobina standardnih smart kartica današnjice:

- 64-KB EEPROM-a
- 8-bitni CPU mikrokontroler – To je mali kontroler za koji mogu da se implementiraju nekoliko formi logike. Na primer kriptografske funkcije za DES, 3DES, RSA 1024-bit, SHA-1, itd.
- Promenljivo napajanje (2,7 do 5,5 V) – Mnoge kartice će raditi na ispod 3 V, nudeći duži vek trajanja i povećanu efikasnost. Takođe, one mogu da rade i do 5,5 V radi usklađivanja sa starim čitačima kartica i sistemima.
- Frekvencija sistemskog sata (1 do 7,5 MHz)
- Izdržljivost – Izdržljivost se odnosi na broj ciklusa pisanja/brisanja. Očigledno, to je važno imajući u vidu korišćenje smart kartice. Većina smart kartica će nuditi između 250.000 i 500.000 ciklusa.
- Zadržavanje podataka – Korisnički podaci i podaci aplikacija sadržani u memoriji imaju vek zadržavanja. Većina kartica pruža period zadržavanja podataka od 7 do 10 godina.

Važno je razumeti da je smart kartica efektivno kompjuter sa mnogim identičnim radnim izazovima. Ona ima IC koji spaja procesor i memoriju, logiku ugrađenu u procesor koja podržava različite servise, i aplikacije ugrađene u procesor i smeštene na EEPROM radi korišćenja na zahtev. One takođe zahtevaju upravljanje protokolom i upravljanje podacima.

2.11.1.3. Vrste kartica

U osnovi, postoje dve vrste smart kartica, koje se razlikuju u tome na koji način imaju interakciju sa drugim sistemima: kontaktne kartice, koje koriste fizički kontakt za

komunikaciju sa sistemima, ili bezkontaktne kartice, koje prave interfejs korišćenjem tehnologije blizine.

- Kontaktne kartice – Kontaktne kartice su retko samo objašnjavaju. Bazirane su na standardu ISO-7816-2, koji navodi ukupno osam električnih kontakata (u upotrebi je samo šest) za interakciju sa drugim sistemima ili uređajima. Kontakti na smart kartici obezbeđuju pristup različitim elementima usađenog IC.
- Bezkontaktne kartice – Kartice koje su zasnovane na komunikacijama blizine rastu u zahtevima i upotrebi. Imaju povećano prihvatanje iz razloga njihove trajnosti, primena u korišćenju, brzini i praktičnosti. Njihov dizajn eliminiše fizički element interakcije sa različitim sistemima, time eliminišući vrstu štete koja se javlja kod kontaktnih kartica sa pločicama ili magnetnim trakama. PCD obezbeđuje svu snagu i signalnu kontrolu za komunikaciju sa karticom. PCD proizvodi RF polje koje aktivira karticu kada je ona unutar petlje elektrometričkog polja. Frekvencija RF radnog polja je $13,56 \text{ MHz} \pm 7 \text{ kHz}$, i ono radi neprekidno unutar minimalnog i maksimalnog opsega snage.

2.11.1.4. Upotreba SMART kartica

Organizacije mogu da razmotre korišćenje smart kartica na mnoge načine: fizički pristup, sigurnost, a čak dodaci aplikacija. Iako svaki pomaže, vrednost leži u pojedinačnosti rešenja – a to je kartica.

Fizički pristup

Mnoge kompanije koriste verifikaciju pristupa zgradi u obliku obične kartice. Nije neobično da se novom zaposlenom izda pristupna kartica za omogućavanje ulaza u zgradu. Pored toga, ta ista kartica može da se iskoristi za određivanje različitih nivoa pristupa do unutrašnjih zona, unapređujući kontrolu kretanja zaposlenih. Korišćenje kartica za pristup može da obuhvati širok opseg rešenja, kao što su kontrolisanje ulaza na parking mesta, u garaže, puteve glavnog ulaza, soba sa podacima, spratove u zgradi, kabinete, itd. U većini slučajeva, pristupne kartice nose logo i naziv kompanije i imaju magnetnu traku za povezivanje sa kontrolnim sistemima. Međutim, neke organizacije koriste blizinske kartice da ostvare iste funkcije kao magnetna traka. Obično, kartica pruža jedinstveni identifikator, ništa neuobičajeno složeno, što omogućava centralnom sistemu da identifikuje karticu.

Provera povezanosti korisnika sa karticom za pristup parking mestu nije važno kao kada korisnik želi da uđe u centar podataka. Jednostavnost tradicionalnih pristupnih kartica ne pruža podatke koji mogu da potvrde vlasnika kartice. Danas, kako se spušta cena smart kartica i veći broj servisa je ugrađen u njih, kao što su magnetne trake i blizinsko očitavanje, korišćenje jedne smart kartice dobija rastuće zahteve.

Identifikacija zaposlenih

U slučaju identifikacije zaposlenog, pored nevidljivih informacija, na karticu su stavljene informacije o zaposlenom, kao što su to fotografija, ime, imenovanje i odsek.

Prijavljivanje (logovanje)

Smart kartice imaju dve osnovne upotrebe za logovanje na sistem i aplikacije. Prva je PSSO, u kojoj su različite kombinacije korisničkog imena i lozinke smeštene na smart karticu i pristupa im se pod budućim izazovima potvrde. Druga, i možda najvažnija, upotreba smart kartice je za čuvanje digitalnih sertifikata. Sertifikati mogu da se koriste u kombinaciji sa asimetričnim kriptografskim funkcijama da omoguće jaku autentifikaciju korišćenjem kriptografije sa javnim ključem, dosta poboljšavajući identifikaciju i potvrdu datog korisnika.

2.11.2. PKI i SMART kartice

Najbolji način za razmatranje korišćenja smart kartica u kompanijama je razumevanje da smart kartica nije alat koji može da podrži višestruke funkcije. Međutim, često se meša smart kartica sa njenim usađenim servisima, kao što je to PKI i digitalni potpisi. Potrebno je razjasniti da je kartica sadržalac informacija, a logika u karticama podržava korišćenje tih podataka, ali da sama kartica nije pružalac širokog skupa servisa. Za digitalni potpis dokumenta, kao što je to e-pošta, kartica omogućava iskorišćenje kriptografskih funkcija sa privatnim ključem na siguran i proveren način. Aplikacija, u većini slučajeva, nije svesna da su privatni podaci poslati preko smart kartice. Preciznije rečeno, smart kartica ima interakciju sa korisnikom i sistemom da omogući korišćenje podataka. Kada se to dogodi, aplikacija će raditi korišćenjem operativnog sistema krajnjeg sistema ili drugih alata koji dozvoljavaju korišćenje podataka za transakciju.

2.12. Inteligentna obrada podataka

Inteligentna obrada podataka (eng. *data mining*) je postupak sortiranja preko velike količine podataka i uzimanje relevantnih informacija. Ona je opisana kao “netrivijalno izvlačenje podrazumevanih, prethodno nepoznatih i potencijalno korisnih informacija iz podataka”²⁸ i kao “nauka izvlačenja korisnih informacija iz velike količine kompleta iz baza podataka.”²⁹ Inteligentna obrada podataka u vezi sa planiranjem resursa kompanije je

²⁸ Frawley, W., Piatetsky-Shapiro, G., Matheus, C. *Knowledge Discovery in Databases: An Overview*, AI Magazine: pp. 213–228. jesen 1992.

²⁹ Hand, D., Mannila, H., Smyth, P., *Principles of Data Mining*, MIT Press, Cambridge, MA, 2001.

statistička i logička analiza velike grupe podataka o transakcijama, traženje obrazaca koje mogu da pomognu pri donošenju oblika.³⁰

2.12.1. Poreklo

Tradicionalno, poslovni analitičari su obavljali posao izvlačenja korisnih informacija iz zabeleženih podataka, ali povećanjem obima podataka u modernom poslovanju i nauka uključuje pristupe zasnovane na računaru. Pošto su paketi podataka porasli u veličini i kompleksnosti, prešlo se sa direktne ručne analize podataka na indirektnu, automatsku analizu podataka korišćenjem kompleksnijih i sofisticiranijih alata. Moderna tehnologija računara, mreža i senzora je dosta olakšala prikupljanje i organizaciju podataka. Međutim, prihvaćeni podaci moraju da se pretvore u informacije i znanje da bi postali korisni. Inteligentna obrada podataka je celokupan postupak primene metodologije zasnovane na računaru, uključujući nove tehnike za otkrivanje znanja, za podatke.³¹

Inteligentna obrada podataka identifikuje trendove unutar podataka koji prevazilaze obične analize. Korišćenjem sofisticiranih algoritama, korisnici (koji nisu statističari) imaju mogućnost da identifikuju ključne atribute poslovnih procesa i ciljne mogućnosti. Međutim, abdikcijom kontrole ovog procesa sa statističara na mašinu može da rezultuje pogrešno pozitivnim ili sveukupno beskorisnim rezultatima.

