Sigurnost i privatnost elektroničke trgovine

Naglić, Luka

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

Luka Naglić

SIGURNOST I PRIVATNOST ELEKTRONIČKE TRGOVINE

Završni rad

Pula, 2016.

Sveučilište Jurja Dobrile u Puli
Fakultet ekonomije i turizma
«Dr. Mijo Mirković»

Luka Naglić

SIGURNOST I PRIVATNOST ELEKTRONIČKE TRGOVINE

Završni rad

JMBAG: 0303036769 , redoviti student

Studijski smjer: Poslovna informatika

Predmet:Elektroničko poslovanje

Mentor: prof.dr.sc. Vanja Bevanda

Pula, 2016.

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student:

U Puli, . . 2016. _____

IZJAVA O AKADEMSKOJ ČESTITOSTI

Ja, dolje potpisani _____, kandidat za prvostupnika _____ovime izjavljujem da je ovaj Završni rad rezultat isključivo mojega vlastitog rada, da se temelji na mojim istraživanjima te da se oslanja na objavljenu literaturu kao što to pokazuju korištene bilješke i bibliografija. Izjavljujem da niti jedan dio Završnog rada nije napisan na nedozvoljen način, odnosno da je prepisan iz kojega necitiranog rada, te da ikoji dio rada krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za koji drugi rad pri bilo kojoj drugoj visokoškolskoj, znanstvenoj ili radnoj ustanovi.

Student:

U Puli, . . 2016. _____

Sadržaj

UVOD

1. INTERNET I ELEKTRONIČKO POSLOVANJE 1

1.1 Internet 1

1.2. Ektranet i Intranet 1

1.3. Pojam elektroničkog poslovanja 2

1.4. Okruženje webocentrične trvtke 3

1.5. Sustav elektroničkog poslovanja 4

1.6. Modeli elektroničkog poslovanja prema kriteriju obavljenih poslova 4

1.6.1. Prodaja vlasitith dobara i usluga 4

1.6.2. Elektroničko trgovanje 5

1.6.2.1. Aspekti socijalnog i institucionalnog elektroničkog trgovanja 7

1.6.2.2. Modeli elektroničke trgovine s obziorm na sudionike 9

1.6.3. On-line zabava i rekreacija 10

1.6.4. Elektroničko bankarstvo 11

2. SIGURNOST 12

2.1. Rizici od nastanka šteta u elektroničkom trgovanju i mjere prevencije 12

2.2. Sigurnosni aspekti zaštite 13

2.3. Digitalni certifikat 14

2.4 Digitalni potpis 15

2.5. Infrastruktura javnog ključa 16

2.6. SSL protokoli 18

2.6.1. SSL protokol za rukovanje 20

2.6.2. SSL protokol za zapise 22

2.7. Kriptografija 22

2.8. Hash funckija 24

3. PRIVATNOST 27

3.1. Zaštita privatnosti podataka 27

3.2. Zakoni u Republici Hrvatskoj u vezi privatnosti podataka 28

3.3. Zakonski propisi privatnosti podataka u SAD-u 29

3.4. Zakonski propisi privatnosti elektroničke trgovine u EU-u 29

4. ZAKLJUČAK 31

5. POPIS SLIKA 32

6. LITERATURA 33

UVOD

Pred sam kraj dvadesetog stoljeća pojavljuje se novi oblik trgovine koji omogućava razmjenu dobara i usluga između kupaca i prodavatelja bez ikakvog fizičkog kontakta. Riječ je o elektroničkoj trgovini. Nastanak Interneta je ključan čimbenik za razvijanje elektroničke trgovine. Internet je razvijen prvi puta pred sam kraj šezdesetih godina dvadesetog stoljeća. Kako se postupno razvijao Internet, tako su stručnjaci postupno dolazili na ideju razvijanja elektroničke trgovine. S gledišta kupovine, Internet donosi mnogobrojne koristi kao što su efikasna ušteda vremena, ali i mnogobrojne opasnosti prilikom koje su ugrožene korisnički podaci.

Elektronička trgovina u Hrvatskoj još se ne koristi u punom pogonu kao kod nekih zapadnih zemalja. Problem vjerojatno leži u tome što državne institucije ne ulažu dovoljno u reklamiranje elektroničke trgovine kao i u educiranje ponajviše starijih osoba na način da im se dokaže, da elektroničko trgovanje nije opasno koliko se ono zapravo smatra.

Cilj završnog rada je istražiti rizike koje se mogu dogoditi prilikom izvođenja transakcija elektroničkog poslovanja i ukazati korisnicima na koji način se osigurati od opasnosti koji vrebaju na svakom koraku. Ciljem završnog rada se smatra educiranje korisnika kome i kako mogu sačuvati svoje privatne informacije koje su u „rukama“ elektroničkog trgovca.

Završni rad sastoji se od tri poglavlja koji obuhvaća tematiku sigurnosti i privatnosti elektroničke trgovine. Prvo poglavlje kreće sa definiranjem pojmova Interneta, Ekstraneta i Intraneta koji su glavni uzroci evolucije elektroničkog poslovanja. Prvo poglavlje govori i o osnovnom pojmu elektroničkog poslovanja i modelima, što predstavlja temelje za daljnju obradu završnog rada. U prvom poglavlju definirano je i elektroničko trgovanje, te aspekti. Nakon elektroničke trgovine dolazi drugo poglavlje koje se odnosi na njenu sigurnost. U nastavku završnog rada sigurnost i njezini aspekti zaštite su ukratko opisani. U sklopu sigurnosti razrađene su sigurnosne komunikacije koje uključuju digitalni certifikat i digitalni potpis. U ovom poglavlju govori se i o infrastrukturi javnog ključa ,SSL protokolima, o hash funkciji i kriptografiji. U zadnjem poglavlju preostala je privatnost elektroničke trgovine gdje su obrađene mjere zaštite privatnosti i zakoni u vezi privatnosti u Republici Hrvatskoj.

1. INTERNET I ELEKTRONIČKO POSLOVANJE

1.1. Internet

Internet je svjetska odnosno globalna računalna mreža koja povezuje mnoga računala i druge računalne mreže (akademske, poslovne, vladine) u jednu cjelinu s namjerom razmjene podataka i korištenja raznih sadržaja, usluga i servisa kao što su www, elektronička pošta i slični[1]. Klijent i poslužitelj trebali bi koristit isti komunikacijski protokol, to jest, ista pravila ponašanja u mreži.

Komunikacijski protokol koji se koristi naziva se TCP/IP što znači Transmission Control Protocol + Internet Protocol. TCP utvrđuje redne brojeve paketa u nizu, te vrijednost kontrolnih bitova. Također, njime se prikazuje na koji način se informacije segmentiraju u pakete podataka. IP je protokol pomoću kojeg se pridržavaju usmjerninici u Internetu. Usmjernik je građevna komponenta koja se koristi kod većih računalnih mreža, a uloga mu je povezivanje podmreža[2]. IP adresa izvorišta i odredišta se nalazi u svakom paketu podataka. IP adresa je jedinstveni broj u računalnoj mreži prema kojemu ga prepoznaju svi drugi elementi mreže. IP adresa može imati četiri broja koja su razdvojena točkama. Pošto, korisnici teško mogu upamtiti IP adresu, korisnici će koristiti simboličke adresa koje se lako pamte i sastoji se od niza znakova koji su također odvojeni točkama. Ti znakovi se nazivaju domene(primjer, www.fet.unipu.hr).

1.2. Ekstranet i Intranet

Ekstranet oblik je povezivanja računalnih mreža dvaju ili više zasebnih poslovnih sustava koji čine stanovitu poslovnu asocijaciju. Ekstranet služi za komunikaciju između tvrtke i njenih poslovnih partnera. Preduvjet kako bi se uspio uspostaviti ekstranet je da sve partnerske tvrtke imaju razvijen intranet. Prema tome, ekstranet se može definirati i kao skupina međusobno povezanih intranet partnerskih tvrtki.

Intranet je, konceptualno govoreći, bilo kakva unutarnja mreža računala neke tvrtke koja funkcionira na način sličan i kompatibilan Internetu.

Uloga intranet varira od slučaja do slučaja tako da on može biti zamjena za lokalnu mrežu i za rasprostranjenu mrežu, može i povezivati više lokalnih mreža i povezivati lokalne i rasprostranjene mreže. Intranet služi tvrtki za povezivanje sa određenim subjektima koji

[1] http://www.oblakznanja.com/2011/07/sto-je-internet/
[2] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 13

posluju na elektronički način, putem Web mjesta. Lokalna mreža odnosno LAN, je mreža koja povezuje mrežne uređaje na bliskim područjima. Rasprostranjena mreža odnosno WAN, je mreža koja globalno povezuje mrežne uređaje.

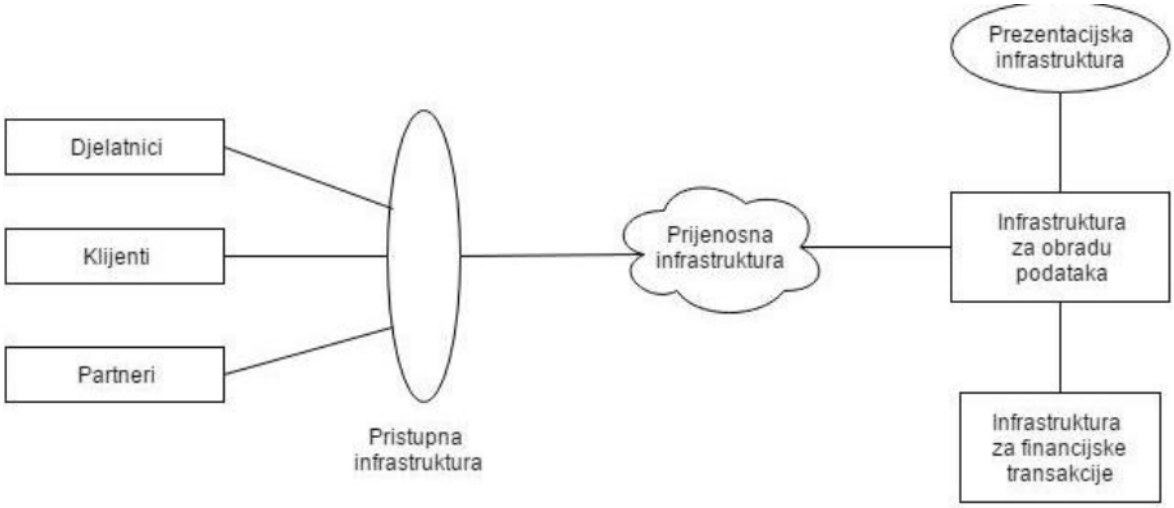
1.3. Pojam elektroničkog poslovanja

Pojam elektroničkog poslovanja javlja u bliskoj prošlosti, sredinom devedesetih godina 20.stoljeća. Pod pojmom elektroničkog poslovanja smatra se svaki onaj oblik organizacije poslovanja koji u izrazito velikoj mjeri ovisi o primjeni informatičke tehnologije i potpori informacijskih sustava[3]. Elektroničko poslovanje je suvremeni oblik organizacije poslovanja koji podrazumijeva intenzivnu primjenu informatičkih i, posebice, internetskih tehnologija u svim ključnim odnosno jezgrenim poslovnim funkcijama[4].

Poslovne transakcije su povećale brzinu i jednostavnost, a rezultat toga je sve jača konkurencija na tržištu. Stoga, tvrtke imaju zadatak, da se stalno prilagođavaju novim tehnologijama i da zadovoljavaju sve složenije potrebe potrošača. Tvrtke koje su prihvatile elektroničko poslovanje trebali bi shvatiti činjenicu, da kupci nemaju potrebu ulagati puno truda za pronalaskom novog ponuđača, ono što im treba je tek nekoliko klikova mišem.

