ŠOLSKI CENTER CELJE
Splošna in strokovna gimnazija Lava

VARNO E-BANČNIŠTVO

Raziskovalna naloga

Mentorica:
Karmen KOTNIK, univ. dipl. inž.

Avtorica:
Karmen KOLAR, 4. e

Celje, marec 2005

Kazalo Vsebine

Kazalo slik

Kazalo tabel

1 Povzetek

V raziskovalni nalogi sem predstavila varnost informacijskega sistema elektronske banke, varnost povezave in prenosa podatkov med banko in varnost, ki jo banka zagotavlja uporabnikom.

Temo raziskovalne naloge, varno e-bančništvo sem si izbrala zato, ker me je vedno zanimalo, ali je sistem elektronskega bančništva v Sloveniji dovolj varen za uporabo.

Pri raziskovanju tega problema sem prišla do zaključka, da imamo v Sloveniji zagotovljeno zelo visoko varnost. Če nimamo časa stati v vrstah pred bančnimi okenci, ali če te storitve radi opravljamo prav v času, ko je banka zaprta, se lahko brez oklevanja odločimo za storitve e-banke. Na žalost je varnost trenutna, saj se vsakodnevno ukvarjamo z novimi virusi, in v bodoče je težko predvideti, kako se načrtujejo vdori v elektronsko banko.

Pri raziskovanju sem uporabila metodo analiza literature.

2 Uvod

V raziskovalni nalogi sem poskusila raziskati, če drži moja predpostavka, da je varnost sistema in zasebnost uporabnika pri uporabi e-bančništva zagotovljena. V bankah sem se pozanimala, kakšno varnost zagotavljajo pri uporabi e-bančništva ter v knjižicah poiskala vrsto literature na to temo. Nato sem literaturo dobro preučila.

Varnost e-bančništva ima namreč pomembno vlogo. Če ljudje niso prepričani o varnosti, se ne odločajo za uporabo e-bančništva. Elektronsko poslovanje pa brez tega nima smisla. Varnost dosegamo z zaščito podatkov tako, da jih zašifriramo in elektronsko podpišemo. Držati se moramo tudi varnostnih ukrepov. Uporabljati samo enkratna gesla ali pa bolj zanesljive pametne kartice. Banke pa nam z svoje strani zagotavljajo varnost z uporabo raznih principov in protokolov kot je SSL (Secure Socket Layer) ter s požarnimi zidovi (firewall). Informacije morajo potovati hitro, enostavno in po varni poti.

Torej e-bančništvo omogoča varno, hitrejše in lažje opravljanje bančnih storitev. Pridobimo si čas, nimamo opravka s papirnatimi obrazci in izognemo se čakalnim vrstam pred bančnimi okenci. Zato uporabljamo elektronsko bančništvo na domu ali v podjetju v času, ki nam najbolj ustreza, saj je odpiralni čas bank za marsikatero podjetje in tudi posameznika nesprejemljiv. Zelo pomembna pri elektronskem bančništvu pa je zasebnost.

3 Kaj omogoča e-bančništvo

Uporabniku ponuja hiter in varen način poslovanja z banko. Takšno poslovanje prinaša mnoge prednosti – poslovanje 24 ur na dan, prihranek časa in denarja, stalen pregled stanja na računih, neodvisnost od poslovnega časa bančnih enot, možnost opravljanja številnih storitev in zasebnost.

Elektronsko bančništvo omogoča komitentom (pravna ali fizična oseba, za katero trgovski posrednik opravlja trgovske ali bančne posle) vpogled v celotno poslovno sodelovanje z določeno banko, ter možnost opravljanja plačilnega prometa. Ob pomoči sistema elektronskega bančništva, so uporabniku kadarkoli na voljo mnogi uporabni podatki za poslovanje. Storitev je namenjena pravnim in fizičnim osebam.

Za delovanje elektronskega bančništva je potreben dostop do interneta, najprej pa je potrebna inštalacija programske opreme določene banke.

Štiri največje slovenske banke in njihove elektronske banke:

	Fizične osebe	**Pravne osebe**
A banka d.d., Ljubljana	Abanet	Abacom
NLB d.d, Ljubljana	Klik NLB	Proklik NLB, Proklik +
SKB Banka d.d., Ljubljana	SKB net	SKB net
Nova kreditna banka Maribor d.d., Maribor	Bank@NET	Poslovni Bank@NET

Tabela 1: E-banke za pravne in fizične osebe

E-bančništvo lahko omogoča:

- vpogled v stanje na računu,
- pregled prometa na računu v določenem obdobju,
- pregled izpiskov,
- pregled sporočil,
- povečanje limita,
- vezavo sredstev (depozit),
- prenos sredstev med računi v matični banki in na račune drugih bank.

<u>Primer storitve elektronske NLB:</u>

Klik NLB je način opravljanja bančnih storitev preko interneta, ki uporabniku omogoča kar od doma, med delom ali na potovanjih 24 ur na dan:

- vpogled v stanje na svojih računih in računih na katerih je pooblaščen,
- poravnavo obveznosti s posebno položnico, s plačilnim nalogom,

- prenos sredstev med računi v matični banki in na račune drugih bank,
- povečanje limita na svojem računu,
- odpiranje in ukinitev trajnih pooblastil,
- vezavo sredstev (depozit),
- pošiljanje in sprejemanje sporočil banke,
- pregled arhiva transakcij opravljenih v Kliku NLB.