2.12.2. Poslovna primena

Inteligentna obrada podataka u primenama CRM može da značajno doprinese krajnjem rezultatu. Mogu da se koriste sofisticirane metode tako da se može predvideti na kojem kanalu i na koju ponudu će pojedinac najverovatnije da odgovori - od svih potencijalnih ponuda. U situacijama gde mnogo ljudi preduzima akciju bez ponude, može se koristiti model podizanja za utvrđivanje koji ljudi će imati najveće povećanje ako im se da ponuda.

Posao koji koristi inteligentnu obradu podataka može da vidi zaradu na investiciju, ali takođe on prepoznaje brojne predvidive modele koji ubrzo postaju veoma veliki.

Dobar primer primene su odeljenja za ljudske resurse. Ova vrsta obrade podataka omogućava identifikaciju karakteristika njihovih najuspešnijih zaposlenih. Dobijene informacije, kao što su univerziteti sa kojih dolaze najuspešniji zaposleni, može da pomogne HR da fokusira napore shodno tome.

Još jedan primer inteligentne obrade podataka, česti nazivan analiza potrošačke korpore, je u vezi sa korišćenjem u maloprodaji. Ova tehnika se svodi na beleženje narudžbina

³⁰ Monk, E., Wagner, B., *Concepts in Enterprise Resource Planning*, Second Edition. Thomson Course Technology, Boston, MA. 2006.

³¹ Kantardzic, M., *Data Mining: Concepts, Models, Methods, and Algorithms*, John Wiley & Sons, 2003.

kupaca, pomoću kojih ovaj sistem može da identifikuje kupce koji preferiraju jednu vrstu proizvoda više od druge.

2.13. Zaštita u E-bankarstvu

E-bankarstvo, koje je definisano kao elektronsko bankarstvo na osnovi Web-a, je područje visokog rizika sa potencijalom za značajne ekonomske gubitke. Visok rizik čini sigurnost primarnom brigom. U 2001. godini, procena je da je ukupno 17 milijardi dolara potrošeno na proizvode i servise za zaštitu informacija samo u SAD. Raznovrsnost korisnika e-bankarstva i nedostatak bilo koje specijalne obuke pre njegovog korišćenja takođe čini da lakoća korišćenja takođe postane primarna briga.

Trenutna varijanta e-bankarstva preko Weba je najnovija od nekoliko generacija sistema. Prva dobro poznata mašina je bila ATM koja pruža elektronski pristup do banaka klijenata. Nakon toga je nastalo telefonsko bankarstvo preko kojeg su korisnici zvali kompjuterski sistem njihove banke preko njihovog običnog telefona i koristili tipke telefona da obave bankarske transakcije. PC bankarstvo je zamenilo telefonsko bankarstvo i omogućilo korisnicima interakciju sa njihovom bankom preko kompjutera da dial-up modemsom konekcijom na telefonsku mrežu. Telefonsko i PC bankarstvo zahtevalo je troškove održavanja vezane za držanje koraka sa najmodernijim različitim modemima i sa izbegavanjem visoko komplikovanih postupaka instalacije. E-bankarstvo koristi web pretraživač za korisnički interfejs i Internet za prenos podataka i preuzimanje softvera, i tako ima potencijal za smanjenje troškova održavanja.

Za korisnike, e-bankarstvo daje trenutne informacije, sa 24-časovnim pristupom do bankarskih servisa – pored poznatog interfejsa pretraživača. Primarni servisi koje pružaju e-banke su transfer novca između ličnih računa pojedinca, plaćanje računa i provera salda računa. Zajmovi, berzanski poslovi, trgovina udelima, itd., su dodati ovim osnovnim servisima. Od kasnih 90tih godina prošlog veka, e-bankarstvo je naraslo od virtualne beznačajnosti do desetina miliona korisnika širom sveta, i usled njegovog velikog prodora, sistemi e-bankarstva moraju da se prilagode širokom opsegu korisnika.

2.13.1. Upotrebljiva sigurnost

Lozinka daje ilustrativni primer konflikta između sigurnosti i lakoće korišćenja, i, stoga, potrebe za konceptom upotrebljive sigurnosti. Dok lozinke kao što su imena osoba ili druge postojeće reči relativno lake da ih korisnik zapamti, one su slabe sa aspekta sigurnosti iz razloga što su ranjive na napade sa rečnikom. Jake lozinke (e.g., x7h!t%C9) su manje ranjive na napad, ali istovremeno teže za pamćenje.

Iako je sigurnost postala aspekt skoro bilo kog sistema, i korisnici su naviknuti na interakciju sa mehanizmima za kontrolu pristupa za, pored ostalog, personalne računare, naloge za e-poštu, i sajtove za e-trgovinu ili e-government, sigurnosna olakšanja takvih sistema su često manja od onih potpuno primenljivih.

Whitten i Tygar su 1999. godine sugerisali sledeću definiciju preko koje je moguće oceniti sisteme e-bankarstva: Softver u vezi sigurnosti je upotrebljiv ako su ljudi koji bi trebalo ga koristiti:

1. pouzdano svesni sigurnosnih zadataka koje treba da izvršavaju;
2. mogu da shvate kako da uspešno izvršavaju te zadatke;
3. ne prave opasne greške; i
4. da su dovoljno komforni sa interfejsom kako bi nastavili da ga koriste.

Ova definicija govori o efektivnosti (stavke 1 i 3), efikasnosti (stavke 1 do 3) i zadovoljstvu (stavka 4) softvera u vezi sigurnosti i stoga je u saglasnosti sa standardom ISO 9241-11 (iz 1998. godine).

Postoje dva načina na koja se mogu adekvatno oceniti ova definicija. Prvo, mnogi sigurnosni zadaci u e-bankarstvu su tesno integrisani u odgovarajuće zadatke e-bankarstva. Drugo, naglašava se da neke sigurnosne zadatke u e-bankarstvu projektanti sistema teško mogu unapred da predvide, što izgleda da je u suprotnosti sa pretpostavkom 1. Stoga, sigurnosni zadaci mogu da budu deo drugih zadataka, i možda ih nije moguće predvideti unapred.

3. Analiza starog i novog sistema SWIFTNet-a

3.1. Stari sistemi – BKE, MAC i SCR

Pošto su u pitanju odlazeći sistemi, ovde su izložene samo osnovne informacije. U nastavku ovog poglavlja nalazi se analiza novog sistema SWIFTNet-a, kao i prednosti u odnosu na stari sistem rada.

Bilateralna razmena ključeva (BKE – eng. *Bilateral Key Exchange*) je šema šifrovanja koju koristi SWIFT (eng. *Society for Worldwide Interbank Financial Telecommunications*).

Bilateralni ključ omogućava sigurnu komunikaciju širom SWIFT mreže. Tekst SWIFT poruke i ključ autentičnosti se koriste da generišu kôd za proveru autentičnosti poruke (MAC – eng. *Message Authentication Code*). MAC osigurava poreklo poruke i proveru autentičnosti sadržaja poruke. To se normalno postiže razmenom različitih SWIFT poruka, koje se specijalno koriste za uspostavljanje komunikacionog para.

BKE ključevi se generišu bilo manuelno unutar SWIFT softvera, ili automatski korišćenjem čitača sigurnosnih kartica (SCR – eng. *Secure Card Reader*).

Od 1994. godine do danas, kraja 2008. godine, ključevi korišćeni u čitačima kartica i sami ključevi za proveru autentičnosti su bili 1024-bitni RSA.

3.2. Opis SWIFTNet PKI

3.2.1. Uvod

SWIFTNet PKI je obavezni SWIFT proizvod koji se zahteva za obezbeđivanje SWIFTNet servisa. On se instalira zajedno sa SWIFTNet Link-om. SWIFT-ov portfolio interaktivnih komunikacionih servisa i proizvoda u vezi njih uključuju proizvode interfejsa SWIFTAlliance Gateway i SWIFTAlliance WebStation.³²

On pruža poslovne aplikacije sa mogućnostima provere autentičnosti, integriteta, poverljivosti i kontrole pristupa.