Ukoliko, tvrtka prihvati ideju elektroničkog poslovanja, tvrtka time uspostavlja djelotvoran sustav elektroničkog poslovanja. To ovisi o veličini tvrtke i djelatnosti,o čemu svjedoči i broj elemenata komponenata. Te komponente su sljedeće: cjelovita infrastruktura za obradu podataka, prezentacijska infrastruktura, infrastruktura za provedbu sigurnih financijskih transakcija s vanjskim subjektima, infrastruktura za prijenos podataka na daljinu i pristupna infrastruktura[5].

[3] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 3
[4] Panian, Željko, Elektroničko poslovanje druge generacije, Ekonomski fakultet, Zagreb, 2013, str. 13
[5] Panian, Željko, Elektroničko poslovanje druge generacije, Ekonomski fakultet, Zagreb, 2013, str. 22



Slika 1: Sustav elektroničkog poslovanja
(Izvor:Panian,Ž.,2013.)

Slika 1 prikazuje shematski prikaz tipičnog sustava elektroničkog poslovanja

1.4. Okruženje webocentrične tvrtke

World Wide Web servis predstavlja oslonac elektroničkog poslovanja. Web mjesto čini temeljnu točku svakog poduzeća koje želi koristiti takav način poslovanja. Osnovni elementi okruženja webocentrične tvrtke su:globalna infrastruktura , struktura veza s dobavljačima, struktura veza s dobavljačima, struktura veza s klijentima odnosno kupcima, struktura veza s poslovnim partnerima i posrednicima u poslovanju.[6] Globalna infrastruktura tvrtke obuhvaća sigurnosnu infrastrukturu, sastavljenu od sustava koji osiguravaju integritet podataka koji su u stanju mirovanja i u prijenosu.

Globalna infrastruktura obuhvaća elektroničko bankarstvo. Elektroničko bankarstvo odnosi se na korištenje elektroničkog poslovanja prilikom obavljanja bankarskih poslova. Globalna infrastruktura uključuje i komunikacijsku infrastrukturu, globalno/nacionalnu strukturu i zakonski okvir. Struktura veza s dobavljačem omogućava razvijanje odnosa poduzeća s dobavljačima elektroničkim putem. Održavanja dobrih odnosa sa klijentima preduvjet je za realiziranje koncepta elektroničkog poslovanja. Osnovni zadaci što ih izvorni proizvođač ili pružatelj usluga pritom mora izvršavati su: promptno odgovaranje na zahtjeve tržišta, nadopunjavanje zaliha, distribucija informacija o proizvodima, realizacija narudžbi, upravljanje izlaznim računima i naplatom i upravljanje rezervnim dijelovima i ugovaranje.[7]

[6] *ibidem, str.* 16
[7] *ibidem, str..*20

1.5. Sustav elektroničkog poslovanja

Ukoliko tvrtka želi prihvatiti ideju elektroničkog poslovanja, tvrtka treba provesti mnogobrojne akcije kako bi se ostvario koncept praktične realizacije. Neovisno o tome koliko je tvrtka velika, takav zahvat je opsežan pošto sustav treba biti kompleksan, odnosno treba obuhvaćati veliki broj komponenata. Te infrastrukturne komponente su sljedeće : cjelovita infrastruktura za obradu podataka, prezentacijska infrastruktura, infrastruktura za provedbu sigurnih financijskih transakcija s vanjskim subjektima, infrastruktura za prijenos podataka na daljinu i pristupna infrastruktura.

Infrastruktura za obradu podataka uključuje potpuni interni informacijski sustav poduzeća s njegovim komponentama, odnosno Hardwareom, Softwareom, Lifewareom, Datawareom i Orgwareom. Kod infrastrukture za prijenos podatak glavnu ulogu ima Internet. Osim Interneta kao infrastruktura za prijenos podataka mogu poslužiti i privatne računalne mreže i virtualne privatne mreže[8].

1.6. Modeli elektroničkog poslovanja prema kriteriju obavljenih poslova

1.6.1. Prodaja vlastitih dobara i usluga

Ideja modela je iskoristiti važna svojstva Interneta i da svi njegovi korisnici mogu po volji, bilo gdje i bilo kada s bilo kojeg mjesta, stupiti u kontakt s korisnikom, a da obadvojica u tome vide potrebu ili korist. Tvrtke ili točnije ljudi u njima, koji imaju nešto ponuditi na prodaju, saznali su da je važno plasirati informaciju u vezi toga putem Interneta. Ukoliko se informacija plasira na takav način, ona će biti dostupna izuzetno velikom broju mogućih kupaca.

Kronološki poredano, najstariji oblik prodaje na daljinu je prodaja nematerijalnih dobara[9]. Nakon toga su bili i pokušaji prodaje klasične robe, to jest, prodaja materijalnih dobara i zadnji razvoji korak je prodaja usluga. I na kraju, iz istoga izvora dolazi se do zaključka, da predmeti prodaje putem Interneta mogu biti[10]:

- Nematerijalna dobra
- Materijalna dobra

---

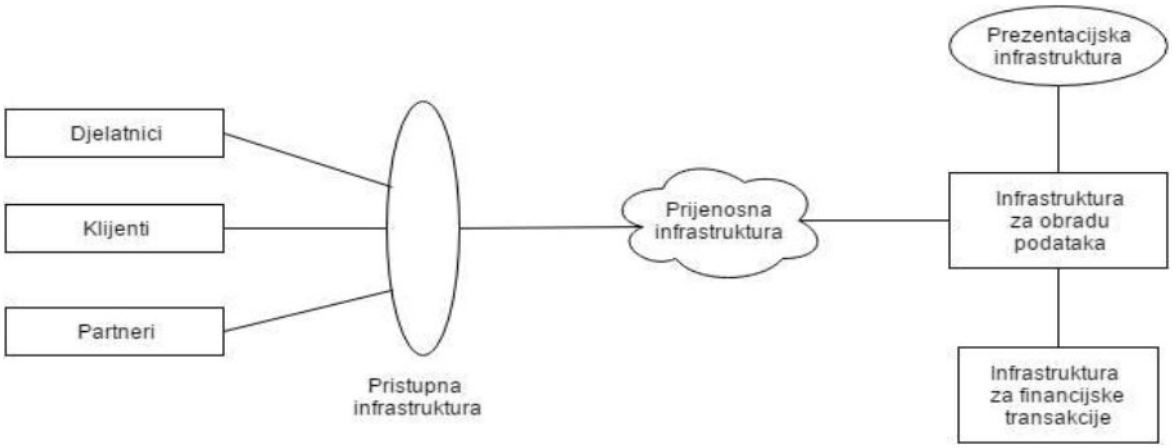
[8] *ibidem, str.*31
[9] *ibidem, str.54*

- Usluge

Slika 2: Elektronička prodaja materijalnih dobara

Izvor: Panian,Ž., 2013.

Slika 2 prikazuje razmjenu tržišnih informacija kod elektroničke prodaje materijalnih dobara.



Slika 3: Elektronička prodaja nematerijalnih dobara

Izvor: Panian,Ž.,2013.

Slika 3 prikazuje proces razmjene i prodaje robe.

Prodaja usluga potpomognuta je digitalnom razmjenom informacija, dok se kod usluga u nekim situacijama može, a u drugima ne može pružiti elektroničkim putem. Svi navedeni oblici Internet prodaje imaju neke sličnosti, a to su: prodaja se obavlja putem vlastitog Web mjesta, svaka prodaja je popraćena odgovarajućim marketinškim aktivnostima, svi oblici razvijaju on-line marketing, svaki oblik prodaje iziskuje korištenje odgovarajućeg načina plaćanja i na kraju, razdvajanje informacija o predmetu prodaje.

1.6.2. Elektroničko trgovanje

. Pojam elektroničkog poslovanja i elektroničkog trgovanja često se smatra istim, a razlog tomu je da se svako poslovanje, u konačnici svodi na kupoprodaju nečeg,točnije trgovanje nečim. Vjerojatno najsnažnije argumente oko raščišćavanja nedoumica glede ovih dvaju

pojmova je dao Adrew Bertels. On, tvrdi sljedeće: Elektroničko trgovanje uključuje razmjenu dobara i usluga između kupca, poslovnih partnera i prodavatelja. Dobavljač je u interakciji s proizvođačem, kupci s prodavačima, a otpremnici s distributerima. Elektroničko poslovanje čine svi ti elementi, ali također i operacije što se obavljaju „iza scene“, unutar same tvrtke. Takve su operacije, primjerice, upravljanje proizvodnjom, razvojem, cjelovitom korporacijskom infrastrukturom i proizvodima[11].

Elektroničko trgovanje, naizgled ima dosta sličnih aktivnosti koje se obavljaju kao i kod on-line prodaje vlastitih dobra i usluga. Web stranica prodavača vlastitih dobara i usluga, po funkcionalnostima i dizajnu su slične, međutim funkcija trgovca, pa samim time i Web mjesta daleko se razlikuju. Prodavač vlastitih dobara i usluga dosta se koncentrira na proizvodnju ili pružanje usluga, dok je Web mjesto samo put kojim će stići do kupca. Elektronički trgovac većinom ništa ne proizvodi sam, već on ponudi potrošačima ono što je proizvedeno ili uslugu koju nudi netko drugi. Oni nude robu i usluge na prodaju iz većeg broja izvora, pa čak i konkurentskih, a time će njihov odnos prema dobavljačima biti drugačiji, nego odnosi prodavača dobara ili usluga. Trgovati se može sa „svime i svačim“ što je netko prethodno posjedovao ili proizveo. Web mjesto treba podržavati raznolike oblike komunikacije, a funkcionalnost mu treba biti takva da u što kraćem periodu reagira na promjene na tržištu prodaje i na tržištu nabave. On-line trgovac je posrednik između proizvođača i kupca i time on ima svoje mjesto u sredini lanca vrijednosti, kojeg i on samostalno formira. Elektronički trgovac samostalno stvara elektroničko tržište i u velikoj mjeri ga i održava, što nije slučaj kod prodavača vlastiti proizvoda i usluga.

Prema predmetima trgovanja, postoje dva osnovna oblika elektroničkog trgovanja[12]: model trgovanja materijalnim i nematerijalnim dobrima ili uslugama i model trgovanja kapitalom.

Trgovački poslovi su u prošlosti imali poslovno raširene aktivnosti[13]. Praktički, trgovalo se sa svime i svačime, prema propisima i protuzakonito. Trgovanje bi trebalo biti djelatnost od koje bi svaki sudionik imao koristi. Povijest svjedoči o sljedećoj zakonitosti:

Što su sredstva korištena pri trgovanju sofisticiranija, veće su šanse za ostvarivanje tržišta koje će se po zakonitostima što na njemu vladaju više približavati perfektnome ili idealnome.

[11] *ibidem*, *str.*13
[12] *ibidem*, *str.*57
[13] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 60

Istodobno, međutim, povećavaju se i rizici od trgovačkih malverzacija različitih tipova i vrsta pa je potreban pojačan društveni nadzor i trgovačka pravna regulativa[14].

U sadašnjosti, kada se u trgovanje uvelo sve više elemenata informacijske tehnologije, dolazi se do zaključka, da elektroničko trgovanje je uvjet bez kojeg se ne može dobro poslovati. Prednosti koje nudi elektroničko trgovanje su brz pristup informacijama, što omogućava bolju i bržu dostupnost proizvoda i usluga na tržištu. Iz istog izvora elektronička trgovina ima prednosti kao što su, transferi dokumenata uz minimalne troškove. Također, omogućuje kreiranja vlastitih baza podataka i obrada njihovih informacija je isto jedna od prednosti, a time se potiče na kreativnost i neovisnost prilikom poslovanja. Elektronička trgovina pruža mogućnost analize proizvoda i usluge, te razmjenjivanje stečenih iskustava među sudionicima. Potom, mogućnost brzog i odgovornog regrutiranja potrebnih djelatnika. Elektronička trgovina također analizira tržište kako bi uočila na neželjene pojave na njemu. I na kraju omogućava stvaranje novih poslovnih prilika.