Vsak uporabnik, ki želi delati preko Klika NLB mora imeti:

- dostop do interneta,
- elektronski naslov,
- spletni brskalnik (Explorer ali Netscape Communicator).

Vsakdo, ki želi postati uporabnik Klika NLB mora izpolniti:

- Vlogo za izdajo digitalnega kvalificiranega potrdila (certifikata) za fizične osebe (obr. CNLVB 01).
- Zahtevek za Klik (obrazec Klik 02).
- Obrazec Klik 03 – v kolikor želi uporabnik delati tudi z računi na katerih je pooblaščen.

Slika 1: Vstopna točka v e-banko na spletni strani KLIK NLB

Vsi podatki, ki se prenašajo med komitentom in banko po javnem omrežju, morajo biti šifrirani (kriptirani/ kodirani). S tem zagotovimo varen prenos podatkov, saj so podatki neprepoznavni. Ker iz teh kodiranih podatkov ne moramo prepoznati uporabnika, so preneseni podatki elektronsko podpisani še z digitalnim potrdilom.

V nadaljevanju bom predstavila sistem šifriranja podatkov ter varnostne ukrepe. Ti zagotavljajo varnost in zasebnost uporabnikov, ki uporabljajo storitve e-bančništva.

4 Kriptologija

Zagotovljena mora biti varnost dostopa in uporabe. Tako je zagotovljena varnost elektronskih transakcij. Ker bi lahko en sam vdor v bančni sistem pustil nepopravljive posledice, se posveča velika pozornost varnosti elektronskih sistemov. Varnost pa dosegamo z šifriranjem podatkov. Najprej pa spoznajmo znanost, ki nam omogoča varovanje in zaščito podatkov, ki se prenašajo pri elektronskem bančništvu.

Kriptologija je veda o šifriranju, tajnosti, zakrivanju sporočil (kriptografija) in razkrivanju šifriranih podatkov (kriptoanaliza). Beseda izhaja iz grščine "kryptos logos" (skrita beseda). Kriptoanaliza je znanost o razbijanju zaščite šifriranih podatkov in njihovi analizi.

4.1 Kriptografija

Eden izmed najpomembnejših ukrepov za varnost elektronskega poslovanja je uporaba kriptografije. Kriptografija je znanost za šifriranje in dešifriranje z uporabo matematike. Njen namen je shranjevanje in prenos podatkov preko nezavarovanih podatkovnih kanalov, tako da jih prebere le tista oseba, ki so ji podatki namenjeni.

Transakcije se v elektronskih bankah izvajajo preko komunikacijskih medijev, zaščita pa se dosega z upoštevanjem osnovnih varnostnih principov:

- **Pristnost (*authentication*):** prejemniku zagotavlja, da je sporočilo res poslal pošiljatelj in da ni ponarejeno. Prisotna je uporaba digitalnih podpisov, certifikatov in gesel.
- **Avtorizacija (*authorisation*):** do podatkov lahko pride le tisti, ki je pooblaščen. Prisotna je uporaba imena in gesla ter biometrična identifikacija.
- **Zaupnost (*confifentiality*):** preprečuje nepooblaščeno razkritje podatkov. Prisotna je uporaba šifriranja, kriptografije, zaupanja vredne tretje strani (CA- Certifiying Authority).
- **Celovitost (*integrity*):** podatki se med prenosom ne spreminjajo. Prisotna je uporaba šifriranja in digitalnih podpisov.
- **Nezavrnitev (*nonrepudation*):** zaščita pred tem, da bi pošiljatelj lažno zanikal, da je podatke poslal, ali prejemnik lažno zanikal, da jih je sprejel.
- **Nadzor pretoka (*transfer control*) –** obrambni zid (*firewall*).

- **Tajnost**: podatki so namenjeni le naslovniku, tako da nikomur drugemu ni treba vedeti za prenos.

Elektronska banka mora omogočiti, da so podatki o plačilnih transakcijah tajni, in da jih lahko prebere le tisti, ki so mu podatki namenjeni. To zagotavlja šifriranje (kriptiranje) pri pošiljatelju in dešifriranje (dekriptiranje) pri prejemniku.

4.1.1 Šifriranje

Da lahko sporočilo varno pošljemo, ga moramo najprej zašifrirati. Sporočilo s šifrirnim algoritmom zašifriramo, pri čemer uporabimo ključ (zaporedje znakov/ sinonim za geslo), ki je nekakšna vrednost za parametre v algoritmu. Šifrirni algoritem vrne kot rezultat zašifrirano sporočilo (tajnopis/ šifropis/ kriptogram). Sogovornika morata biti dogovorjena o algoritmu in ključu, tako da si lahko pošiljata šifrirana sporočila. S šifriranjem prikrijemo vsebino pred napadalci, katerim sporočilo ni namenjeno. Od dolžine ključa in šifrirnega algoritma je odvisna tajnost šifriranih podatkov. S procesom dešifriranja dobimo nazaj pravo vsebino prikritega sporočila.