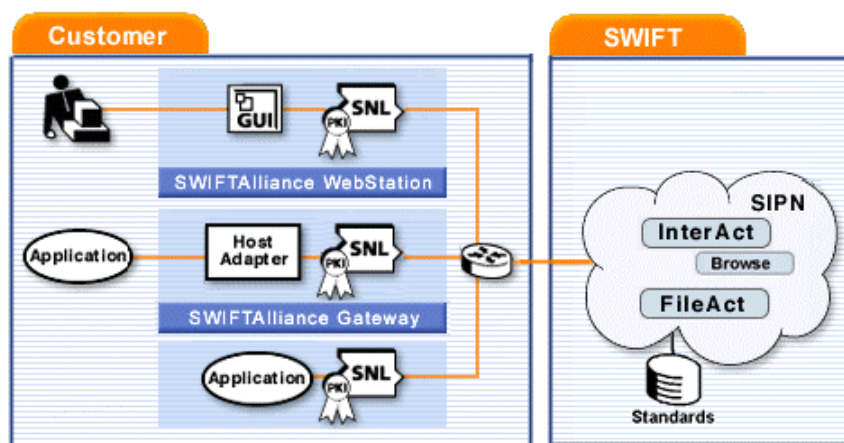
³² SWIFT, *SWIFTNet Public Key Infrastructure – PRODUCT OVERVIEW*, September 2002.

SWIFTNet PKI i SWIFTNet Link su obavezne komponente koje, zajedno, omogućavaju korišćenje SWIFTNet servisa koje nudi SWIFT preko svoje sigurne IP mreže.

SWIFTNet PKI obezbeđuje komplet programskih interfejsa aplikacije (API – eng. *Application Programming Interface*) koje direktno koristi aplikativni program. Ovi API kompleti omogućavaju aplikativnom programu klijenta da koristi funkcije za kriptografiju i kontrolu pristupa, kao i za dobijanje digitalnih sertifikata i upravljanje njima.

SWIFTNet PKI takođe obezbeđuje aplikaciju za krajnjeg korisnika koja služi za dobijanje digitalnih sertifikata i upravljanje njima.

Slika 9. SWIFT portfolio komunikacionih servisa



Izvor: SWIFT, *SWIFTNet Public Key Infrastructure – PRODUCT OVERVIEW*, September 2002, p. 1

3.2.2. Vrednosti za klijente

3.2.2.1. Uopšteno

SWIFT-ovi servis Infrastrukture sa javnim ključem (PKI) izdaje digitalne sertifikate finansijskim institucijama i korporacijama, time omogućavajući istovremeno poverljivu, neodrecivu, dokazivu i poverljivu komunikaciju preko SWIFTNet-a. Digitalni sertifikati pružaju najveći nivo provere autentičnosti za institucije, krajnje korisnike i servere.

3.2.2.2. Poverenje

Osnovni princip PKI je lanac poverenja. On počinje identitetom korespondenta, bazirano na validnosti sertifikata, a završava se digitalnim potpisom.

Primalac potpisane poruke ima poverenje u identitet poruke pošiljaoca i nemogućnost pošiljaoca da se odrekne poruke zbog postojanja sledećih garancija:

- Rigoroznog postupka za pretplatu korisnika na SWIFTNet PKI
- Pouzdanog postupka izdavanja sertifikata pretplatnicima
- Virtuelne nemogućnosti pravljenja lažnog sertifikata
- Virtuelne nemogućnosti reprodukovanja potpisa sa informacija sertifikata
- Obaveze da se odmah opozovu kompromitovani sertifikati
- Provere statusa sertifikata prilikom prijema poruke
- Veze između digitalnog sertifikata i sadržaja poruke preko digitalnog potpisa.

Nivo poverenja u sertifikate je određen rigoroznim postupkom registracije i opoziva. Ovi postupci su bazirani na SWIFTNet PKI - Opisu servisa. Ovaj dokument prevodi pravila, uloge i odgovornosti u stvarni PKI proces sa svojim specifičnim postupcima, pravilima i sporazumima za nivoe servisa (eng. *Service Level Agreements*). On je sastavni deo ugovornog odnosa između klijenata, kao i između klijenata i SWIFT-a. Sertifikati koje je izdao SWIFT eksplicitno se odnose na SWIFTNet PKI – Opis servisa.

U slučaju da je poverenje kompromitovano, SWIFT ima rigorozan postupak trenutnog opoziva. Na primer, poverenje može da bude kompromitovano pod sledećim okolnostima:

- kada je ukradena smart kartica ili je otkrivena lozinka (izlaganje javnog ključa)
- kada je prekinuta povezanost između vlasnika sertifikata i Registracionog tela (RA) kada zaposleni napušta kompaniju

U takvim slučajevima potrebno je proglasiti sertifikat, koji sadrži odgovarajući javni ključ, nevažećim i on mora da se trenutno opozove i onesposobi.

3.2.2.3. Garancije

Korisnik može da pretpostavi sledeće garancije za izdate sertifikate:

- **Autentičnost** – Klijentima je garantovan identitet stvaraoca bilo koje instrukcije, izjave, upita ili odgovora. Proverom potpisa, primalac poruke može da potvrdi da pošiljalac, koji je naveden u zaglavlju poruke, poseduje privatni ključ koji je korišćen za potpisivanje poruke.
- **Integritet** – Klijentima je garantovano da su podaci koje primaju potpuno odgovaraju originalu koji je napravio pošiljalac. Proverom potpisa, primalac poruke može da potvrdi da sadržaj poruke nije izmenjen za vreme prenosa.

- **Nemogućnost odricanja slanja** – Klijenti mogu da dokažu da je podneti stvaralac efektivno potpisnik poruke. To je iz razloga što je stvaralac jedini vlasnik jedinstvenog ključa za potpis, koji je potreban za stvaranje digitalnog potpisa. Ova garancija je zavisna od mogućnosti za opoziv sertifikata, po čemu vreme zahteva za opoziv može da se dokaže da je u vezi sa vremenom u kojem je poruka potpisana.
- **Kontrola pristupa** – Pristup pojedinca njegovom ili njenom privatnom ključu, koji je sačuvan u smart kartici, je povezan sa pristupom na SWIFTNet i kontroliše se preko privatne lozinke.
- **Poverljivost** – Opciono šifrovanje poruke na više nivoa garantuje da samo primalac, kome je ona namenjena, može da je pročita i da interpretira podatke. To je iz razloga što je primalac jedini vlasnik jedinstvenog ključa za dešifrovanje.

Digitalni potpis na osnovi PKI menja kôd za proveru autentičnosti poruke (MAC) koji je do skora korišćen u finansijskim mrežama.

3.2.3. Rigorozan PKI

Pre dobijanja poverljivog sertifikata, institucije se registruju i sertifikuju preko SWIFTNet PKI. Ova SWIFTNet PKI registracija i sertifikacija garantuje:

- **Jasno definisan postupak registracije** – Pre dobijanja pristupa do SWIFT Servisa, uključujući i SWIFTNet PKI, institucije se pažljivo proveravaju. Provera je bazirana na kriterijumima za ulazak koji se nalaze u statutu SWIFT-a. Pored toga, Službenici za sigurnost se primaju isključivo pod definisanim uslovima, imaju ograničene mogućnosti i, gde je to moguće, rade u parovima.
- **Okruženje brzoreagujuće konfiguracije** – Brzo uspostavljanje krajnjih korisnika i brz opoziv kompromitovanih sertifikata su zahtevi za sistem visokog nivoa poverenja. SWIFTNet PKI nudi onlajn sredstva za upravljanje krajnjim korisnicima i njihovim sertifikatima i njihovo potvrđivanje.
- **Radno okruženje sa rigoroznom odgovornošću (R&L)** – Da bi mogao da prihvati odgovornost za PKI procese, SWIFT i korisnik se zajedno obavezuju na radno okruženje sa jakim R&L. Radi prihvatanja odgovornosti za grešku, prevaru i propust, SWIFT implementira rigorozne unutrašnje procedure i kriterijume za kvalifikaciju softvera.
- **Potpuna sigurnost ključnih komponenti** – Sertifikaciono telo (CA) je fizički i operativno zaštićeno i izolovano od drugih servisa. Pored toga, komunikacija sa

Sertifikacionim telom je moguća samo od strane sertifikovanih Registracionih tela (RA) korišćenjem jakog i sigurnog protokola. Raspoloživost CA i imenika SWIFTNet-a je kritično za servis opoziva sertifikata. On se garantuje preko visokog stepena redundantnosti sistema.