Nažalost, uz sve silne prednosti koje nudi elektroničko trgovanje, postoji i određeni broj nedostataka, a razlog tome je zlouporaba informacijske tehnologije. Na temelju istog izvora najvažniji rizici odnosne se na: osiguranje podataka od uništenja, zaštitu tajnosti informacijskih sadržaja, zaštitu privatnosti korisnika, ovlaštenost pojedinaca, grupe ili institucija da obavlja određene tipove poslova, potom kontrolu podmirivanja obveza iz trgovačkog poslovanja prema državi i na kraju zaštitu nacionalnih interesa.

1.6.2.1. Aspekt socijalnog i institucionalnog elektroničkog trgovanja

Elektroničko poslovanje potrebno je razmatrati s najmanje tri aspekta[15]: s aspekta socijalnog i institucionalnog okruženja u kojemu se elektroničko trgovanje realizira, s aspekta prodavatelja i mogućnosti ostvarivanja njegovih resursa, s aspekta kupca i mogućnosti ostvarivanja njegovih interesa.

Aspekt socijalnog i institucionalnog okruženja elektroničkog trgovanja uključuje zakonske odredbe koje se primjenjuju na elektroničko trgovanje u Republici Hrvatskoj.

Temeljne odrednice koje trebaju biti uređene svakim ugovorom o kupoprodaji su stvar ili pravo , cijena i rizik. Predmeti kupoprodaje, to jest trgovanja, su stvari i prava koji trebaju biti u prometu. U prometu se isto tako može pojaviti i buduća stvar ili pravo, to jest, ono što u

[14] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 60
[15] *ibidem, str.* 61

trenutku pravljena ugovora ne postoji. Cijena je jedna od odrednica ugovora i ukoliko cijena nije određena taj se ugovor smatra poništenim. Cijena je izražena u novčanoj valuti koja treba biti navedena. Rizik je značajna činjenica kupoprodajnog ugovora o kojoj treba brinuti tijekom sklapanja ugovora. Rizik se može definirati kao vjerojatnost da će stvarni povrat od investicije biti niži od predviđenog povrata[16].

U Republici Hrvatskoj svaki kupoprodajni ugovor treba biti u pisanom obliku i da bi bio pravovaljan, treba sadržavati potpise od prodavatelja i kupca. Potpis se ovjerava kod javnog bilježnika. Također, prodavatelj bi trebao prema kupoprodajnom ugovoru predati stvari kupcu u određeno vrijeme i na određenom mjestu. Postoji i primjer specifičnog slučaja kada se roba prodaje prema uzorku ili modelu. Ukoliko, isporučena roba ne odgovara predviđenom uzroku, kupac ima pravo dokazati da je oštećen. Također, u Republici Hrvatskoj kupac ima pravo u slučaju da se određena stvar pokvari, zatražiti prema jamstvenom listu popravak te stvar ili povrat novca.

Prema aktivnostima prodavatelja u elektroničkom trgovanju, prodavatelj je jedna od vitalno zainteresiranih strana u svakome obliku trgovanja pa tako i onome elektroničkom. Poslovi koji proizlaze iz elektroničkog načina trgovanja su[17]: uspostavljanje elektroničkog prodajnog mjesta, elektronički marketing, kreiranje elektroničke poslovne dokumentacije, odabir i angažman prodajnog osoblja, elektronička prodajna operativa i statistika i analiza prodajnih aktivnosti te utvrđivanje poslovnih rezultata. Modeli elektroničkih prodajnih mjesta su[18]: tradicionalna on-prodavaonica, aukcijska kuća, virtualna prodavaonica, mješovita realno/virtualna prodavaonica, elektronički distribucijski centar, prodajno skladište, klupska trgovina, intranetska trgovina i mnogi drugi. Elektronički marketing ostvaruje marketinške aktivnosti određene tvrtke pomoću informacijske i komunikacijske tehnologije. Kreiranje elektroničke poslovne dokumentacije ovisi o kvaliteti poslovanja i učincima. Elektroničko poslovanje, točnije trgovanje kreira i koristi novi tip dokumenta koji se naziva elektroničke poslovne dokumentacije. Ukoliko se uspostavi elektroničko trgovanju potrebno je primijeniti odgovarajuću pripremu i osposobljavanje postojećeg osoblja. Jedan od glavnih zadataka prodavatelja je privlačenje kupaca,a to uspijeva pomoću akcijskih ponuda, besplatnih dodatnih usluga, besplatne aukcije, nagradnim igrama i brzo reagiranje na oscilacije potražnje izazvane modnim trendovima.

[16] http://www.moj-bankar.hr/kazalo/R/Rizik
[17] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 71
[18] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 71

Aktivnosti kupca u elektroničkome trgovanju su:

Kupac koji želi kupovati preko Interneta treba imati računalo, priključak na Internet, program pretražnik ugrađen u računalo, kreditnu karticu i volju i znanje. Kupac također bi trebao znati koji tipovi elektroničkih prodavatelja postoje, to jest, kojeg je prodavatelja odabrao. A to su[19]: proizvođači nuđene robe, stvarni trgovci, specijalizirane virtualne prodavaonice, virtualni prodajni centri i on-line aukcije. Elektronički prodavatelj nudi kupcu na svojoj web stranici opciju kataloga ili usluga i mogućnost traženja. Ukoliko je kupac odlučio što će kupiti, potom slijedi faza plaćanja, koja uglavnom obavlja putem kreditne kartice(postoji još virman i pouzećem). Virtualna potrošačka kartica omogućava kupnju više artikala odjednom i time se isključuje kupnja jednog po jednog proizvoda. Virtualno tržište nude sve i svašta, pri tome kupac treba paziti na sve opasnosti koje nude primamljivi trgovci. Elektroničko tržište je opasnije od klasičnih tržišta. Također, svaka kupovina preko Interneta iziskuje od kupca plaćanje dodatnih usluga, na primjer, poštarinu. Kupac ukoliko je nezadovoljan robom ima ju pravo vratiti, zamijeniti ili tražiti povrat novca. Normalno je, da kupac želi doći do preferirane robe, odnosno do kvalitetne ponude i ponuđača. Načelo prevencije od obmane i prijevara tvrdi da nikada ne bi trebalo kupovati na Web mjestu koje ne otkriva svoju stvarnu adresu, također nije dobro odgovarati na anonimne poruke i pozive, ne treba pristajati na naizgled fantastične dobre financijske aranžmane, ne treba nasjedati na nerealno povoljnije ili problematične ponude[20]. Prijevaru nekad nije moguće izbjeći, najgore što kupac može učiniti je da nakon prijevare ne reagira. Ukoliko se dogodi prijevara kupac bi trebao u što kraćem roku kontaktirati prodavača.

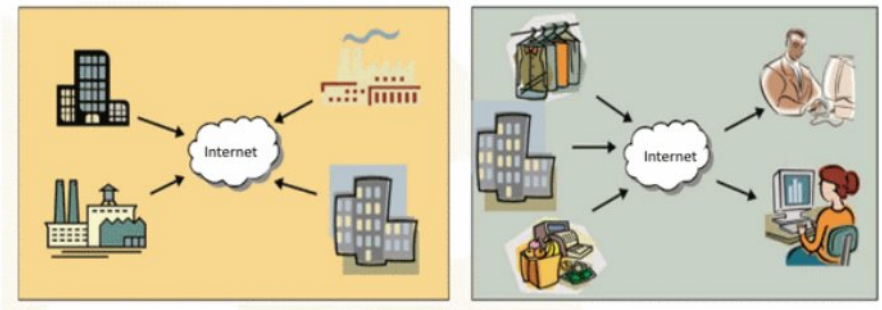
1.6.2.2. Modeli elektroničke trgovine obzirom na sudionike

Najvažniji modeli elektroničkog poslovanja prema kriteriju sudionika su[21]:

- poslovi između privatne tvrtke kao ponuditelja i fizičke osobe kao klijenta (engl. Business to Customer, B2C)
- poslovi među privatnim tvrtkama (eng. Business to Business, B2B)

[19] *ibidem*, *str.*.113
[20] *ibidem*, *str.*.129
[21] Panian, Željko, Elektroničko poslovanje druge generacije, Ekonomski fakultet, Zagreb, 2013, str.76

- poslovi u kojima je jedan od aktera država: - poslovi u kojima je privatna tvrtka ponuditelj,a država klijent (eng. Business to Goverment, B2G) i poslovi u kojima je država ponuditelj, a privatna tvrtka klijent (eng. Goverment to Bussines, G2B)
- poslovi među fizičkim osobama (eng. Customer to Customer , C2C)



Slika 4: B2B i B2C

Izvor: http://e-ucenje.unipu.hr/mod/resource/view.php?id=673

Slika 4 prikazuje razlike između B2B modela i B2C modela. Poslovi među privatnim tvrtkama odnosno B2B je model elektroničkog poslovanja između dvije ili više tvrtke. Podrazumijeva da organizacije prodaju vlastite proizvode i usluge drugim organizacijama za njihove potrebe, to jest, na način da druge organizacije kreiraju vlastite proizvode i usluge za dalju prodaju, dok B2C podrazumijeva da organizacije prodaju proizvode i usluge za krajnju potrošnju[22].

1.6.3. On-line zabava i rekreacija

Industrija zabave i rekreacije tijekom druge polovice 20. stoljeća doživjela je brz rast i ogromnu profitabilnost, a taj trend se nastavlja i u 21. stoljeću. Internet i World Wide Web od početka su se našli kao vodeći u industriji zabave, koji su se potom transformirali u industriju on-line zabave i rekreacije. U početku, korisnički preglednici omogućavali su samo sporu konverzaciju tekstom i razmjenu podataka i slika. Industrija zabave je na taj način prepoznala Internet kao budućeg distribucijskog kanala za igre, filmove, glazbu i druge oblike zabavnog sadržaja.

Prema istraživanju tvrtke Nielsen NetRating, koje je objavljeno početkom 2011. godine u suradnji s kompanijom U.K Online Measurements, među pedeset najposjećenijih Web mjesta

[22] http://savjetnik.ba/wp-content/uploads/2011/06/b2b%20poslovni%20koncept.pdf

u Velikoj Britaniji, čak njih šesnaest se našlo koji potječu iz kategorije medija koji nude zabavno-rekreacijske sadržaje. Prema istom tom istraživanju 2004. godine bilo je devet[23].

Web predstavlja i bogat izvor mogućnosti igranja besplatnih igara , od onih osnovnih pa sve do igara na sreću, pa do pravih igara i kockanja. Tako primjerice, mjesečna zarada od on-line kockanja samo u mjesecu listopadu 2011. godine u saveznoj Američkoj državi Nevada nadmašila 866 milijuna USD[24].

1.6.4. Elektroničko bankarstvo

Primjenjivanjem komunikacijskih i informacijskih tehnologija u bankarstvu naziva se elektroničko (on-line) bankarstvo. Primjena komunikacijskih i informacijskih tehnologija omogućila je da banka vlastite bankarske poslove obavlja bez nazočnosti komitenta u prostorima banke između djelatnika i komitenata. Ukoliko se kao medij koristi Internet, banka aktivira vlastito Web mjesto(,to jest, neko računalo ili čvor privatne mreže) i otvara Web stranicu. Svi oblici bankarskih poslova koji koriste Internet kao medij, koristi se naziv Internet bankarstvo.