Podatke šifriramo običajno s simetričnimi kriptoalgoritmi, ključe za te algoritme pa z asimetričnimi.

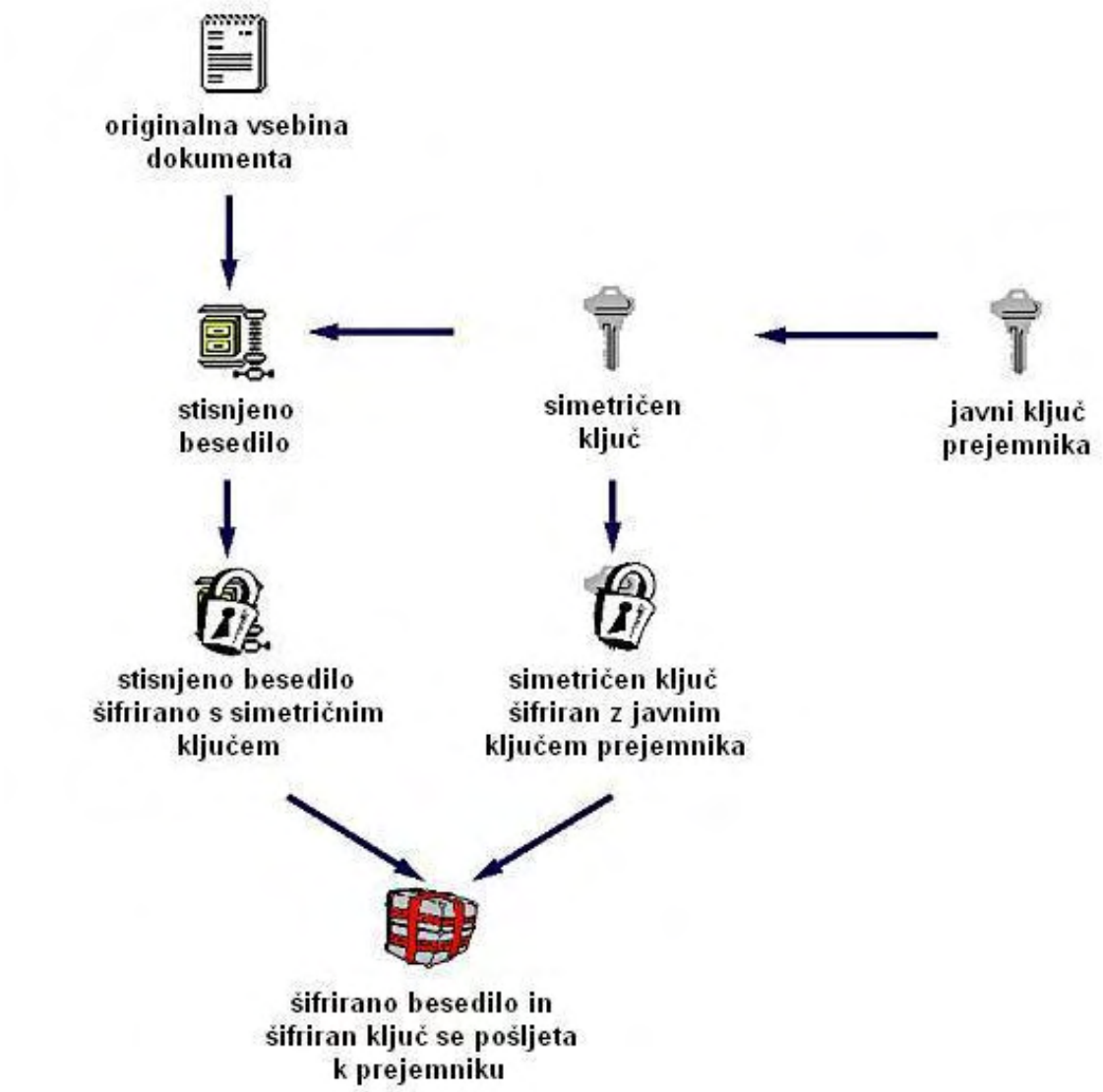
Slika 2: Javni in zasebni ključ

Varnostni ključ: po naključju izbrano zaporedje znakov, ki omogoča varno elektronsko poslovanje. Za šifriran prenos podatkov se v banki uporablja metodologija dvojnih ključev (*javni in zasebni ključ*). Zasebni ključ je sestavni del digitalnega potrdila, ki je tajen in shranjen na lastnikovem računalniku oziroma na pametni kartici. Javni ključ je pa tisti ključ, ki ga uporabnik objavi. Šifrirni ključ (cipher) določa delovanje algoritma.

Za šifriranje podatkov poznamo dve vrsti algoritmov:

- **simetrični algoritmi (DES, IDEA, AES, RC2, RC4, 3DES, FORTEZZA)**: za šifriranje in dešifriranje uporabljamo samo en tajen ključ, ki ga uporabljata tako pošiljatelj kot prejemnik. Problem predstavlja kako skupni ključ varno razdeliti med pooblaščene subjekte. Da dosežemo najvišjo varnost izmenjave ključev, uporabljamo simetrični algoritem hkrati z drugimi algoritmi.