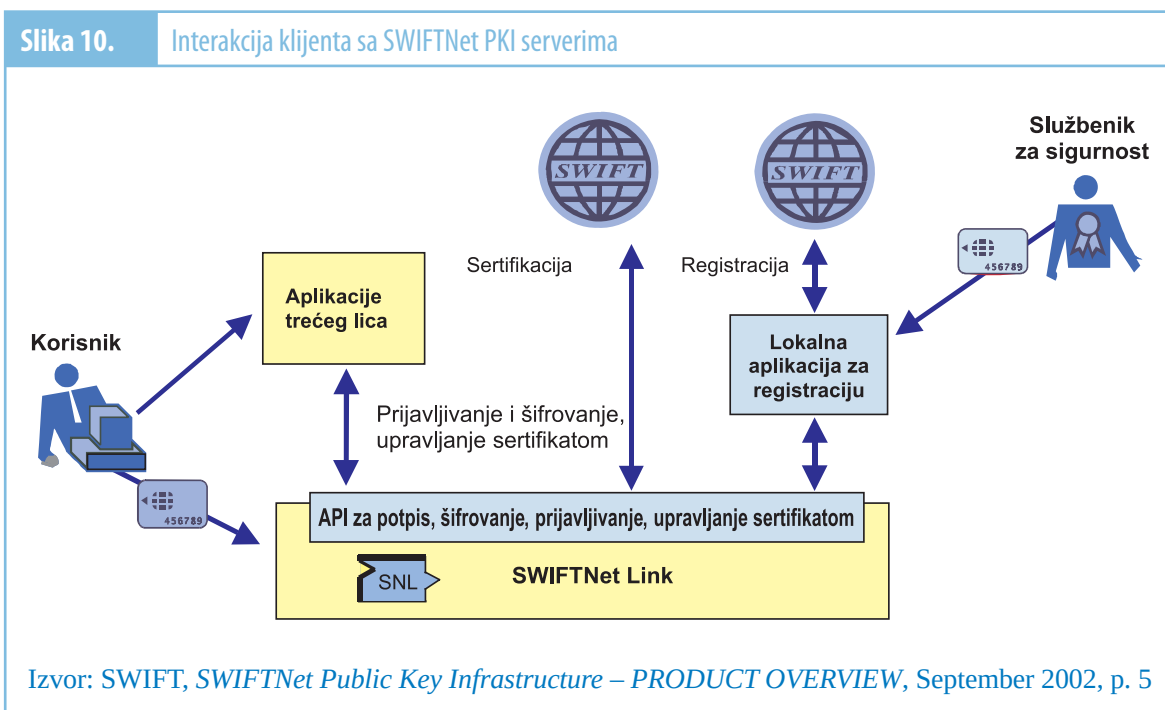
- **Snažno kriptografsko okruženje** – SWIFT koristi algoritme sa maksimalnim praktičnim dužinama ključa. Pored toga, gde je to moguće, privatni ključevi na serveru, kao i na strani klijenta, se generišu i čuvaju u hardveru i zaštićeni su preko lozinke.

Ova snažna PKI osigurava najbolju vrstu zaštite i poverenja za finansijsku komunikaciju, koja je posebno važna u interaktivnom i transakcijskom okruženju. Ona nudi dokazive autentičnosti poruka, nemogućnost odricanja porekla poruka, poverljive vremenske pečate i pojedinačno šifrovanje poruka.

3.2.4. Osobine i funkcije

3.2.4.1. PKI komponenta za klijente

Klijent PKI ima interakciju sa centralnim SWIFTNet PKI serverima, a to su servisi Registraciono telo (RA), Sertifikaciono telo (CA) i SWIFTNet imenik, kojima rukovodi SWIFT. PKI klijent se sastoji od API-ja za funkcije kriptografije i upravljanja sertifikatom, i gotove Lokalne aplikacije za registraciju (LRA – eng. *Local Registration Application*) za upravljanje sertifikatom.



- **Lokalna aplikacija za registraciju** – LRA isporučuje SWIFT kao aplikaciju ili je obezbeđuje treće lice na osnovi SWIFTNetLink API-ja. Sa LRA klijent može da uradi sledeće:
 - Registruje nove korisnike
 - Opozove sertifikate korisnika
 - Onemogućiti korisnike i ukloni njihove sertifikate iz SWIFTNet imenika

Ova aplikacija takođe kontroliše pristup korisnika sistemu i njihovim ključevima, a obezbeđuje i upravljanje lozinkama.
- **API-ji za kriptografiju i upravljanje sertifikatom** – API za kriptografiju obezbeđuje sigurnost poruke:
 - Potpisivanje poruke, kompletno, odnosno parcijalno
 - Verifikaciju potpisa i potvrdu sertifikata
 - Šifrovanje poruka, kompletno, odnosno parcijalno
 - Dešifrovanje poruka
 - Sertifikaciju korisnika
 - Automatsko obnavljanje ključa i sertifikata
 - Oporavak ključa i sertifikata korisnika

API za upravljanje sertifikatom pruža istu funkcionalnost kao i LRA.

3.2.4.2. Komponente PKI SWIFT-a

Komponente PKI SWIFT-a su:

- **Registraciono telo** – Registraciono telo (RA) ima centralnu ulogu u uspostavljanju lanca poverenja. Ono je odgovorno za pretplaćivanje institucija na SWIFT-Net PKI i poveravanje pretplata dodatnim korisnicima. Početna pretplata uključuje registraciju prva dva Službenika za sigurnost (SO), koji zatim koriste LRA za njihovu sopstvenu sertifikaciju i za izdavanje dodatnih zahteva za upravljanje sertifikatima do registracionog tela (RA).
- **Sertifikaciono telo** – Sertifikaciono telo (CA) proizvodi sertifikate i objavljuje ih u Imeniku sertifikata (eng. *Certificate Directory*). To se izvršava kada to zahteva PKI klijent i nakon provere od strane RA. Sistem CA je nalazi u jako zaštićenim zgradama u SWIFT Operativnim centrima. Jednako tome, pristup osoblja sistemu je rigorozno zaštićen. Iz razloga redundancije, CA se sastoji od višestrukih sistema koji se nalaze u različitim geografskim regijama.

- **SWIFTNet imenik** – SWIFTNet Imenik ima hijerarhijsku strukturu u saglasnosti sa X.500. Imenik sadrži:
 - Sertifikate korisnika za prijavljivanje i šifrovanje
 - Imena i attribute korisnika
 - Spiskove opoziva sertifikata

LRA može da nadgleda sadržaj SWIFTNet Imenika unutar okvira svoje sopstvene institucije. API za kriptografiju klijenta PKI može da povрати sertifikate iz Imenika ili može da pogleda Spisak opoziva sertifikata (CRL – eng. *Certificate Revocation List*).

CA i RA jedini mogu da kreiraju ili modifikuju sadržaj SWIFTNet Imenika.

3.2.4.3. Ključevi

Generisanje ključeva

PKI je baziran na parovima asimetričnih ključeva. U SWIFTNet PKI, generisana su dva odvojena para ključeva: jedan par ključa za potpisivanje i drugi za šifrovanje. Svaki par se sastoji od javnog i privatnog ključa.

Javne ključeve je sertifikovao CA i oni su publikovani kao sertifikati u Imeniku sertifikata (eng. *Certificate Directory*). Privatni ključevi su u ekskluzivnom vlasništvu korisnika. Korisnik mora da vodi računa o njihovoj privatnosti.

Ključevi su kreirani za vreme procesa sertifikacije i dugački su 1024 bita. Datumi produženja i prestanka važnosti ključeva su definisani u Izjavi o praksi sertifikacije (eng. *Certification Practices Statement*).

Čuvanje ključa

Da bi se sačuvao koncept nemogućnosti odricanja slanja, privatni ključ za potpisivanje ne sme da se otkriva i stoga nikad ne sme da napusti svoj medijum za čuvanje.