Što se tiče daljinskog bankarstva, važno je razlikovati dvije osnovne vrste poslova[25]:

- Međubankarski poslovi
- Poslovi s komitentima i u ime komitenta

Međubankarski poslovi čine poželjnu vrstu poslova, budući da se u takvim poslovima radi o velikim transferima novčanih sredstava. Zbog toga, međubankarski poslovi zahtijevaju visok stupanj sigurnosti i zaštite podataka. Međubankarski poslovi se neće obavljati putem Interneta ukoliko se ne realiziraju sigurnosni zahtjevi. Primjena bankomata vezana je za poslove s komitentima i u njihovo ime. Bankomati su uređaji za izdavanje gotovog novca vlasnicima bankovnih računa bez fizičkog posredovanja ljudi-bankovnih djelatnika[26]. Bankomat ima dva osnovna dijela: dio za fizičku manipulaciju novca i dijela za manipulaciju podacima o novčanim sredstvima na računu komitenta iz istog izvora.

[23]Panian, Željko, Elektroničko poslovanje druge generacije, Ekonomski fakultet, Zagreb, 2013, str.58
[24] Panian, Željko, Elektroničko poslovanje druge generacije, Ekonomski fakultet, Zagreb, 2013, str.59
[25] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 155
[26] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 158

2. SIGURNOST

Sigurnost je proces održavanja niske razine rizika. Niti jedna organizacija se ne smije smatrati sigurnom niti u jednom trenutku nakon što se uskladi s vlastitim sigurnosnim pravilima. Sigurnost nije konačni proizvod nego proces. Kada se na to misli, onda se misli na činjenicu da sigurnost se ne može kupiti, kao na primjer proizvod ili uslugu, već se proizvod ili usluge koriste u procesu. Smatra se da postoje i drugi bitni elementi kao što su podizanje svijesti,edukacija i stalno praćenje stanja[27].

Logično je da svaka elektronička trgovina želi imati veću sigurnost, ali ukoliko to želi trebati će ulagati u sigurnost, čime se umanjuje izloženost sistema i računalne mreže riziku. Gledano s druge strane sigurnost traži veliko ulaganje, a kao rezultat toga utječe na smanjenje profitabilnosti. Zato je izrazito važno da organizacija postigne ravnotežu između ulaganja u sigurnost i postignutih efekata.

Sigurnost kao proces može se podijeliti na četiri osnovna koraka[28]: procjena, zaštita, otkrivanje i odgovor. Procjena se smatra pripremom za ostale tri komponente. Procjena je vezana s pravilima, procedurama, pravnom i drugom regulativom, budžetom i drugim upravljačkim dužnostima. Zaštita podrazumijeva primjenu protumjera kako bi se smanjila mogućnost ugrožavanja sistema. Otkrivanje ili detekcija je proces kojim se identificira „upad“, to jest, povreda sigurnosnih pravila. Odgovor ili reakcija je proces opravka od posljedica upada. Iz istog izvora u novije vrijeme sve se češće koriste sudski procesi protiv onoga tko ugrožava sigurnost.

.U načelu, do zloporabe informacijske tehnologije dolazi iz dva razloga:[29] radi ostvarivanja neopravdanih ili protupravnih koristi od strane pojedinaca ili organiziranih skupina i radi namjernoga i svjesnoga nanošenja materijalne ili nematerijalne štete pojedincu, skupini ili zajednici.

2.1. Rizici od nastanka šteta u elektroničkom trgovanju i mjere prevencije

U općem smislu, rizik je opasnost da poduzeta aktivnost dovede do neželjenih posljedica. Primjenjujući tu opću definiciju pojma rizika u oblasti informacijske tehnologije, dolazi se do zaključka kako su rizici informacijske tehnologije opasnosti da njezina primjena dovede do

[27] Pleskonjić,D. i ostali, 2007, str. 9
[28] Pleskonjić,D. i ostali, 2007, str. 12
[29] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 185

neželjenih posljedica (šteta) u organizacijskom sustavu i/ili njegovoj okolici.[30] U svemu postoji rizici. Rizik treba prihvatiti i upravljati njime i nikako se ne smije ignorirati. Težina i učestalost su dva glavna obilježja karakterizacije rizika. Iz istog izvora težina rizika prikazuje koliko rizik može napraviti štete, a najčešće je prikazano u novčanom obliku. Ovisno o uzroku rizici mogu biti: objektivni, kada proizlaze iz prirode i zakonitosti funkcioniranja sustava u kojemu se informacijska tehnologija primjenjuje i subjektivni, kada nastaju namjerom pojedinaca ili skupina, ili onda kada se u sustavu ne poduzimaju raspoložive mjere zaštite (prevencije) od objektivnih rizika. Ukupnost mjera prevencija rizika kod primjene informacijske tehnologije, a to znači i u elektroničkome poslovanju, može svrstati u dvije temeljne kategorije:[31] mjere osiguranja integriteta podataka u prijenosu i mjere zaštite od zloporabe informacijske tehnologije.

2. 2. Sigurnosni aspekti zaštite

Sigurnosni aspekti zaštite se često mogu definirati u odnosu na njihov položaj u informacijskom ili računalnom sustavu ili računalnoj mreži.

Nivoi sigurnosnih aspekata zaštite su[32]:

Zaštita na razini aplikacije može obuhvatiti, na primjer, neke od ovih elemenata: softversku zaštitu aplikacije, izoliranje važnih aplikacija koje se nalaze na namjenskim serverima i povezanim računalima i primjena posebnih protokola. **Zaštita na nivou operativnog sustav-** obuhvaća složeno i obilno područje koji se odnosi na neki način na sve slojeve operativnog sustava. Također obuhvaća i vezu operativnog sistema i aplikacije, kao i odnose sa mrežnom arhitekturom. **Zaštita na nivou mrežne infrastrukture** uglavnom obuhvaća sljedeće elemente[33]: primjenu mrežne zaštite (engl. *firewall*), blokiranje nepotrebnih portova, šifriranje putanje, izoliranje putanje uz pomoću usmjernika ili pomoću specifične arhitekture. **Proceduralna i operacijska zaštita.** Na temelju istog izvora ovaj nivo sigurnosne zaštite obuhvaća elemente kao što su: definiranje i provođenje pravila zaštite, politike i procedure, detekciju napada, provođenje mjera u cilju zaštite i umanjivanja ranjivosti sustava, upravljanje konfiguracijskim sistemom, podizanje svijesti o sigurnosnim problemima i obrazovanje zaposlenih i korisnika.

[30] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 186
[31] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 188
[32] Pleskonjić,D. i ostali, 2007, str. 20
[33] Pleskonjić,D. i ostali, 2007, str. 21

Posebne i odvojene aspekte zaštite čine zaštite od elementarnih nepogoda (požari, poplave, zemljotres) i zaštita od terorizma ili drugih uništavajućih akcija. Vrlo je važno poštivanje etničkih, društvenih, pravnih i psiholoških aspekata.

2.3. Digitalni certifikat

Ukoliko Osoba1 i Osoba2 žele komunicirati preko elektronske pošte koristeći javni ključ. U tom slučaju, Osoba1 posjeduje javni ključ od Osobe2 . Najveći problem koji se događa na ovom primjeru je integritet njihovih javnih ključeva, to jest, treba potvrditi da je javni ključ od Osobe2 zaista u vlasništvu te osobe, a ne ključ napadača. Ovaj problem se rješava pomoću digitalnog certifikata i infrastrukture javnog ključa.

Digitalni certifikat se sastoji od[34]:javnog ključa, informacije o identiteta, informacije koje se tiču ovlaštenja korisnika, npr. dozvole za pristup resursima i jednog ili više digitalnih potpisa.

Digitalnim potpis ne ovjerava cijeli certifikat, već samo vezu između identiteta korisnika i javnog ključa. Prema tome, certifikat je javni ključ s identitetom korisnika i potpisom koji je izdan od strane kojoj se vjeruje, time se otvara veza između identiteta i ključa. Digitalni certifikat ima naziv i identifikacijski certifikat iz razloga što se koristi za identifikaciju pojedinca, kompanije ili servera.

Digitalni certifikat pruža potporu za[35]:

Provjeru identiteta - pojedinačnim korisnicima i organizaciji je omogućeno da provjere identitet pojedinaca u komunikaciji odnosno transakciji, a sve to zahvaljujući digitalnom certifikatu koji izdaje PKI. Provjera identiteta je identifikacija entiteta, a certifikatu su jedan on načina podrške toj provjeri. Jedan od boljih dokaza o provjeri identiteta je digitalni potpis elektronske pošte u kombinaciji s certifikatom koji identificira pošiljatelja.

Provjera integriteta- digitalni certifikat osigurava poruke, na način da onemogućava da korisnik primi izmijenjenu ili oštećenu poruku.

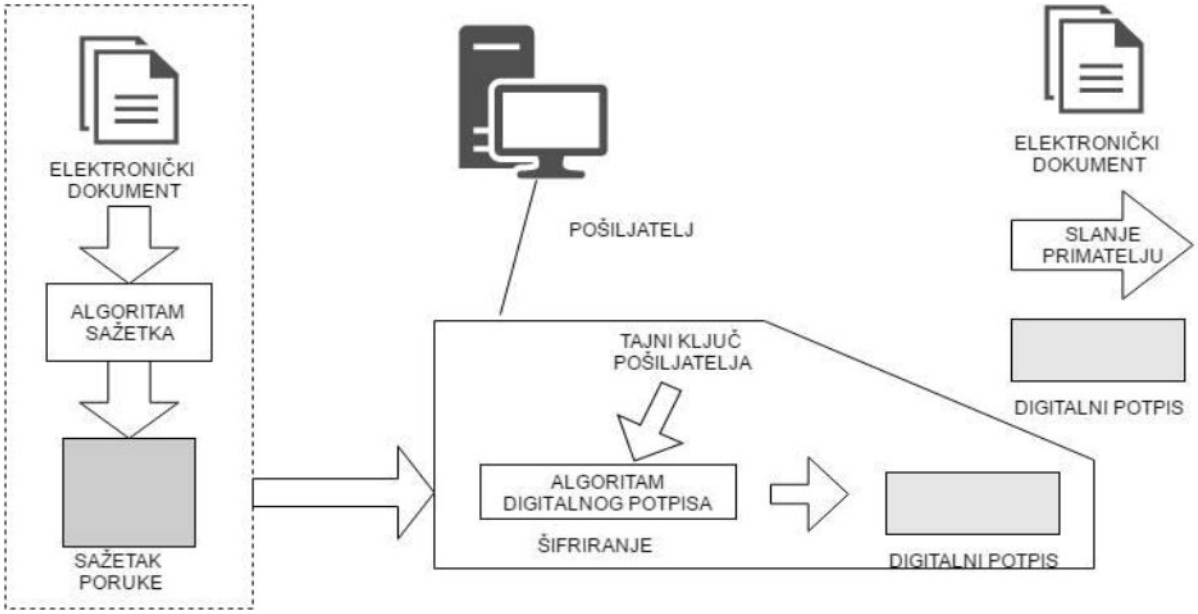
Autorizacija pristupa- digitalni certifikat ima ulogu da često dolazi do zamjene zaboravljenih korisničkih imena ili lozinaka na Internetu.

[34] *ibidem, str..*124
[35] *ibidem, str..*125

Neporicanje -funkcionalna uloga digitalnog certifikata je nemogućnost odbacivanja digitalno „označene“ transakcije koja je ranije potvrđena korisničkim identitetom, na primjer kupovinom preko Web lokacije.