- **asimetrični algoritem (RSA, ElGamal, ECC):** uporabnik ima dva ključa. Tisti ključ, katerega objavi, imenujemo javni ključ, tistega, ki pa shrani pa imenujemo zasebni ključ. Vsi, ki mu želijo sporočilo poslati, uporabljajo uporabnikov javni ključ za šifriranje sporočila. Slabosti, ki se pojavijo pri asimetričnih algoritmih, je overjanje javnih ključev ter hitrost šifriranja in dešifriranja. Asimetrična kriptografija torej uporablja infrastrukturo javnih ključev, t.i. strežnik PKI (Public Key Infrastructure). PKI ob pomoči digitalnih potrdil poskrbi za povezavo javnih ključev z realnimi objekti, razpečavo javnih ključev in vzpostavitev zaupanja v javne ključe. V njem so vključeni digitalni certifikati, šifriranje z javnimi ključi ter certifikatne agencije (izdajatelji certifikatov).



Slika 3: Proces šifriranja podatkov

Za varnost je pomembno, da je velikost in število ključev čim večja. Kako močno so zaščiteni podatki je odvisno od velikosti šifrirnega ključa. Pri šifriranju pa je najpametneje uporabiti že preizkušene algoritme, katerih velikost ključev je vsaj 72 bitov.

Večina slovenskih bank za avtentikacijo (identifikacijo) in izmenjavo ključev uporablja 1024-bitni asimetrični algoritem RSA, za kodiranje podatkov pa simetrični 128-bitni algoritem RC4. (Interno gradivo NLB in SKB, 2002)

5 Varnostni ukrepi

Ob zagonu programa oz. aplikacije določene banke, ki je nameščena na uporabnikovem osebnem računalniku, je potreben vnos uporabniškega imena in gesla za vstop. Tako se uporabnik lahko preko interneta poveže z banko ter pošilja in sprejema podatke. Uporabniško ime in geslo za prvi dostop določi pooblaščena oseba družbe. Za zagotovitev varnosti je potrebno geslo spremeniti vsaj enkrat mesečno. Geslo naj bi bilo sestavljeno iz velikih in malih črk ter številk, dolgih vsaj šest znakov.

Poznamo dva načina preverjanja identitete: enkratna gesla in pametne kartice. Enkratna gesla je mogoče uporabiti le enkrat, in veljajo le za trenutno povezavo, medtem ko pametna kartica nudi več možnosti identificiranja z geslom.

5.1 Pametna kartica

Ta varnostna kartica je plastična kartica, ki je namenjena preverjanju identitete, elektronskemu podpisovanju in šifriranju podatkov.

Uporablja se v vseh sodobnih bankah, saj je zaščita v elektronskih bankah ključnega pomena. Kartica je podlaga za identifikacijo uporabnikov in digitalno podpisovanje transakcij na podlagi zasebnih in javnih ključev, saj je na njej shranjeno digitalno potrdilo. V pametni kartici teče program za zaščito podatkov. Ta program nosi vlogo šifratorja, dešifratorja in podpisovalca podatkov.

Dostop do uporabe kartice je zaščiten z geslom, ki si ga uporabnik določi sam. Če uporabnik trikrat napačno vnese geslo, se kartica uniči.
Nekatere kartice pa vsebujejo mikroprocesor, majhen zaslon in uro, ki jo sinhronizira z uro v strežniku. Kartica generira novo geslo na podlagi časa (večina bank uporablja sistem ene minute), lastnik kartice pa ga pretipka z zaslona in geslo se pošlje do strežnika, ki preveri, če je geslo pravo. Geslo pozna le lastnik in elektronska banka. Tako je ob rednem menjavanju gesel zagotovljena večja varnost. Sodobnejše banke pa imajo že vgrajene tudi čitalnike prstnih odtisov, s čimer kartico res lahko uporablja samo njen pravi lastnik.

Če se kartica ne uporablja več kot dva meseca, lahko pride do desinhronizacije kartice z bančnim strežnikom. Takrat se v banko ne da več pošiljati sporočil. Da se kartica nazaj sinhronizira, je potrebno obvestiti skrbnika elektronskega bančništva. Varnostni mehanizmi za preklop preko interneta na bančno infrastrukturo, so na tej pametni kartici zelo zanesljivi. Banka pa še posebej zavaruje dostop preko interneta s požarnim zidom (*firewall)*. Tako uporabniki storitev dostopajo samo do strežnikov zunaj požarnega zidu. Pametna kartica se prejme ločeno v pošiljki in ob poskusu odpiranja se avtomatsko uniči.

Edina nevarnost pri pametnih karticah je ta, da lahko računalnik kartici podtakne v podpis drug element, pa tega ne bo opazila ne kartica, ne mi.

Za branje podatkov iz kartice uporabnik uporablja:

- **USB čitalec pametne kartice** (računalnik mora imeti USB priključek) ali
- **PCMCIA čitalec** (uporaben pri prenosnih računalnikih).