Ključevi se čuvaju u hardveru. Na smart karticama se čuvaju ključevi koje poseduje osoba, a na disku ključevi koje koristi aplikacija. Kao medijum za čuvanje na raspolaganju su hardverski sigurnosni moduli (HSM – eng. *hardware security modules*). Ključevi su zaštićeni lozinkom. Smart kartice, čitači kartica i HSM uređaji su standardni proizvodi, koji su prisutni na tržištu i koje je kvalifikovao SWIFT.

Digitalno potpisivanje i šifrovanje

U sistemu SWIFTNet PKI, pojedinačni vlasnik privatnih ključeva može da potpiše i dešifruje poruke. Korespondenti koriste javne ključeve, sadržane u sertifikatima, da provere potpis ili da šifruju poruke.

Nemogućnost odricanja slanja

Potpisane poruke isporučuju dokaz porekla s obzirom da vlasnik privatnog ključa za potpisivanje jedini može da proizvede potpis.

3.2.4.4. Digitalni sertifikati

Sertifikat je elektronski fajl potpisan od strane CA koji neopozivo identifikuje vlasnika ključeva i u stvari sadrži javni ključ. On garantuje da vlasnik poseduje odgovarajući privatni ključ. Sistem SWIFTNet PKI obezbeđuje svakom korisniku verifikaciju potpisa i sertifikat šifrovanja.

Pored ostalog, sertifikat sadrži sledeće:

- Identitet vlasnika
- Identitet izdavanja CA
- Serijski broj sertifikata
- Javni ključ
- Datum startovanja i datum isticanja
- ID polise za poslovne sertifikate
- Potpis CA

Sertifikati sistema SWIFTNet PKI su u saglasnosti sa formatom X.509, imaju verziju 3 i čuvaju se u SWIFTNet Imeniku.

Potvrda sertifikata

Sertifikati moraju da imaju mogućnost efikasnog povrata. Stoga, korisnik mora da bude u direktnoj komunikaciji sa imenikom. Ovaj imenik mora da bude autentičan, što znači da korisnik mora da bude u mogućnosti da potvrdi da se nalazi u imeniku SWIFT-a.

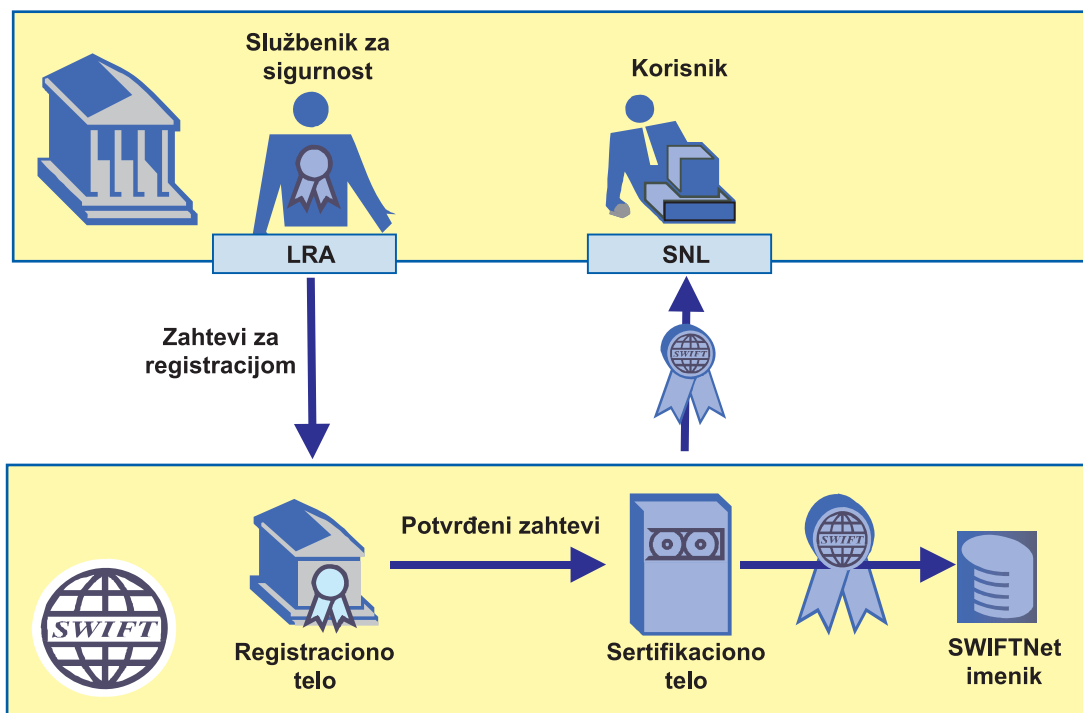
- Sertifikat CA mora da bude autentičan. Stoga, korisnik mora da potvrdi potpis CA na sertifikatu CA koristeći sertifikat CA i proverom otiska prsta.
- Sertifikat CA mora da bude važeći. Stoga, korisnik mora da proveriti Datume startovanja i isticanja sertifikata. Takođe, korisnik mora da proveriti da sertifikat nije opozvan.

Ove funkcije su obezbeđene automatski preko PKI klijenta.

3.2.5. Sertifikaciono telo

Službenik (eng. *Security Officer*) za sigurnost koristi LRA za administraciju sertifikata unutar okvira svoje sopstvene institucije. I službenik za sigurnost i korisnik koriste LRA za dobijanje svojih sertifikata. To ilustruje sledeća slika:

Slika 11. Sertifikaciono telo



Izvor: SWIFT, *SWIFTNet Public Key Infrastructure – PRODUCT OVERVIEW*, September 2002, p. 8

3.2.5.1. Registracija

Službenici za sigurnost (SO) kreiraju korisnike u SWIFTNet Imeniku. Ovi korisnici potom mogu da budu sertifikovani. SO identifikuje korisnike dodeljujući im formalno X.500 ime, (eng. *Distinguished Name*). Korisnici dobijaju registrovani status samo nakon što su definisani u SWIFTNet Imeniku.

3.2.5.2. Ko dobija sertifikaciju

Institucija odlučuje ko ili šta dobija sertifikaciju. Obično, sertifikati se izdaju zaposlenima ili poslovnim entitetima, kao što su to departmani. Sertifikate zatim koriste pojedinci ili aplikacije u ime poslovnih entiteta.

3.2.5.3. Priprema za sertifikaciju

U ovom koraku, Službenik za sigurnost zahteva od RA da postavi registrovanog korisnika za sertifikaciju. CA postavlja status korisnika da bude spreman za sertifikaciju, i on generiše aktivacione tajne koje će korisniku trebati u procesu sertifikacije. RA vraća ove aktivacione tajne Službeniku za sigurnost, koji ih prosleđuje korisniku.

3.2.5.4. Sertifikacija

Da bi se sertifikovao, krajnji korisnik primenjuje aktivacione tajne primljene od strane Službenika za sigurnost. Zatim se generišu parovi ključeva i javne ključeve sertifikuje CA. Sertifikati korisnika za potpisivanje i šifrovanje se objavljuju u SWIFTNet Imeniku.

3.2.5.5. Priprema za povraćaj

Ako korisnici izgube svoje ključeve ili lozinku, onda će Službenik za sigurnost podneti zahtev u RA da postavi korisnika za povraćaj podataka. CA će zatim generisati i vratiti nove aktivacione tajne koje će korisniku biti potrebne postupku povraćaja.

3.2.5.6. Povraćaj

Kao i kod sertifikacije, korisnik pokreće postupak povraćaja ako je on ili ona spreman za ovaj proces. Uspešan povraćaj kao rezultat ima nove ključeve i dva nova sertifikata su publikovana u SWIFTNet Imeniku.

3.2.5.7. Opoziv

Službenik za sigurnost mora da opozove sertifikate kad god je prekinuta poverljiva relacija sa njihovim vlasnikom. To je uglavnom iz razloga što je ključ kompromitovan. Na primer kada su izgubljene ili ukradene lozinke, smart kartice ili ključevi. Opoziv sertifikata čini ih beskorisnim. Opozvani sertifikati su publikovani u Spisku opoziva sertifikata (CRL) u SWIFTNet Imeniku.

Ako se to zahteva, korisnik može da se povрати nakon opoziva.

3.2.5.8. Onemogućavanje

Onemogućavanjem korisnika, Službenik za sigurnost ukida automatsko obnavljanje sertifikata i uklanja ih iz SWIFTNet Imenika. To je tipično slučaj za korisnike kojima više nisu potrebni njihovi sertifikati.