2.4. Digitalni potpis

Digitalni potpis je elektronički ekvivalent vlastoručnog potpisa koji osigurava autentičnost podatkovnog sadržaja. Digitalni potpis pruža[36], autentičnost koja predstavlja sigurnost kojim potvrđuje da je dokument poslan od određene osobe,to jest, da dokument nije potpisan od strane neautorizirane osobe. Neporecivost, koja je korisna tijekom pravnih i drugih sporova, a time se potvrđuje tko je autor određenog dokumenta. I izvornost digitalno potpisanog dokumenta koja predstavlja dokument koji je ostao netaknut,odnosno nepromijenjen od svog nastanka

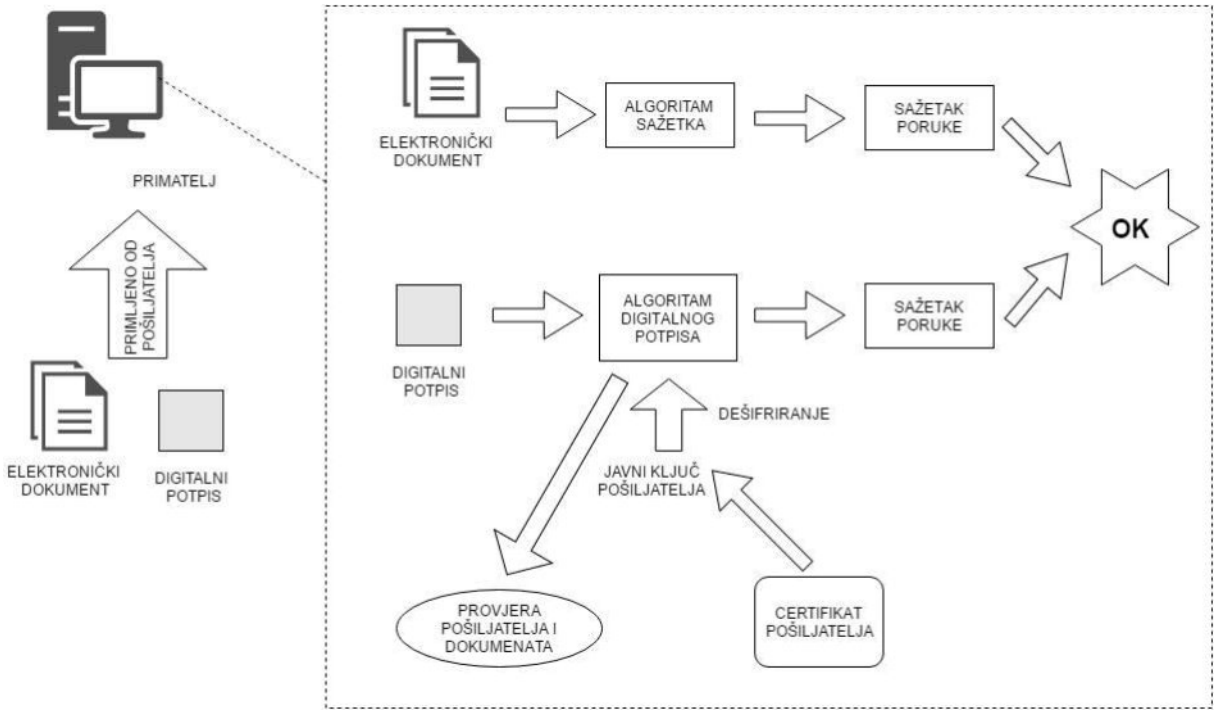


Slika 5: Potpisivanje digitalnog potpisa

Izvor: Bača,M.,2013.

Slika 5 :Primatelj prvo dobije elektronički dokument, dobivenim digitalnim potpisom se dešifira ključem te se time može odreidti izvorni tekst. Dokument će postati digitalno autentičan ukoliko se ta dva teksta poklapaju. Izvođenje digitalnog potpisa može se podjeliti na dva oblika:digitalni potpis s tajnim ključem i digitalni potpis s javnim ključem.

[36] Miroslav Bača „Uvod u računalnu sigurnost“, Narodne novine,Zagreb,2004, str 189



Slika 6:Provjera digitalnog potpisa

Izvor: Bača,M.,2013.

Slika 6-Na temelju poruke prva korak je generiranje sažetka, koji se nakon toga šifira privatnik ključem. Primatelj poruke provjerava digitalni potpis na način da izračuna sadržaj poruke. Zatim se dešifrira sadržaj javnim ključem,i na kraju ako se ova dva elementa podudaraju kao rezultat dobijemo da je uistinu potpisnik ujedno i vlasnik privatnog ključa koji odgovara javnom ključu. Primatelj provjerava poruku koju je potpisnik potpisao i jeli poruka ostala ista tijekom svog putovanja na glavno odredište. DSS i RSA su najpopularniji standardi koji se koriste za digitalni potpis. RSA digitalni potpis se temelji na RSA asimetričnom algoritmu za šifriranje[37]. DSS je standard koji propisuje način dobivanja i provjere korištenja digitalnog potpisa[38].

2.5. Infrastruktura javnog ključa

Infrastruktura javnog ključa (engl.public key infrastructure,PKI) je strukturirani sistem koji skladišti i osigurava dodatne funkcije koje izdaju i poništavaju certifikate, kao i funkcije za uspostavljanje relacija povjerenja. Glavna uloga koju ima PKI je da omogući sigurnu komunikaciju preko nesigurnih kanala.

[37] Miroslav Bača „Uvod u računalnu sigurnost“, Narodne novine,Zagreb,2004, str 190
[38] *ibidem*, *str.*.190

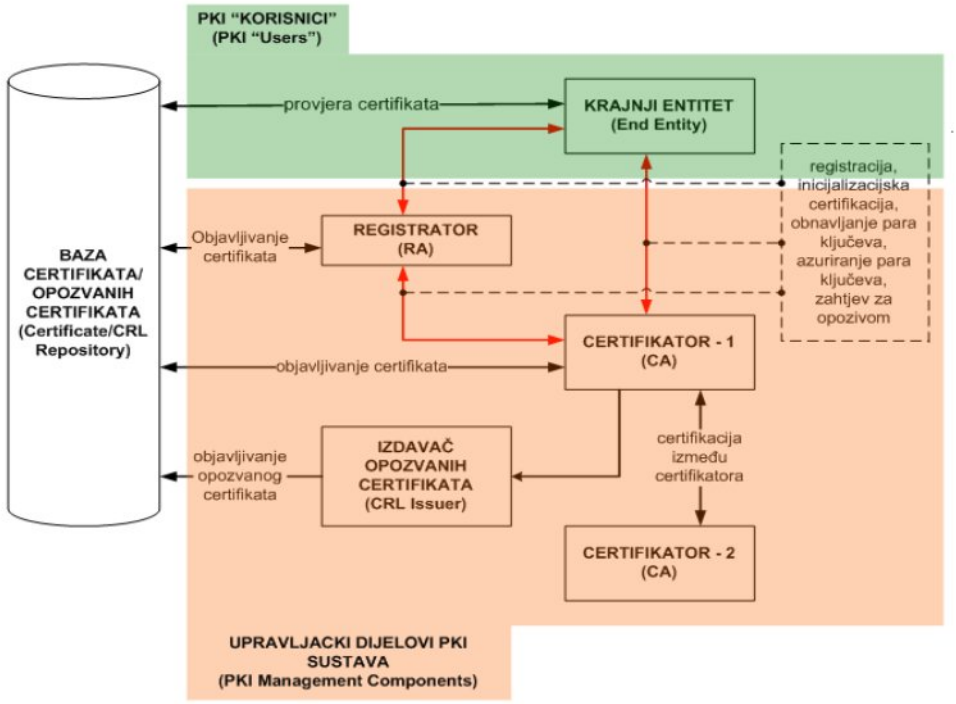
Postoje tri glavne komponente infrastrukture javnih ključeva,a to su[39]:

Certifikacijski centar (engl.certificate authority, CA)- je glavna komponenta PKI-a, koja ima ulogu u izdavanju i poništavanju certifikata i potpisuje izdate certifikate svojim privatnim ključem. Certifikacijski centar je odgovoran za generiranje certifikata i njihov integritet. Korištenjem javnog ključa CA, svatko ima pravo provjeriti potpis CA na certifikatu, potom i integritet certifikata. CA ima jednu vrlo posebnu metodu zaštite javnih ključeva ukoliko dođe do situacije u kojoj se ugrožava integritet PKI-a, odnosno samouništenja svih javnih ključeva. Osnovni zadatak CA je da ulije povjerenje u učesnike u komunikaciji prilikom pružanja usluge izdavanja digitalnih certifikata.

Registracijski centar (engl. Registration authority, RA) je komponenta infrastrukture javnog ključa koja osigurava proces prihvata,proces registracije i obrađuje zahtjeve za izdavanje certifikata. Potom ih prosljeđuje certifikacijskom centru radi izdavanja certifikata zato što RA ne smije imati ulogu izdavanja certifikata. Za RA/CA se može dati primjer kao pravljenje putovnice, grupa ljudi(RA) radi provjeru identiteta čovjeka koji želi provjeriti putovnicu, nakon toga se provjerava smije li mu se izdati putovnica, a CA izdaje putovnicu i prosljeđuje do određenog korisnika. Ključni korak u izdavanju certifikata je identifikacija korisnika tokom registracije, koja je ujedno i prvi i najvažniji korak u neporecivosti.

Skladište certifikata je skup u kojem nastaju javni ključevi i certifikat korisnika i liste poništenih certifikata.

[39] *ibidem, str.* 125



Slika 7: Sustav infrastrukture javnog ključa

Izvor: http://os2.zemris.fer.hr/pki/2005_rebac/#infrastruktura_javnog_kljuca

Slika 7 prikazuje osnovne komponente PKI sustava kao što su:krajnji entitet(subjekti certifikata ili krajnji korisnici), registracijski centar, certifikacijski centar, spremište ili baza certifikata i izdavač opozvanih certifikata (komponenta PKI sustava koja služi za izdavanje lista certifikata)

2.6. SSL protokoli

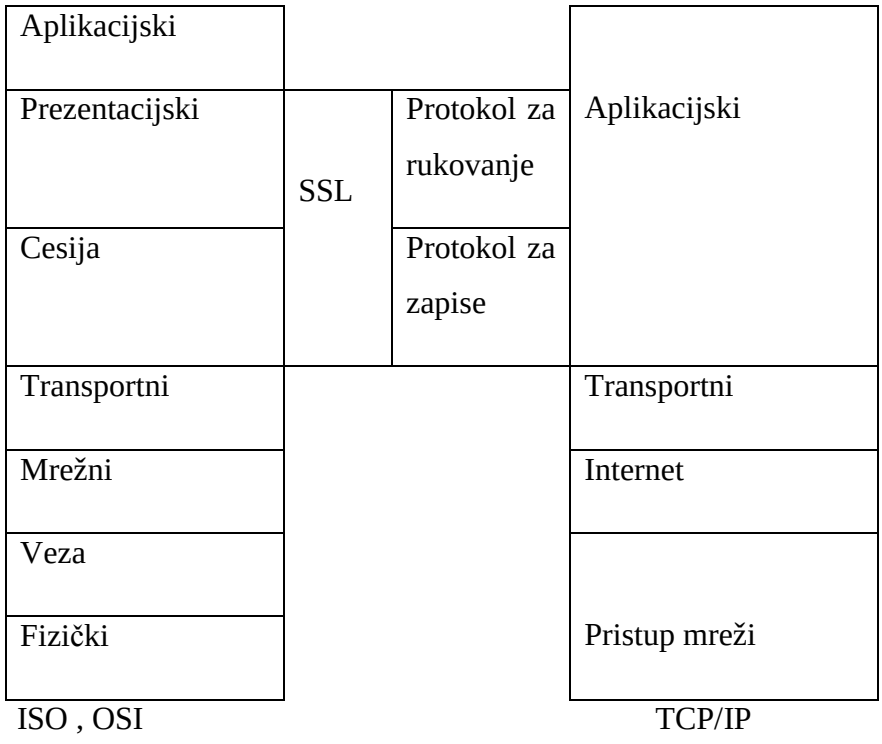
Protokol Secure Socket Layer ili skraćeno SSL je protokol koji osigurava mehanizme za identifikaciju dvaju sugovornika povezanih putem računalne mreže i koji imaju zaštićeni prijenos podataka između njih.