5.1.1 Primerjava varnostnega sistema Klika NLB in Bank@Net

	Kartica	*Ključ*	*Čitalec kartic*
Klik NLB	Pametna kartica	da, 128-bitni	da
Bank@Net	Identifikacijska (ID) kartica	ne	ne

Tabela 2: Varnostni mehanizmi NLB in NKB

Elektronska banka Nove Ljubljanske Banke, Klik NLB

Uporabniki e-banke uporabljajo za dostop do sistema pametno kartico, na kateri je lahko shranjen ključ. Ključa iz kartice ni mogoče prekopirati. Zasebni ključ je lahko shranjen tudi na računalniku uporabnika v obliki datoteke. Da preprečimo dostop do te datoteke, je ta dodatno zavarovana z geslom. Vendar je priporočljivo, da je zasebni ključ shranjen samo na kartici.
Na pametni kartici je shranjeno tudi digitalno potrdilo (certifikat), ki je zavarovana z osebnim geslom. Tega uporabnik določi in vpiše sam. Kartica se po nekaj poskusih napačne številke samodejno zaklene.

Če se uporabnik odloči za uporabo pametne kartice, mora imeti čitalec kartice in na svojem računalniku nameščeno programsko opremo ActivCard, ki jo je možno prenesti tudi s spletne strani NLB. Večinoma vse slovenske elektronske banke uporabljajo ActivCard čitalce in kartice, razen A banke, ki uporablja Abacom čitalec.

Vsi prenosi podatkov med komitentom in banko so šifrirani, prenašajo pa se preko *https* protokola. Za šifriranje podatkov se uporablja algoritem RC4 z dolžino ključa 128-bitov. Algoritem RSA z dolžino ključa 1024-bitov služi za avtentikacijo in izmenjavo ključev. Podatki med banko in uporabnikom se prenašajo preko protokola SSL, ki kodira podatke.

Slika 4: Oprema ActivCard

Uporaba sistema je preprosta, saj je potrebno v čitalec vstaviti pametno kartico in zagnati internetni brskalnik (Internet Explorer ali Netscape Communicator). Ko je računalnik priklopljen na internet, izberemo naslov bančne spletne strani.

Postopek priklopa je avtomatičen. Na ekranu se pokaže osnovni meni sistema elektronskega bančništva, ki je pripravljen za uporabo.

Primer: Plačevanje naloga prek interneta

1. *Program se poveže z banko;*
2. *Ko se povezava izpostavi, se nam iz bančnega strežnika prikaže seznam podpisnikov podjetja z njihovimi statusi;*
3. *Z dvoklikom izberemo svoje ime. Odpre se okno za vnos enkratnega gesla z ID kartice;*
4. *V vnosna polja vnesemo PIN-kodo in enkratno geslo, ki se pojavi na ID kartici;*
5. *Ko vnesemo zahtevane podatke za avtorizacijo, program preveri, če želimo naloge poslati v plačilo;*
6. *Ko plačilo izvršimo, nam program izpiše zbirno sporočilo o prenosu v banko;*

Elektronska banka Nove kreditne banke Maribor, Bank@Net

V identifikacijski kartici se vsako minuto generira enkratno geslo, ki se ga da uporabiti samo enkrat. Geslo je znano le lastniku in banki. Geslo se prikaže na zaslonu ID kartice, od koder ga uporabnik pred vstopom v e-banko prepiše v določeno polje. Poleg ID kartice dobi uporabnik tudi PIN številko, brez katere je kartica neveljavna.

5.2 Požarni zid

Požarni zid (firewall) omogoča izvajanje omejevanje dostopa med dvema omrežjema. Sloni na uporabi dveh mehanizmov in sicer:

- omejuje promet,
- dovoljuje promet.

Njegov namen je, da zaščiti računalnike in podatke enega omrežja pred zlorabami iz drugega omrežja. Požarni zid z usmerjevalnikom (router) pregleda posamezen paket ter na podlagi vnaprej postavljenih pravil ugotovi ali ga sme poslati na ciljno lokacijo.