3.2.5.9. Oflajn zahtevi

U slučaju da Službenici za sigurnost ne mogu da izvrše onlajn opozivi ili povraćaj korisnika, potrebno je kontaktirati SWIFT radi manuelne intervencije. Bilo koji Službenik za sigurnost, koji je registrovan kod SWIFT-a, može da zahteva od SWIFT-a manuelnu intervenciju.

3.2.6. Glosar

Tabela 1. – Glosar termina korišćenih za opis SWIFTNet PKI

Originalan termin (na engleskom)	Prevod	Akronim ili skraćenica	Objašnjenje
Application Programming Interface	Programski interfejs aplikacije	API	Skup rutina koje aplikativni program koristi za upravljanjem izvršavanja procedura od strane operativnog sistema računara.
Authentication	Provera autentičnosti (autentifikacija)	–	Postupak koji se koristi da osigura da je osoba za koju on/ona tvrdi da jesu, ili proveri integritet specifične informacije. Poruka u proveri autentičnosti uključuje određivanje njenog izvora i proveru da ona nije promenjena ili zamenjena u prenosu.
Certificate	Sertifikat	–	Jedinica informacije sadržane u fajl koja, u najmanju ruku, navodi njenog izdavaoca, javni ključ, pokazuje korisnika koji čuva privatni ključ koji odgovara navedenom javnom ključu i digitalno je potpisana od strane sertifikacionog tela.
Certification Authority	Sertifikaciono telo	CA	Centralni sistem u SWIFT-u za pravljenje i publikovanje digitalnih sertifikata.
Certificate Practices Statement	Izjava o praksi sertifikacije	CPS	Izjava o praksi koje Sertifikaciono telo SWIFT-a angažuje prilikom izdavanja sertifikata.
Certificate Revocation List	Spisak opoziva sertifikata	CRL	Spisak svih opozvanih sertifikata koje je publikovalo Sertifikaciono telo SWIFT-a u centralnom imeniku i učinilo ih raspoloživim onlajn svim PKI klijentima.
Encryption	Šifrovanje	–	Činjenje sadržaja poruke nečitljivim putem šifrovanja. Dešifrovanje ima obrnuto dejstvo.
Hardware Security Module	Hardverski sigurnosni modul	HSM	Hardverski medijum za čuvanje ključeva.
Local Registration Application	Lokalna aplikacija za registraciju	LRA	Aplikacija koju Službenik za sigurnost koristi za registrovanje korisnika institucija i za upravljanje njihovim sertifikatima.

Originalan termin (na engleskom)	Prevod	Akronim ili skraćenica	Objašnjenje
PKI Cryptographic Module	Kriptografski modul PKI	–	Softver na strani kupca za zaštitu poruka i upravljanje sertifikatima. On izvršava stvarno potpisivanje, proveru potpisa, šifrovanje/dešifrovanje i upravlja jedinstvenim privatnim ključem kupca i njegovih sertifikata. On se isporučuje kao deo proizvoda SWIFTNet Link
Public Key Infrastructure	Infrastruktura sa javnim ključem	PKI	Infrastruktura od koje se zahteva da daje sigurnosne servise bazirane na asimetričnoj kriptografiji.
Registration Authority	Registraciono telo	RA	Telo u organizaciji SWIFT koje je odgovorno za identifikaciju i autentifikaciju institucije i inicijalnih korisnika SWIFT PKI, kao što su Službenici za sigurnost kod institucije.
Security Officer	Službenik za sigurnost	SO	Osoba odgovorna za manipulisanje sigurnosnim pitanjima za finansijske institucije.
Signature	Potpis	–	Matematički rezultat izračunat iz jedinice digitalne informacije i privatnog ključa. Digitalni potpis baziran na PKI je zamenio MAC, koji je do skora korišćen u finansijskim mrežama.
SWIFTAlliance	SWIFTAlliance	–	Naziv SWIFT-ovog brenda za opseg proizvoda interfejsa za povezivanje na SWIFT servise.
SWIFTNet	SWIFTNet	–	Naziv SWIFT-ovog brenda za sve servise za mrežu i procesiranje transakcija.
SWIFTNet Directory	SWIFTNet Imenik	–	Infrastruktura koja omogućava SWIFTNet Link-u da pogleda i povрати različite korisnike klijenta i njihove javne atribute.
SWIFTNet FileAct	SWIFTNet FileAct	–	SWIFTNet FileAct je servis za prenos fajlova koji podržava razmenu fajlova koji sadrže puno podataka.
SWIFTNet InterAct	SWIFTNet InterAct	–	SWIFTNet InterAct osigurava sigurnu, interaktivnu komunikaciju u realnom vremenu između dve strane preko sigurne IP mreže.
SWIFTNet Link	SWIFTNet Link	–	Obavezni softverski proizvod SWIFT-a za pristup svim SWIFTNet servisima. SWIFTNet Link povezuje kupca na SWIFTNet servise.
SWIFTNet PKI	SWIFTNet PKI	–	Obavezni sigurnosni softver i hardver SWIFT-a instaliran zajedno sa SWIFTNet Link-om.

3.3. Poređenje starog i novog sistema

Nakon opisa elemenata starog i novog sistema, moguće je izvršiti analizu promena i odgovoriti na pitanja šta je promenjeno, kako je izvršena promena na novi sistem i koje su prednosti proizišle iz prelaska na Infrastrukturu sa javnim ključem (PKI).

3.3.1. Šta je promenjeno?

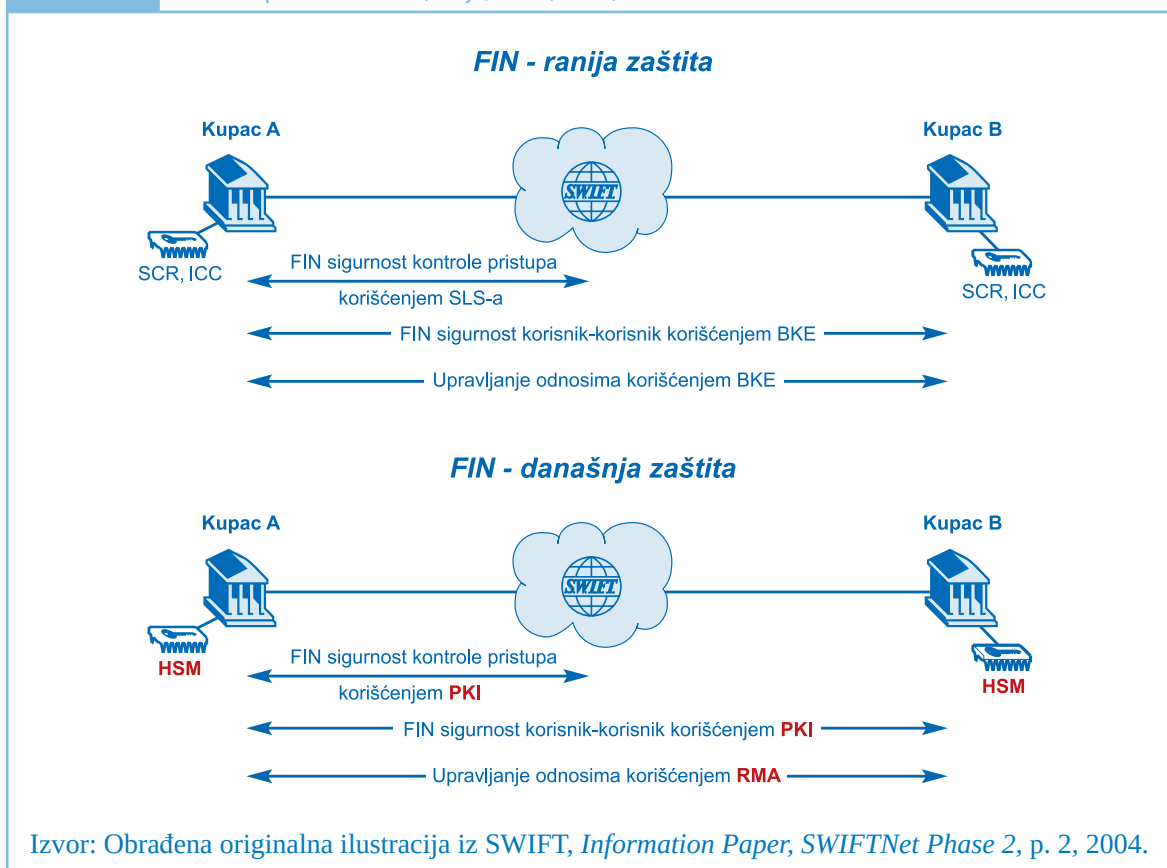
Pristupni kôdovi, koji su ranije korišćeni za pristup FIN servisu zamenjeni su digitalnim potpisima.