Protokol Secure Socket Layer osigurava sljedeće ciljeve:kriptografsku zaštitu, nezavisnost od softvera i hardvera, proširivost i efikasnost. Kriptografska zaštita osigurava mehanizme za šifriranje podataka, to jest, za ostvarivanje sigurne veze u komunikaciji između dvaju sugovornika. Nezavisnost od softvera i hardvera je vrsta ciljeva koja omogućava programerima da napišu softver sa dva različita programa(na primjer, Web server i Web čitač), tako da mogu zamijeniti parametre šifriranja. Kod proširivosti okvir treba biti tako napravljen, da se u slučaju potrebe mogu uklopiti novi simetrični algoritmi i algoritmi s javnim ključem. S tim funkcionalnim okvirom istovremeno izbjegavamo potrebu za

projektiranjem novih protokola. Kod efikasnosti SSL pamti komunikacijske parametre ostvarenih veza, kako bi se smanjio broj koji treba ponovno uspostavljati.

Zadatak SSL protokola je da omogući zaštitu podataka koji se prenose putem mreže. SSL osigurava identifikaciju za sever, za klijenta i šifriranu razmjenu podataka, što to čini zaštićen sistem komunikacije dvaju mrežnih entiteta. Za ostvarivanje ovakve zaštite potrebno je da SSL protokol sadržavaju oba dva mrežna entiteta. Zaštita komunikacije SSL-a ima svojstva:provjere, pouzdanosti i mogućnost provjere identiteta.

SSL se najčešće koristi u situacijama pri plaćanju robe kreditnom karticom, gdje se prenosi samo broj kreditne kartice i na taj način povećava sigurnost prilikom kupovine preko interneta.



Slika 8: SSL u skupu protokola

Izvor: Pleskonjić,D. i ostali,2013.

Slika 8 prikazuje kako SSL protokol stvara poseban komunikacijski sloj koji se nalazi iznad transportnog sloja. Iznad SSL-a nalazi se aplikacijski sloj. Na strani pošiljatelja, SSL dobiva poruku od aplikacijskog sloja koju potom rastavlja na manje složene dijelove kako bi bile pogodnije za dešifriranje. Također se dodaje kontrolni broj i šifrira rastavljene dijelove. Nakon toga, pošiljatelj šalje šifrirane dijelove poruke,a primatelj prima dijelove te ih dešifrira

i provjeri kontrolne brojeve. Sedam slojeva OSI referentnog oblika su[40]: application, presentation, session, transport, network, dana link i physical layer. ISO opisuje mrežni sistem.

SSL se sastoji od dva protokola[41]:

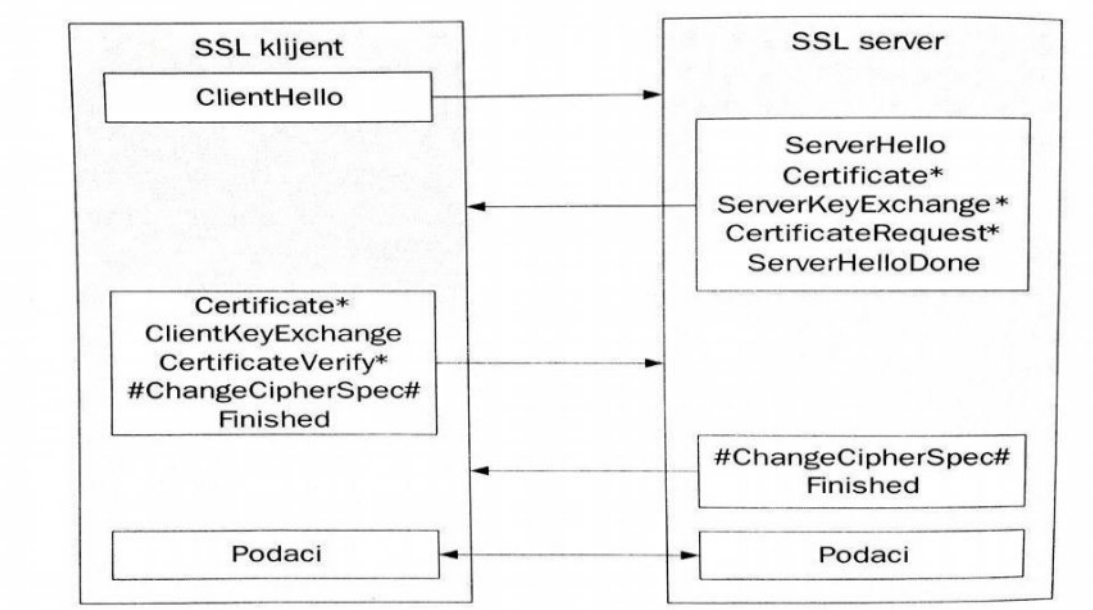
- SSL Handshake ili protokol za rukovanje,to jest, uspostavljanje sesije
- SSL Record ili protokol za zapise

SSL zahtjeva identifikaciju servera kako bih se uspostavio zaštićen prijenos. To se događa u fazi uspostavljanja sesije, slanjem certifikata klijentu. Za identifikaciju je potreban digitalni potpis servera i javni ključ. Nakon toga, klijent i server mogu razmijeniti poruke koji su šifrirane simetričnim algoritmom. Nakon identifikacije klijenta može početi razmjena podataka. SSL također nudi mogućnost uspostavljanja veze između servera i klijenta bez njihove identifikacije, ali time razine zaštite podataka se drastično smanjiva.

2.6.1. SSL protokol za rukovanje

SSL protokol za rukovanje djeluje iznad SSL protokola za zapise, a njegova važna uloga je stvaranje atributa kojim se opisuje sesija. Protokol za rukovanje šalje poruke protokolu za zapise, koji ih potom šifrira i šalje. Kada SSL server i SSL klijent krenu komunicirati, dogovaraju se o verziji protokola, a potom o izboru algoritama za simetrično šifriranje. Identificiraju se i koriste algoritam javnog ključa kako bi podijelili tajnu odnosno ključ za simetrično šifriranje.

[40] https://sysportal.carnet.hr/node/352
[41] Pleskonjić,D. i ostali, 2007, str.177



Slika 9:SSL protokol za rukovanje

Izvor: Pleskonjić,D. i ostali,2013.

Slika 9 prikazuje sav proces koji se zbiva u protokolu za rukovanje. Prvo, SSL klijent šalje poruku ClientHello, na koju SSL server odgovara svojim pozdravom ServerHello; u suprotnom, komunikacija se prekida. Pozdravne poruke koriste za kako bi se uspostavile: verzije protokola, algoritmi šifriranja, identifikator sesije, algoritmi za kompresiju i slučajne vrijednosti koje uspostavljaju klijent i server. SSL klijent prilikom svog pozdrava nudi SSL serveru popis mogućih načina šifriranja i sažimanja. Iz tog popisa sever odabire najbolju kombinaciju koju može prihvatiti. Nakon pozdravne poruke server šalje Certificate kojeg često treba identificirati. SSL server koji je pozitivno identificiran u mogućnosti je potražiti od klijenta certifikat (CertificateRequest), ukoliko je sve po dogovoru, server šalje poruku o završetku pozdrava (ServerHelloDone). Ukoliko je SSL server zatražio od SSL klijenta certifikat, onda server očekuje odgovor koji sadržava certifikacijsku poruku ili izvještaj da SSL klijent ne podržava certifikat.

Slijedeća radnja je da SSL klijent šalje nove atribute(#ChangeCipherSpec#) kojima će slati šifrirane podatke i potom „nove atribute“ zamjenjiva za „aktivne atribute“. Nakon toga se šalje izvještaj o završetku slanja, koji je šifriran „aktivnim atributima“ (Finished).

Faza uspostavljanja sesije je završena, te SSL server i SSL klijent mogu početi razmjenjivati podatke sa aplikacijskog sloja.

2.6.2. SSL protokol za zapise

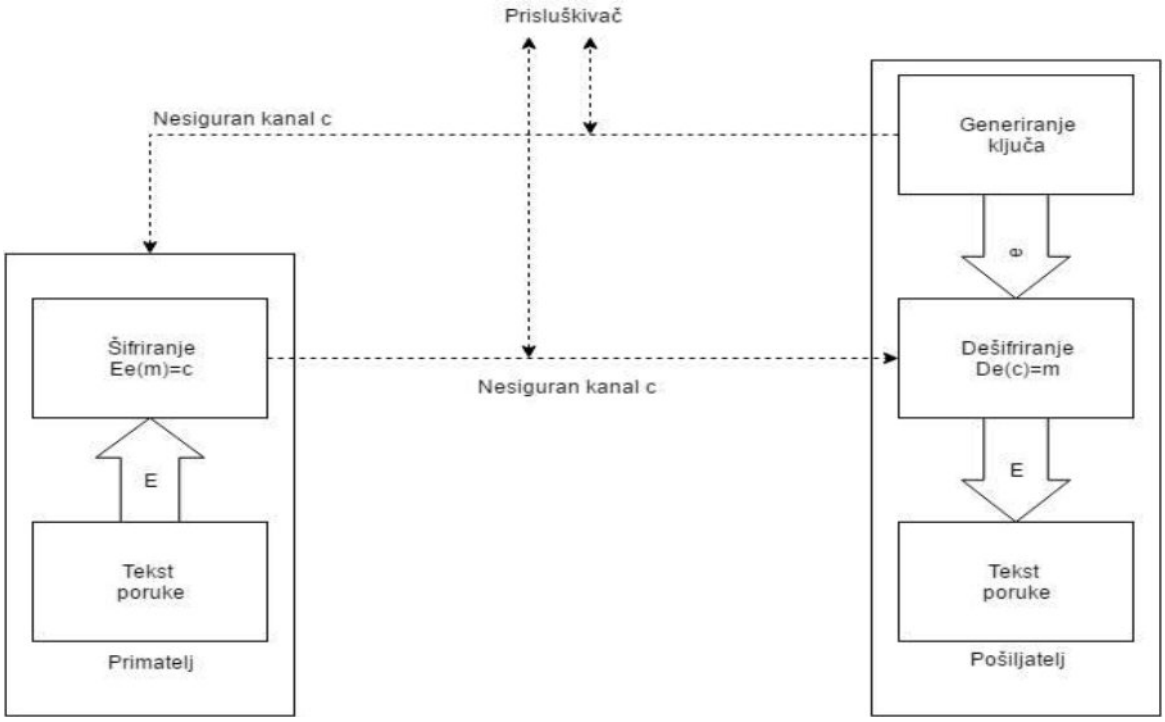
SSL protokol za zapise prima podatke s višeg sloja u blokovima proizvoljnih veličina, ne interpretira ih, već ih razdvaja na dijelove odgovarajuće veličine, kriptografski štiti i kriptografski šalje sugovorniku, gdje se odvija obrnuti proces[42]. Slijedi opis poslova na strani pošiljatelja. Prije buduće obrade, primljeni podaci će se dijeliti na blokove fiksne dužine. Time se ne obraća pažnja na dužinu klijentove poruke. Također tim načinom se više klijentskih poruka može povezati u jedan fragment ili jednu poruku podijeliti na više fragmenata. Svi fragmenti protokola koji se zapisuju, komprimiraju se algoritmom definiranim u atributu sesije. Algoritam treba imati biti takav da ne gubi podatke prilikom kompresije. Ukoliko u atributima, sesija kompresije ima NULL[43] vrijednost, tada se kompresija ne izvršava.Poruke imaju zaštitu simetričnim algoritmom za šifriranje i algoritmom MAC, koji su određeni atributima sesije. Ukoliko se u tim atributima nalaze zapisane NULL vrijednosti, podaci neće biti zaštićeni. Nakon šifriranja fragmenta i dodavanja MAC vrijednosti, rezultat se može poslati. MAC je dio informacije koji se koristi za autentifikaciju poruke. Uz takav obrađeni fragment šalju se i ostali podaci koji su nužni za prijenos poruke.