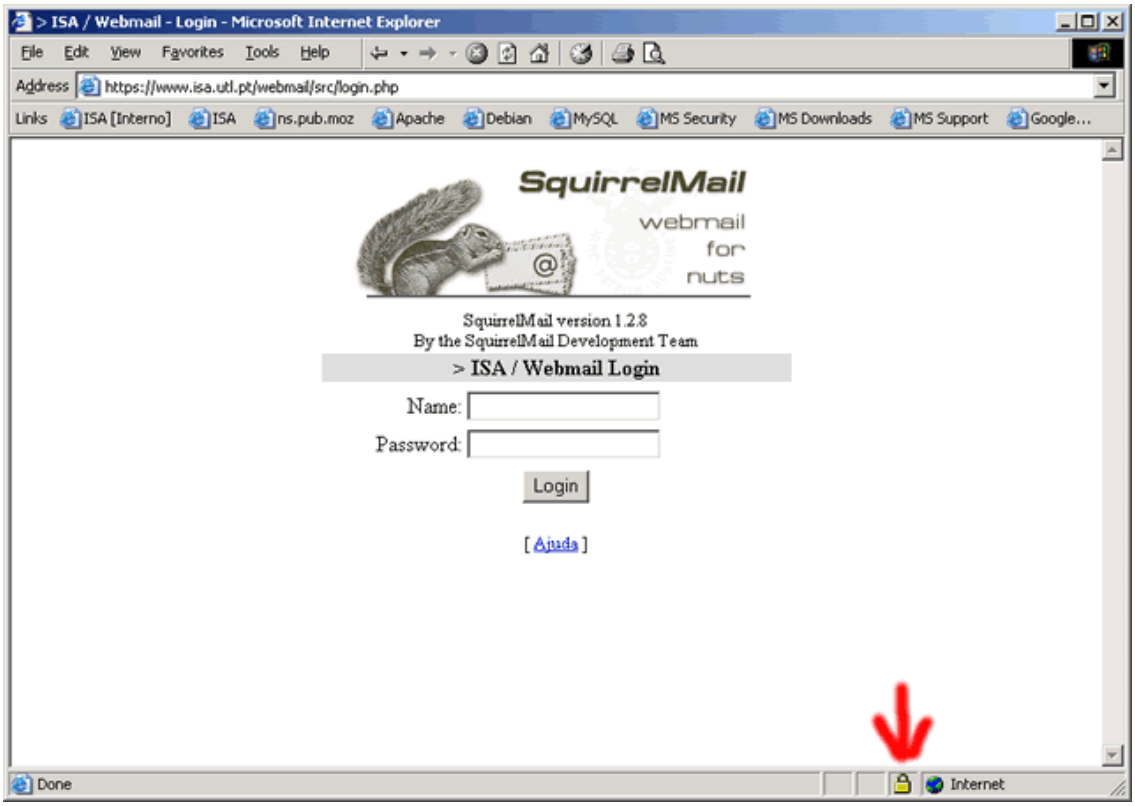
5.3 Varnostni protokol SSL

Banke v elektronskem bančništvu uporabljajo protokol SSL- Secure Socket Layer, ki ga je razvil Netscape. Strežnik (server) in odjemalec (client) vzpostavita povezavo po omrežnem protokolu TCP na običajen način, SSL pa poskrbi za šifriranje izmenjanih sporočil. Uporablja se predvsem za zaščito transakcij v svetovnem spletu. Strežnik preveri identiteto stranke, uporabnik pa se medtem prepriča ali komunicira s pravim bančnim strežnikom. SSL po overjanju zagotavlja varno izmenjavo podatkov, saj šifrira celoten komunikacijski kanal.

Sestavljen je iz dveh slojev. V zgornjem sloju so protokoli, ki se dogovorijo o načinu šifriranja in o izmenjavi simetričnega ključa. V spodnjem sloju pa se izvaja šifriranje podatkov po simetričnem algoritmu. Protokol SSL je torej sestavljen iz dveh delov:

1. *SSL Handshake Protocol* omogoča usklajevanje algoritma, prenos digitalnih certifikatov in določitev skupnega ključa za simetrični kriptoalgoritem.

2. *SSL Record Protocol* definira osnovni format izmenjanih podatkov in zagotavlja neokrnjenost in šifriranje.



Slika 5: Primer SSL - pregledovalnik prikaže zaklenjeno ključavnico

Uporabo protokola SSL v svetovnem spletu spoznamo po predponi *https* v naslovih spletne strani namesto običajnega *http*. Internet Explorer prikaže v statusni vrstici tudi zaklenjeno ključavnico, kar je razvidno s slike 5.

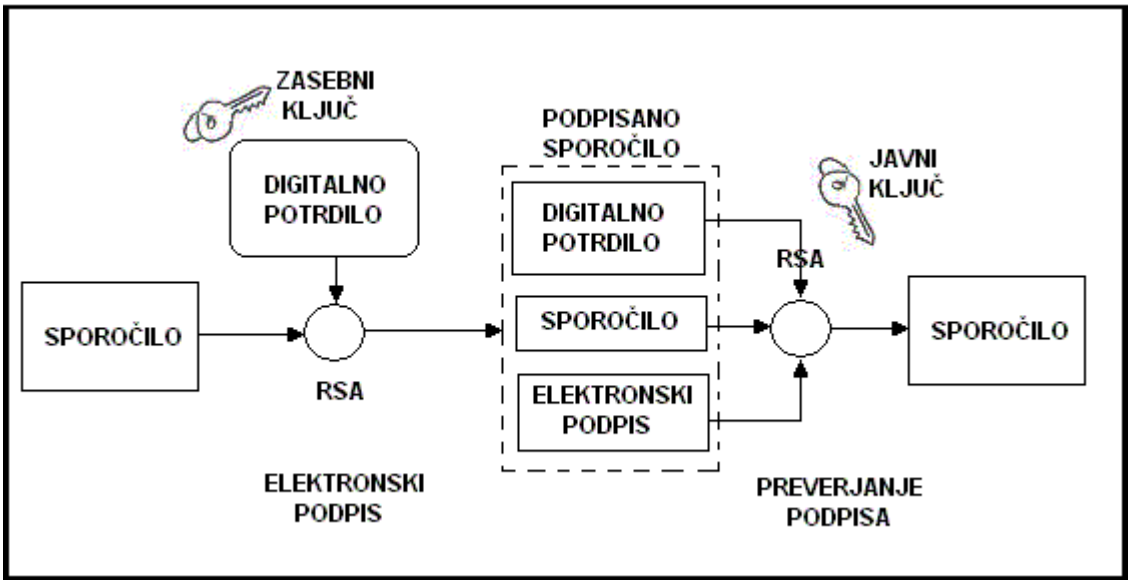
5.4 Elektronski (digitalni) podpis

Varen elektronski podpis je elektronski podpis, ki izpolnjuje naslednje zahteve:

- *Da je povezan izključno s podpisnikom.*
- *Da je iz njega mogoče zanesljivo ugotoviti podpisnika.*
- *Da je ustvarjen s sredstvi za varno elektronsko podpisovanje, ki so izključno pod podpisnikovim nadzorom.*
- *Da je povezan s podatki, na katere se nanaša, tako da je opazna vsaka kasnejša sprememba teh podatkov ali povezave med njimi.*

Varen elektronski podpis, overjen s kvalificiranim potrdilom, je glede podatkov v elektronski obliki enakovreden lastnoročnemu podpisu ter ima zato enako veljavnost in dokazno vrednost. (Slovenski zakon o elektronskem poslovanju in elektronskem podpisu, 15.člen)

Razvil se je zato, da nadomesti lastnoročni podpis uporabnika, torej za identifikacijo uporabnika, in da ohrani varnost pošiljanja sporočil po internetu.



Slika 6: Digitalno podpisovanje sporočila

Torej je elektronski podpis enakovreden lastnoročnemu, in ima prednost v tem, da zagotavlja tako avtorstvo dokumenta kot njegovo neokrnjenost. Uporabnik podpiše dokument tako, da ga najprej zgosti z eno izmed enosmernih zgoščevalnih funkcij v blok konstantne dolžine. Blok nato šifrira s svojim skritim ključem in ga doda originalnemu dokumentu. Nastali šifriran blok imenujemo elektronski podpis CMS (Crypographic Message Syntax). Podpis se lahko preveri z objavljenim javnim ključem.

Obstaja več oblik izdelave digitalnega podpisa, ki jiga vsebuje protokol SSL. Najbolj znani so:

- **Asimetrični algoritem RSA (Rivest-Shamir-Adleman):** ta kriptografski sistem z javnim ključem je poimenovan po začetnicah priimkov avtorjev: Ron Rivest, Adi Shamir, Leonard Adleman. Algoritem temelji na razbitju velikih števil, zato morajo biti ključi tako dolgi, da jih nikakor ne moremo razcepiti na prafaktorje. Poleg izdelave digitalnega podpisa omogoča tudi šifriranje. Ta algoritem nastopa v kombinaciji z enosmernimi zgoščevalnimi funkcijami (MD5, RIPEMD, SHA 1, z DESom). Danes najpogosteje uporabljamo algoritme MD5 (velikost rezultata 128 bitov) in RIPEMD ter SHA 1 (Secure Hash Standard) z velikostjo rezultata 160 bitov.

- **Eliptična krivulja ECDSA**

- **Metoda DSS (Digital Signature Standard)**

- **algoritem PGP** (Pretty Good Privacy): je kombinacija simetričnih kriptografskih sistemov in sistemov z javnim ključem. Uporabniku omogoča

šifriranje in digitalno podpisovanje datotek ter sporočil. Ščiti zasebnost sporočila ali vsebine.

Digitalni podpis je torej pod določenimi pogoji primeren za zaščito pri izmenjavi podatkov. Pomanjkljivost zaščite se pojavi le pri preverjanju podpisov, ker se pri dolgoročnih pogodbah, shranjenih v centrali, podpis nikoli več ne preveri. Digitalen podpis je tako rekoč enakovreden lastnoročnemu.

Varnost je odvisna predvsem od zaščite zasebnega ključa. Če je ta shranjen na disku, obstaja nevarnost, da bo ključ razkrit. Vsaj med uporabo je ključ v nezaščiteni obliki v pomnilniku računalnika. S tem je na voljo različnim trojanskim konjem. Pred nekaj leti, se je pojavil trojanski konj "Lažni podpis", ki je napadal uporabnike elektronskega bančništva. Škodo, ki jo je povzročil trojanski konj, so že občutili uporabniki Klika NLB. Dobili so ga kot priponko v okuženem elektronskem pismu. Škodljiv je postal šele pri zagonu te priponke. Trojanski konj v pregledovalniku opazuje, kaj dela uporabnik, in ko se uporabnik prijavi v storitev elektronskega bančništva, ga zamoti in izvede škodljive akcije. Ob uporabi pametne kartice je napad možen le iz računalnika, na katerega je priključena pametna kartica. Da se zaščitimo pred trojanskimi konji, je priporočljiva uporaba protivirusnih programov.