Digitalni potpisi takođe služe i kao osnova za proveru autentičnosti poruke na relaciji korisnik-korisnik, menjajući stare kôdove za proveru autentičnosti poruke (MAC) koji su ranije generisani i verifikovani korišćenjem bilateralno razmenjenih ključeva (BKE).

Kao zamena za ranije čitače sigurnosnih kartica (SCR i ICC), predstavljeni su i ušli u upotrebu novi hardverski uređaji otporni na spoljne uticaje, poznati kao Hardverski sigurnosni moduli (HSM).

Na narednom prikazu današnje zaštite, crvenom bojom su istaknuta mesta promene.

Slika 12. Paralelni prikaz rada BKE (ranije) i PKI (danas)



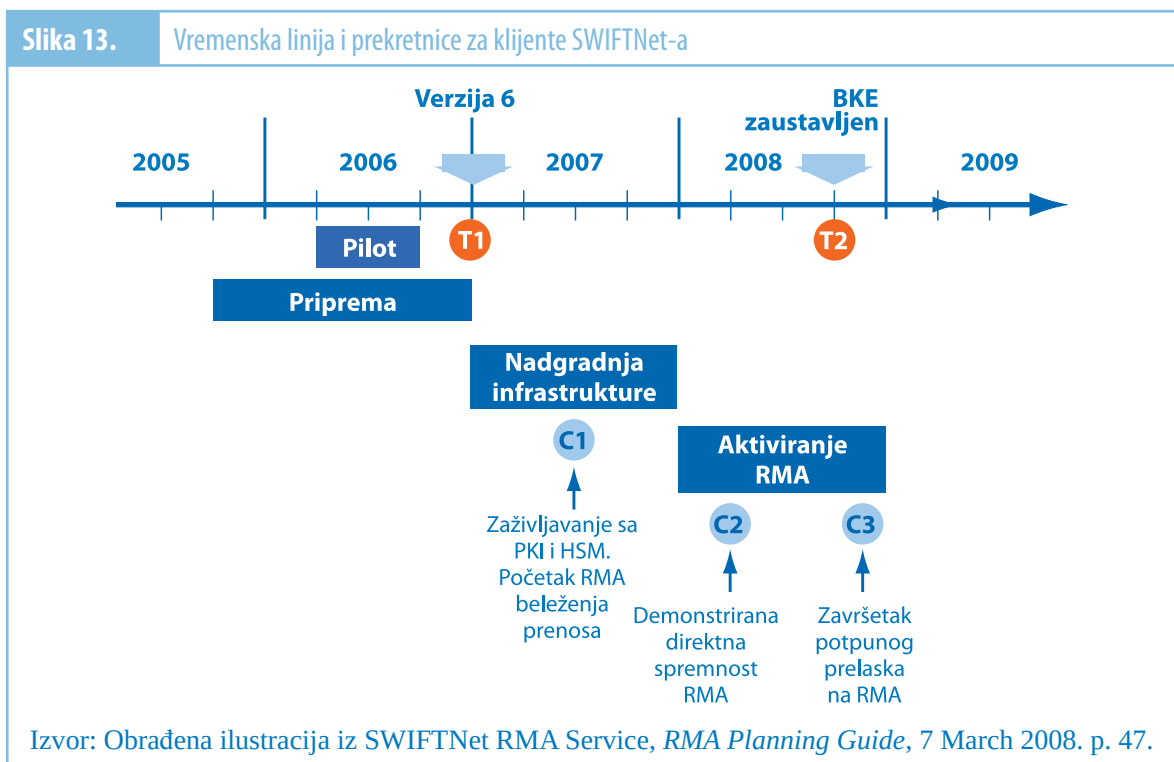
3.3.1.1. Nova aplikacija

Nova aplikacija za upravljanje odnosima (RMA – eng. *relationship management application*) je zamenila stari model bilateralne razmene ključa (BKE). On osigurava da svaki korisnik SWIFT-a može da odražava poslovne odnose koje imaju u mestu, obezbeđujući punu kontrolu preko prenosa koji se prima od njihovih korespondenata. RMA može da se koristi sa svim servisima baziranim na SWIFTNet-u. On čuva CRM informacije i ima interakciju sa relevantnim interfejsom da obezbedi da se pošalje isključivo prenos za koji postoji autorizacija. RMA i BKE sprečavaju neželjen autentifikovani prenos sa izvora. Pored toga, RMA je jednostavan za rad i raspoloživ za sva rešenja bazirana na SWIFTNet-u, a ne samo FIN.

3.3.1.2. Zaštita sigurnosnog ključa

BKE se oslanjao na privatne čitače sigurnosnih kartica (SCR – eng. *Secure Card Reader*). Iako su oni i dalje veoma sigurni, SCR se približava granici svojeg tehnološkog životnog ciklusa. Predstavljanjem i uvođenjem HSM-a na SWIFTNet-u, korisnici SWIFT-a će izvući koristi od najnovije sigurnosne tehnologije. HSM je uređaj otporan na spoljne uticaje koji se koristi za čuvanje različitih osetljivih podataka. U slučaju SWIFTNet PKI, HSM se koristi za čuvanje privatnog ključa(ključeva) korisnika. U upotrebi su dva tipa HSM-a: zasebnog HSM za korisnike sa malim obimom poslovanja i HSM bazirane na LAN vezi napravljene za korisnike sa velikim obimom poslovanja.

3.3.2. Faze prelaska na novi sistem



- **Prekretnica T1 (2. januar 2007. godine)**

Od tog datuma sve komponente SWIFTNet faze 2 su raspoložive od SWIFT-a.

- **Prekretnica C1 (2007. godina)**

Klijenti su završili infrastrukturnu nadgradnju. Klijenti su instalirali SNL Verziju 6 i pripadajući softver interfejsa SWIFTNet FIN. Sertifikati, koje koriste klijenti za SWIFTNet FIN, se nalaze na uređajima HSM. Korisnici mogu da se uloguju na direktni SWIFTNet FIN sa protokolom verzije 3, i šalju direktne, dvostruko potpisane SWIFTNet FIN poruke.

Poslate poruke su imale dvostruki potpis na sledeći način:

- jednom sa MAC potpisom računatim preko BKE ključa
- jednom sa PKI potpisom računatim u uređaju HSM

Interfejs SWIFTNet FIN automatski je pokrenuo beleženje RMA prenosa.

- **Početak zaživljavanja RMA servisa (januar 2008. godine)**

Ovo je bio najraniji datum kada su korisnici mogli da se aktiviraju na direktnom RMA servisu.

- **Pre prekretnice C2 (prvi i drugi kvartal 2008. godine)**

Demonstrirana spremnost za izvršavanje direktnog RMA.

- **Prekretnica T2 (kraj septembra 2008. godine)**

Korisnici više ne mogu da koriste BKE za održavanje međusobnih relacija, a za to koriste direktan RMA, i mogu da koriste pune prednosti iz novih mogućnosti koje nudi RMA.

- **Prekretnica C3 (četvrti kvartal 2008. godine)**

Klijenti završavaju kompletan prelazak na RMA. Prestalo je beleženje RMA, prestalo je korišćenje BKE ključeva i zaustavljeno je dvostruko potpisivanje. Nakon što su svi korisnici dostigli C3, migracija SWIFTNet Faza 2 je završena.

- **Prekretnica T3 (planirana u 2009. godini)**

SWIFT sistem u potpunosti odbija poruke sa dvostrukim potpisom.

3.3.3. Prednosti prelaska na novi sistem

Prelazak na PKI pruža sledeće prednosti:

- Pобољшanje sigurnosti za SWIFTNet FIN: stari sigurnosni mehanizmi SWIFTNet FIN-a su se oslanjali na čitače kartica SCR/BCR i ICC. Iako su ovi čitači kartica i smart kartice i dalje sigurne, oni se približavaju kraju njihovog veka trajanja i stoga su zamenjeni sa PKI.
- Jačanje PKI: SWIFT je pojačao PKI sigurnost uvođenjem uređaja koji su otporni na spoljne uticaje, poznate kao Hardverski sigurnosni modul (HSM – eng. *Hardware Security Modules*), da bi garantovao siguran smeštaj PKI tajni.
- Jedan sigurnosni mehanizam za sve SWIFTNet servise: SWIFTNet PKI menja stare sigurnosne mehanizme za FIN i stoga je napredovao do jednog prozora za sve SWIFTNet servise i smanjuje trošak korišćenja držanjem dva posebna sigurnosna modela.
- Jednostavnije upravljanje ključem: sa SWIFTNet PKI, upravlja se isključivo sopstvenim ključevima i nije potrebno razmenjivanje ključeva sa svakim od korespondenata (kao u predašnjem BKE svetu), i time smanjuje potreban napor kao i rizik od greške.