2.7. Kriptografija

Skrivanje i enkripcija prikazuju način koji ograničava pristup podacima. Algoritam enkripcije predstavlja matematičku metodu, javnu ili privatnu, kojim se pomoću ključa izvorni tekst mijenja u kriptogram, odnosno kriptogram u izvorni tekst, dok ključ opisuje način primjene transformacija kroz algoritam.[44] Kriptografija može osigurati sadržaj poruke i pruža sigurnost izvornom tekstu. Kriptoanaliza je suprotna funkcija kriptografije, a predstavlja transformacije za neovlašteno otkrivanje šifriranog sadržaja.[45] Iz istog izvora osobe koje se bave kriptoanalizom nastoje iskoristiti mane u implementiranju algoritma, kao mane u veličini ključa radi identifikacije izvornog sadržaja. IDEA algoritam razvijen je 1990. Godine i objavljen pod nazivom IPES. a, radi s blokovima od 64 bita i ključem od 128 bita, a koristi se miješanim opcijama iz različitih algebarskih grupa. IDEA je vrlo povjerljiv i siguran algoritam zahvaljujući podršci od PGP-a[46]. Prije završne transformacije IDEA se sastoji od

[42] Pleskonjić,D. i ostali, 2007, str.177
[43] Vrijednost koja nedostaje
[44] Miroslav Bača „Uvod u računalnu sigurnost“, Narodne novine,Zagreb,2004, str 182
[45] Ibidem str 182
[46] Engl. Pretty Good Privacy

osam rundi. Asimetrični algoritmi nastali su kao odgovor na rješavanja problema koji je vezan za prijenos tajnog ključa preko kanala koji nisu sigurni. Ukoliko se poruka šifrira javnim ključem, tada se ona može dešifrirati samo s privatnim ključem i obratno. Asimetrični algoritmi u odnosu na simetrične algoritme sporiji su od 100 do 10 000 puta, pa se stoga najčešće koriste za prijenos kratkih poruka.[47]



Slika 10:Shematski prikaz prijenosa poruke asimetričnim algoritmom s javnim ključem
Izvor: Bača,M.,2013.

Kod slike 10 prilikom komunikacije svaki sudionik objavi javni ključ vlastitim potencijalnim sugovornicima. Nakon toga, svi sudionici koriste javni ključ za šifriranje poruke koju je u mogućosti dešifrirati samo vlasnik privatnog ključa. Takav mehanizam ne služi samo za prijenos poruka, moguće ga je i koristiti za digitalno potpisivanje poruka.

[47] Miroslav Bača „Uvod u računalnu sigurnost“, Narodne novine,Zagreb,2004, str 188

2.8. Hash funkcija

Hash funkcija omogućava pretvaranje podataka promjenjive dužine u izlazne podatke fiksne dužine, odnosno hash. Primjer je računanje vrijednosti operacije ekskluzivno ILI nad svim bajtovima poruke. Neovisno o dužini poruke rezultat će uvjek biti 1 bajt. Hash funkcija je preslikavanje tipa više u jedan, beskonačan skup se preslikava u konačan skup hash vrijednosti. Hash funkcije se dijele na jednoparametarske (ulazni argument je poruka) i dvoparametarske (ulazni argument su poruka i tajni ključ)[48]. Prema funkcionalnoj podjeli hash funkcije se dijele na mehanizme za uočavanje promjena i mehanizme za provjeru identiteta poruka. Jedan od glavnih problema sigurnosti je autentičnost korisnika. Sustav treba prepoznati da li je korisnik ovlašten ili neovlašten i zbog toga se korisnik prije ulaska u sistem treba identficirati. Nakon identifikacije, sustav korisniku daje pravo da upravlja samo određenim resursima za koje je taj korisnik ovlašten. Identitet se može provjeriti navođenjem povjerljivih insformacija (lozinka) specijalnim hardverom (ključevi i pametne kartice) ili provjerom biometrijskih atributa korisnika (otisak prsta, snimak mrežnice oka i potpis)[49]. Identifikacija korisnika najčešće se pregledava lozinkom jer za taj postupak nije potreban specijalan hardver već samo tipkovnica. Korisnik upisuje svoje korisničko ime, a zatim sistem traži potvrdu u obliku lozinke. Ako je vrijednost lozinke koja se nalazi u sustavu odgovarajuća, operativni sustav pretpostavlja da je korisnik zadovoljio korak identifikacije. Lozinke su ranjivo mjesto stoga se zahtjeva od korisnika da se redovito mjenjaju i da budu što složenije. U mnogim sustavima postoji politika jakih ili strogih lozinki. Ona definira minimalnu dužinu lozinke uz obvezatno korištenje velikih i malih slova te specijalnih znakova.

Jednosmjerna funkcija je funkcija oblika y=f(x) za koju vrijedi:[50]

- za x, f(x) se određuje relativno lako i efikasno
- za y=f(x), $x=f^3(y)$ određuje se relativno teško. Iako se $f^3(y)$ određuje relativno teško ne znači da je nemoguće odrediti x na osnovu poznatog y, već da je za to potrebno nekoliko milijuna godina ukoliko se koristi procesorska snaga svih računala na svijetu.

Jednosmjerna funkcija sa zamkom, tj. privatna jednosmjerna funkcija je funkcija za koju vrijedi:[51]

[48] Pleskonjić,D. i ostali, 2007, str. 107
[49] Pleskonjić,D. i ostali, 2007, str. 113
[50] *ibidem*, *str.*.106

- za x, f(x) određuje se relativno lako i efikasno,
- za y=f(x), $x=f^3(y)$ određuje se relativno teško,
- za y=f(x) i tajnu informaciju z (zamka), $x=g(f^3(y), z)$ određuje se relativno lako i efikasno.

Jednosmjerna hash funkcija h = H(m) je preslikavanje za koje vrijedi:[52]

- na osnovu ulaznog podatka m proizvoljne dužine, hash h fiksne dužine određuje se lako i efikasno
- na osnovu hash vrijednosti h, odgovarajući ulazni podaci m_1, m_2, itd., ne mogu se odrediti ili se određuju teško i neefikasno.

Na temelju istog izvora kolizija je pojava kada dvije ili više različitih ulaznih poruka rezultiraju istim izlazom. Hash funkcije se preslikavaju tipa više na jedan i upravo zbog toga nisu imune na kolizije. Ako se hash funkcije koriste u provjeri identiteta, to može predstavljati veliki problem.Iz istog izvora hash funkcije se spominju pod različitim imenima. Funkcije sažimanja, funkcije izrade otiska prsta, kriptografski kontrolni zbir. Vrlo su važne za kriptografiju i primjenjuju se u kriptografskim protokolim, za digitalni potpis i provjeru identiteta.

Algoritme MD2, MD4 i MD5 razvio je Ronald Rivest za RSA Dana Security, Inc[53]. Iz identičnog izvora sva tri algoritma proizvode 128-bitni hash s tim da je MD2 prilagođen 8-bitnim mikroprocesorima, dok su MD4 i MD5 prilagođeni 32-bitnim računalina. Sva tri algoritma mogu se koristiti besplatno, te nije potrebna licenca za korištenje. Utjecaj na odabir hash funkcije je dužina proizvedene hash vrijednosti. 64-bitni hash je prekratak što se može dokazati rođendanskim paradoksom. Dužina od 128 bitova je prihvatljiva, zbog toga što napadač koristi napad koji je osnovan na rođendanskom paradoksu, a pri tome treba izračunati hash od 2^{64} različitih dokumenata. Takav pristup je puno kompliciraniji od računanja 2^{32} hasha, i puno je teže pronaći dva dokumenta sa istim hash vrijednostima. MD2, MD4 i MD5 hash dužine 128 bitova,a SHA i RIPEMD-160 proizvode hash dužine 160 bitova, što

[51] *ibidem, str.* 106
[52] *ibidem, str* .107
[53] *ibidem, str..*107

odgovara dužini koju je NIST propisao za SHS (engl. *secure hash standard*)[54]. Hash se može uvećati pomoću algoritama:[55]

- $h_1 = H(m)$
- $h_2 = h_1|H(h_1| m)$
- $h_3 = h_2|H(h_2| m)$

[54] *ibidem, str.* 108
[55] *ibidem, str* .108

3. PRIVATNOST

Razvijanjem Internet, razvila se i zloupotreba korisnikovih osobnih podatka čime se narušava korisnikova privatnost. Marketinški stručnjaci postali su veoma efikasni prilikom analiziranja i prikupljanja detaljnih podataka o potrošaču. Marketinški stručnjaci su u mogućnosti pratiti posjetitelje njihovih stranica, a mnogi potrošači koji ih posjećuju ostavljaju svoje osobne podatke. Tvrtke mogu zlouporabiti korisnikove podatke, tako da ih razmjenjuju sa ostalim tvrtkama ili ih koriste u privatne marketinške svrhe, čime dolazi do informacijske zlouporabe. Radi toga danas postoji velik broj korisnika koji su zabrinuti za svoju sigurnost i privatnost na Internetu, a razlog je zato što postoje marketinški prevaranti koji prate korisnikove transakcije i brojeve kreditnih kartice i time imaju mogućnost obavljati kupovinu preko Interneta.

3.1 Zaštita privatnosti korisnika

Problem zaštite privatnosti korisnika pripada u područje zaštite ljudskih prava, privatnost će biti ugrožena svakim neprimjerenim korištenjem informacijske tehnologije. Slijedi nekoliko naputaka o mogućim aktivnostima s time u svezi:[56]

- Kupac bi se trebao unaprijed informirati o politici zaštite privatnosti što je podržava trgovac, dakle, prije no što uopće posjeti njegovo Web mjesto i upusti se u trgovanje. Do takvih se informacija može u Internetu doći na mnogo raznih formalnih i neformalnih načina (sudjelovanje u radu diskusijskih skupina, elektroničke ploče, brbljanje, surfanje, itd).
- Valja se prikloniti onim elektroničkim trgovcima koji podržavaju politiku nemiješanja u privatnost kupaca. U sklopu takve politike trgovci se obvezuju da informacije o svojim kupcima do kojih su došli na bilo kakav način neće dijeliti s drugim kompanijama i tako „denuncirati“ svoje kupce.
- Uvijek kada se ispunjava neki ekranski ili drugi obrasci, dobro je u njih unijeti samo minimum traženih informacija. To je posebno važno imati na umu onda kada trgovac ili neka marketinška agencija probode ankete i druge vrste „opipavanja bila“ potrošača, jer nije rijetkost da se pri tome, svjesno ili ne, prekorači granica minimuma privatnosti ispitanika. Sve ono što se čini sumnjivim u upitnicima i sličnim dokumentima valja naprosto ignorirati.

[56] Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000, str. 202,203

- Uvijek pri ispunjavanju bilo kakvih elektroničkih obrazaca treba pomno pročitati ono što, obično negdje pri kraju, piše „sitnim slovima“. Na takvim se mjestima nerijetko kriju zamke koje mogu ugroziti privatnost kupca.
- Valja provjeriti podržava li politiku privatnosti neki konkretan trgovac u suglasju s pravilima i kriterijima što ih proklamiraju organizacije za zaštitu ljudskih prava.
- Kupac može, ako to smatra potrebnim, zaštititi od „kolačića“. Načelno, ne bi trebalo svakome dopustiti da postavlja „kolačiće“ na klijentov disk, što zbog zaštite privatnosti, a što zbog opasnosti od zaraze virusima. Tako, primjerice, oba najpoznatija internetska pretražnika, Microsoft Explorer i Netscape Navigator, nude takve opcije („Disable All Cookies Use“ ili neka slična opcija).

3.2. Zakoni u Republici Hrvatskoj u vezi privatnosti podataka

E-trgovac je prema zakonu obvezan omogućiti zaštitu osobnih podataka korisnika i privatnost kupaca elektroničke trgovine. Ukoliko se trgovac drži pravila on će korisnikove podatke koristiti u svrhe koje on nudi. Trgovac poštuje svoje korisnike i pruža ima visok stupanj povjerljivosti osobnih podataka, kako bi svoje korisnike zaštitio pred mogućom opasnosti. Ako trgovac poštuje izjavu o čuvanju osobnih podataka, tada on neće *„ni pod koju cijenu“* proslijediti ili omogućiti uvid u osobne podatke svojih korisnika nekoj *„trećoj“* osobi, iznimka je ukoliko državne institucije zahtijevaju uvid u podatke.

Zakon u Hrvatskoj koji se odnosi na privatnost podataka prilikom elektroničkih transakcija je zakon o elektroničkom trgovanju. Odredbe se ovoga Zakona ne primjenjuju na zaštitu podataka, područje oporezivanja, javnobilježničku djelatnost, zastupanje stranaka i zaštitu njihovih interesa pred sudovima, te na igre na sreću s novčanim ulozima, uključujući lutrijske igre, igre u casinima, kladioničke igre i igre na sreću u automatima, a u skladu s odredbama posebnih zakona koji uređuju odnosna područja. Prema zakonu o elektroničkoj trgovini(NN, br. 173/03, 67/08 i 36/09), članak 22.a govori da, onaj tko smatra da davatelj usluga krši neko njegovo pravo, može podnijeti tužbu nadležnom sudu u skladu sa zakonom[57]. Članak 22.b, onaj tko smatra da davatelj usluga krši neko njegovo pravo, može nadležnom sudu podnijeti zahtjev za određivanje privremene mjere. Ako ovim Zakonom nije propisano drugačije, u

[57] http://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini

postupku za određivanje privremene mjere primjenjuju se odredbe zakona koji uređuju pitanja ovrhe i osiguranja.[58]

3.3. Zakonski propisi privatnosti podataka u SAD-u

Federal Trade Comission (FTC) je nezavisna vladina agencija koja je iznijela nekoliko korisnih savjeta i uputa kako američki državljani mogu očuvati svoju privatnost i izbjeći nepoželjne situacije putem kupovine preko Interneta. Treba dobro proučiti s čim se bavi potencijalni prodavatelj, pošto danas svatko može otvoriti trgovinu na Internetu pod bilo čijim imenom. Na e-mailove ili pop-up poruke koje pitaju za financijske podatke treba uopće ne treba odgovarati niti pratiti sljedeće linkove. Legitimne tvrtke neće tražiti privatne informacije na taj način. FTC ističe da treba pročitati prodavateljev opis i usporediti cijene proizvoda koji želimo kupiti s ostalim prodavateljima. FTC upozorava na to, da se ne šalje gotovina ili transfer novca ni pod kojim uvjetima. Također, treba provjeriti može li se vratiti sav novac ukoliko proizvod ili usluga nije u skladu s očekivanim i tko će platiti troškove prijevoza. FTC upozorava na to da treba voditi evidenciju transakcija. To jest, da nakon svake transakcije treba zapisati i spremiti podatke o cijeni, o izmijenjenim e-mail porukama sa trgovcem, kao i o opisu proizvodu. FTC ističe da putem e-maila se ne objavljuju nikakvi financijski podaci. E-mail nije ni malo siguran način slanja financijskih informacija naspram kreditnih kartica i tekućih računa. Ukoliko se odabere takav način slanja podataka da se osobne informacije ostavljaju na web-u, treba odabrati one web stranice kojima URL započinje sa htpps.

Ukoliko se proizvod ili usluga plaća putem kreditne kartice ona će biti osigurana sa Fair Credit Billing Act ili FCBA. FCBA je savezni zakon koji je dizajniran kako bi mogao zaštiti potrošače od nepoželjnih situacija prilikom kreditne naplate. Zakon o Fair Credit naplati daje upute vjerovnicima i potrošačima. Također, zakon uključuje kakve postupke i akcije treba učiniti prilikom upravljanja sporova u vezi izjave o naplati.

3.4. Zakonski propisi privatnosti elektroničke trgovine u EU

Neovisno gdje se kupi proizvod u EU, trgovac treba dati točne, povjerljive i jasne informacije o proizvodu ili usluzi prije kupovine. Ugovor o kupnji treba sadržavati:[59] glavne karakteristike proizvoda, ukupnu cijenu uključujući poreze i sve troškove, troškove isporuke, dogovore za plaćanja, isporuke ili izvršenja, zatim identitet trgovca, geografska adresa i broj telefona,

[58] http://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini
[59] http://europa.eu/youreurope/citizens/consumers/shopping/contract-information/index_en.htm

trajanje ugovora. Zaštita osobnih privatnih podataka temeljno je pravo i sadržana je u Lisabonskome ugovoru. Povelja o temeljnim pravima Europske unije propisuje da svatko ima pravo na protekciju osobnih podataka. Ti podaci se trebaju obrađivati korektno za posebne namjene. Obrada osobnih podataka treba biti poštena, zakonita i razmjerna. Podaci od pojedinaca koje daju izravno ili neizravno ne bi se trebale koristiti za druge svrhe, nego što je prvobitno namijenjen. Prava Europske unije odnose se na svakoga, neovisno o nacionalnosti ili mjestu stanovanja. Osobni podaci koji otkrivaju rasno ili etničko podrijetlo, politička stajališta, vjerska ili filozofska uvjerenja, članstva u sindikatima i obradu podataka o zdravlju ili spolnom životu, je dopušteno samo uz izričitu suglasnost pojedinca.[60]

Pojedinci imaju pravo dobiti informacije od ljudi i tvrtki koje imaju neke od njihovih osobnih podataka u svojim datotekama, kao što su web stranice, baze podataka, usluge ("kontrolore podataka"), i oni imaju pravo ispraviti ili izbrisati ove podatke ako su nepotpuni ili netočni[61]:

- Kontrolori podataka dužni su obavijestiti potrošače kada će prikupljati osobne podatke o njima.
- Pojedinci imaju pravo znati ime kontrolora podataka, namjenu obrade podataka, i kome se podaci mogu prenositi.
- Pojedinci imaju pravo pitati kontrolora podataka, hoće li će on obrađivati osobne podatke.
- Pojedinci imaju pravo dobiti kopiju njihovih podataka u razumljivom obliku.
- Pojedinci imaju pravo tražiti blokiranje ili brisanje podataka ako su nepotpuni, netočni ili dobiveni nezakonito.
- Pojedinci imaju pravo usprotiviti se obradi osobnih podataka.

[60] https://ec.europa.eu/digital-single-market/en/code-eu-online-rights
[61] https://ec.europa.eu/digital-single-market/en/code-eu-online-rights

4. ZAKLJUČAK

Svima je jasno da privatnost u današnjem svijetu praktički i ne postoji. Cijeli Internet vrvi od privatnih informacija koje kolaju preko raznih društvenih mreža. Upravo iz tog razloga je potrebno voditi računa o sigurnosti. Ukoliko nešto želimo kupiti, moramo ostaviti podatke na Web stranici na kojoj se nalazi željeni proizvod. Na taj način, mi svoje osobne podatke stavljamo na raspolaganja određenoj kompaniji, a o njoj ovisi za što će ona rabiti te informacije. Danas je česta pojava da kompanije trguju informacijama korisnika, najveći primjer je Google. Na taj način informacije mogu stići do zlonamjernih korisnika koji te informacije mogu zloupotrijebiti. Takve stvari je vrlo teško izbjeći, ali ih se može umanjiti Stoga svaki puta kada se pristupa određenoj web stranici, poželjno bi bilo da se informiramo, na primjer čitanjem raznih foruma na kojima korisnici mogu izraziti svoja mišljenja.

Svijet je pun internetskog kriminala. Sami trebamo biti dobro informirani da zaštitimo osobne podatke. Zahvaljujući stručnjacima u tom području koji se bore protiv mogućih opasnosti, te opasnosti možemo smanjiti na minimalnu razinu. Osobne podatke treba što manje izlagati ukoliko to nije potrebno zbog zlonamjernih korisnika. Treba znati kako funkcionira kupoprodaja na elektroničkoj trgovini. Najbolja zaštita korisnika je definitivno informiranost prije same kupovine. Ljudi su počeli biti svjesniji tog problema u novije vrijeme, tako što se samostalno obrazuju ili u infrastrukturama u kojima postoje takvi programi. Na internetu nikome se ne smije vjerovati, čak i s onim s kojima komuniciramo svaki dan, jer možda baš iza tog „ekrana“ u tom trenutku stoji neka treća osoba koja želi iskoristiti naše podatke.

Ukoliko tvrtka želi podići stupanj reputacije, ona treba održavati pozitivne odnose sa svojim klijentima. A takve odnose može održavati pomoću kvalitetnog rada na privatnosti kupca. Taj odnos će zadovoljiti obje strane, prodavač će zaraditi profit, a kupac će dobiti kvalitetnu uslugu kakvu je i sam očekivao. Kvalitetnu uslugu koju kupac dobije od prodavača je prodavaču najbolja moguća reklama, pošto će kupac širiti svoja iskustva s tim prodavačem i na taj način mu maksimizirati reputaciju.

5. POPIS SLIKA

Slika 1: Sustav elektroničkog poslovanja..…….3

Slika 2: Elektronička prodaja materijalnih dobara……...5

Slika 3: Elektronička prodaja nematerijalnih dobara….……..5

Slika 4:B2B i B2c……...10

Slika 5: Kreiranje digitalnog potpisa…….…….....15

Slika 6: Provjera digitalnog potpisa……..…….…15

Slika 7: Sustav infrastrukture javnog ključa ……..18

Slika 8: SSL u skupu protokola….……..19

Slika 9: SSL protokol za rukovanje…….21

Slika 10::Shematski prikaz prijenosa poruke asimetričnim algoritmom s javnim ključem...23

6. LITERATURA

a) Knjige

D. Pleskonjić, N. Maček, B. Đorđević, M. Carić: “Sigurnost računarskih sistema i mreža”, Mikro knjiga, Beograd, 2007

Prof.dr.sc.Željko Panian;Elektroničko poslovanje druge generacije, Ekonomski Faukltet, Zagreb, 2013

Miroslav Bača „Uvod u računalnu sigurnost“, Narodne novine,Zagreb,2004

Panian, Željko, Elektroničko trgovanje, Sinergija, Zagreb, 2000

b) Internet

http://os2.zemris.fer.hr/pki/2005_rebac/(11.09.2015)

http://security.lss.hr/images/dokumenti/lss-pubdoc-2010-10-002.pdf (12.09.2015)

http://www.odbojkaskaoprema.hr/politika-privatnosti (09.09.2015)

file:///C:/Users/Korisnik/Downloads/Dosezi_elektronicke_trgovine_u_Hrvatskoj_i_svijetu.pdf(08.09.2015) (12.09.2015)

http://e-ucenje.unipu.hr/mod/resource/view.php?id=673 (15.09.2015)

http://savjetnik.ba/wp-content/uploads/2011/06/b2b%20poslovni%20koncept.pdf (16.09.2015)

http://www.oblakznanja.com/2011/07/sto-je-internet/ (16.09.2015)

http://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini (17.09.2015)

https://sysportal.carnet.hr/node/352 (17.05.2016)

http://europa.eu/youreurope/citizens/consumers/shopping/contract-information/index_en.html (17.05.2016)

https://ec.europa.eu/digital-single-market/en/code-eu-online-rights (17.05.2016)

http://www.zakon.hr/z/199/Zakon-o-elektroni%C4%8Dkoj-trgovini (17.05. 2016)

http://www.moj-bankar.hr/kazalo/R/Rizik (16.05.2016)

https://www.ftc.gov/about-ftc (17.05.2016)