4. Zaključna razmatranja

Iz istorijata protokola i Interneta jasno se vidi osnova nastanka svetske mreže. Porastom broja operativnih mreža i korisnika paralelno se odvijalo stalno prilagođavanje protokola i razvoj savremenih računarskih mreža kao jednog od bitnih elemenata za njihovo međusobno povezivanje.

E-bankarstvo, kao jedna od najzastupljenijih oblasti e-poslovanja, takođe je nastalo zbog prednosti korišćenja moderne tehnologije za naprednije i rentabilnije poslovanje. Jedan od primera elektronske finansijske institucije je SWIFT, svetsko udruženje za interbankarske finansijske telekomunikacije. SWIFT, koji je osnovan 1973. godine, predstavlja dobar primer korišćenja najnovijih tehnoloških i naučnih rešenja u praksi. Pored toga, stalan rast broja korisnika SWIFT-a kao i broja razmenjenih poruka između njih, motivisalo je menadžment ove organizacije da pripremi i realizuje najnoviju modernizaciju sistema, koja je za cilj imala da svi korisnici pređu na novi sistem rada do kraja 2008. godine i da se sa starim sistemom rada raskrsti u prvom kvartalu 2009. godine. Sa računarskog aspekta, ova promena se može uopšteno nazvati “Prelazak SWIFT mreže na infrastrukturu sa javnim ključem”.

PKI predstavlja kombinaciju hardverskih i softverskih elemenata, ljudi, politika i procedura neophodnih za generisanje, skladištenje, upravljanje, distribuciju i opoziv digitalnih sertifikata. Osnovna uloga je uspostavljanje digitalnog identiteta subjekata u okviru mreže baziranog na digitalnim sertifikatima, čime se stvara pogodno okruženje za realizaciju drugih bezbednosnih servisa, prvenstveno onih kod kojih je od značaja autentičnost subjekata koji komuniciraju. Navedene karakteristike su bile ključne za menadžment SWIFT-a da pređene na PKI i odrekne se starog BKE sistema rada, iako je on i dalje bio izuzetno siguran ali mu se bližio kraj veka eksploatacije. Pored prelaska sa BKE na PKI, paralelno su zamenjeni i uređaji za čuvanje ključeva uvedena je nova aplikacija za upravljanje odnosima (RMA).

Šta je promenjeno?

Prilikom prelaska sa starog na novi sistem rada SWIFTNet-a napravljene su sledeće značajne promene:

- Pristupni kôdovi su zamenjeni digitalnim potpisima.
- Kôdovi za proveru autentičnosti poruke su takođe zamenjeni digitalnim potpisom.

- Za čuvanje privatnog ključa(ključeva) korisnika ranije su korišćeni čitači sigurnosnih kartica (SCR i ICC), koji su sada zamenjeni sa dva nova tipa hardverskih uređaja otpornih na spoljne uticaje (HSM).
- Nova aplikacija za upravljanje odnosima (RMA) je zamenila stari model bilateralne razmene ključa (BKE)

Kako je izvršena promena?

Prelazak na novi sistem je rađen u unapred definisanim fazama, a ispoštovane su sve planirane prekretnice. Tokom promene, paralelno je radio novi i stari sistem. Početkom 2009. godine, planirano je potpuno isključivanje starog sistema.

Koje su stvarne prednosti prelaska na novi sistem rada?

- Poboljšanje sigurnosti – za SWIFTNet FIN prelakom na PKI.
- Jačanje PKI – uvođenjem uređaja koji su otporni na spoljne uticaje (HSM) da bi garantovao siguran smeštaj PKI tajni.
- Jedan sigurnosni mehanizam – jedan prozor za sve SWIFTNet servise.
- Jednostavnije upravljanje ključem – upravlja se isključivo sopstvenim ključevima i nije potrebno razmenjivanje ključeva sa svakim od korespondenata. Ujedno smanjen potreban napor i rizik od greške.

Očekivani doprinosi ovog rada su:

- Saznanje o tome šta je promenjeno u SWIFT mreži i zašto, pogotovo imajući u vidu da je ona do sada bila sinonim sigurne mreže.
- Kako je izvršena promena bez prekidanja rada sistema, koji je inače dostupan 24 sata dnevno/7 dana u nedelji tokom cele godine.
- Prednosti koje je jedan kvalitetan model zaštite doneo SWIFT mreži samo iz razloga što je njegova implementacija urađena striktno.
- Svakako, biće interesantna mogućnost budućeg istraživanja. Tim koji je projektovao rad SWIFT mreže preko Infrastrukture sa javnim ključem, svakako je odredio okvire zastarevanja ovog novog sistema rada. Iako će do tog trenutka proći možda i više od deset godina, on je neminovan. Stoga, u budućim istraživanjima moći će da se prati dalja promena i prilagođavanje sistema izazovima modernog tehnološkog i naučnog sveta. Takođe, u bližnoj budućnosti moći će da se i preciznije predvidi da li će te promene biti parcijalne ili sveobuhvatne.

5. Literatura

1. Beekman, G., Rathswohl, E.J., *Computer Confluence*, Prentice Hall, 2003, NJ, USA
2. Božidar Radenković, *Elektronsko poslovanje*, FON, Beograd.
3. Frawley, W., Piatetsky-Shapiro, G., Matheus, C. *Knowledge Discovery in Databases: An Overview*, AI Magazine, 1992.
4. Groth, D., Beer, M. de, Wall, D., *i-Net+ Study Guide*, 2000.
5. Heimann, J., *Oracle9I for eBusiness: Security for your eBusiness Applications*, USA, 2001. <http://otn.oracle.com/deploy/security/pdf/oow00/ebiz.pdf>
6. Hand, D., Mannila, H., Smyth, P., *Principles of Data Mining*, MIT Press, Cambridge, MA, 2001.
7. Hertzum, M., Jørgensen, N., Nørgaard, M. *Usable Security and E-Banking: Ease of Use vis-à-vis Security*, Roskilde University, Denmark, 2004.
8. Kantardzic, M., *Data Mining: Concepts, Models, Methods, and Algorithms*, John Wiley & Sons, 2003.
9. Naugle, M., *Illustrated TCP/IP*, John Wiley & Sons, 1999.
10. Microsoft, *Encarta Encyclopedia Deluxe 2004*.
11. Microsoft, *Računarski rečnik*, Prevod petog izdanja, CET, Beograd, 2003.
12. Milosavljević, M., Grubor, G., *Osnovi bezbednosti i zaštite informacionih sistema*, Fakultet za poslovnu informatiku, Univerzitet Singidunum, Beograd, 2006. godine.
13. Monk, E., Wagner, B., *Concepts in Enterprise Resource Planning, Second Edition*. Thomson Course Technology, Boston, MA. 2006.
14. Roberts A., Murray, G., Findlay, P., *Collaborative Working*, UK, 2001, http://www.firsteBusiness.co.uk/whitepapers/pdf/WP_Collaborative%20Working.pdf
15. Saunders, M., Lewis, P., Thornhill, A., *Research Methods for Business Students, 3rd Edition*, Harlow, Prentice Hall, 2003.

16. Stankić, R., Marinčić, D., *Računarstvo i informatika*, ZUNS, Beograd, 2003.
17. SWIFT, *Information Paper – SWIFTNet Phase 2*, 2004.
18. SWIFT, *SWIFTNet Public Key Infrastructure – PRODUCT OVERVIEW*, September 2002.
19. SWIFT, *SWIFTNet RMA Service – RMA Planning Guide*, 7 March 2008.
20. *The Internet Encyclopedia*, Vol. 1-3, John Wiley & Sons, New Jersey, 2004.
21. Tipton, H.F., Krause, M., *Information Security Management Handbook*, 6th Edition, Auerbach Publications, 2007.