Da bi bila dosežena še večja varnost in zaščita elektronskega podpisa, bi potrebovali "elektronske" notarje in arhive digitalno podpisanih dokumentov. Dandanes ustanove za overjanje javnih ključev preverjajo le, če so podatki o lastniku javnega ključa pravi in izdajajo digitalna potrdila.

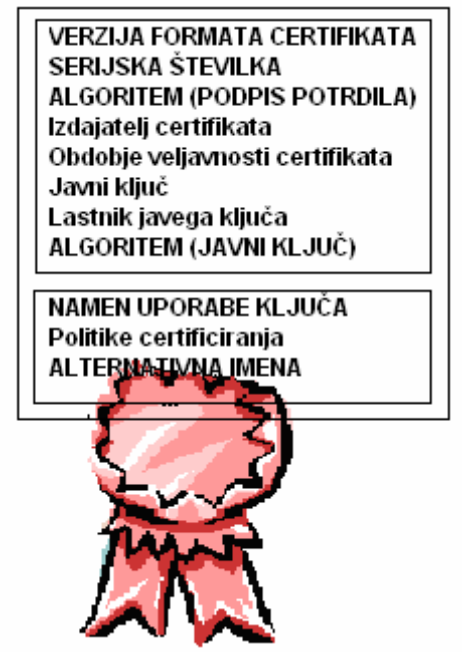
Določanje stopnje varnosti omogočajo standardi, med katerimi so najbolj znani evropski ITSEC (Information Technology Security Evaluation Criteria), ameriški TSEC (Trusted Computing System) in CC (Common Criteria).

5.5 Digitalni certifikat (potrdilo)

Digitalni certifikat (Digital Certificate) imenovan tudi digitalno potrdilo ali digitalni dokument, potrjuje povezavo med javnim ključem in osebo ali strežnikom ali institucijo. Uporablja se za overjanje javnih ključev oz. da ugotovi, ali je javni ključ naslovnika ponaredek. To je temeljni pogoj za uporabo varnostnih mehanizmov, ki temeljijo na asimetrični kriptografiji. Digitalni certifikat vsebuje:

- javni ključ,
- podatke o imetniku (ime, e-naslov, enolična številka…),
- podatki o overitelju oz. izdajatelju digitalnega potrdila,
- obdobje veljavnosti digitalnega potrdila, ki je digitalno podpisan z zasebnim ključem izdajatelja potrdila.

Overitelj javnih ključev (CA-Certification Authority), ki je lahko oddelek, podjetje, združenje ali agencija za certificiranje javnih ključev, preverja certifikate in s svojim podpisom jamči avtentičnost. Dokument (Certification Policy) opisuje postopek, kako in komu overitelj podeljuje digitalna podpisana potrdila, in na kakšen način varuje svoj zasebni ključ. Overitelj mora poskrbeti, da so imetniki potrdil enolično določeni. Potrdila pa lahko izdaja na različnih nivojih zaupanja. S tem potrdilom lastnik dokazuje lastništvo ključa in svojo identiteto.
Problema, ki se lahko pojavita pri uporabi digitalnih certifikatov sta v tem, da je certifikat lahko ponarejen ali pa podpisan brez predhodnega preverjanja avtentičnosti. Da se certifikat podpiše brez predhodnega preverjanja, se lahko doseže z direktnim, hierarhičnim oz. z mrežnim zaupanjem.



Slika 7: Shematski prikaz vsebine digitalnega certifikata

Digitalni certifikat je digitalno podpisan dokument, ki ga podpiše izdajatelj. V njem so naslednji podatki:

- različica zapisa (v1, v2 ali v3),
- enolična številčna oznaka certifikata v okviru izdanih certifikatov posamezne AC (authority certification), na primer zaporedna številka izdanega certifikata,
- informacija o algoritmu, s katerim je bil narejen digitalni podpis certifikata,
- ime izdajatelja certifikata,
- obdobje veljavnosti certifikata,
- ime lastnika javnega ključa,
- javni ključ in informacija o algoritmu, v katerem se ključ uporablja.

6 Vdori v sisteme e-bančništva

Vdorov v sisteme elektronskega bančništva je številčno najmanj, če jih primerjamo z vdori v druge sisteme vendar pa povzročijo največ škode.

Glavni varnostni problemi pri uporabi elektronskega bančništva, ki lahko povzročijo sprožen transfer denarja, razkritje ali ponarejanje zaupne informacije, lažno zanikanje izvedbe plačila, uničenje podatkov, okužbo z virusom, onemogočanje dela itd. so:

- *Elektronsko vohunstvo* (prisluškovanje prenosu podatkov med komitentom in banko).
- *Elektronski vandalizem* (spreminjanje podatkov).
- *Vdor v sistem* (navadno z uporabniškim imenom in geslom enega izmed uporabnikov. Geslo se lahko ukrade tudi s prisluškovanjem uporabnikom. Obstaja tudi možnost, da se program podtakne v sistem, ki poroča nazaj lastniku.).
- *Prestrezanje sporočil in vmešavanje* (načeloma je prek strežnika mogoče prisluškovati vsem sporočilom. Nekdo lahko spremeni vsebino našega sporočila in ga naprej podaja, kot da je prišlo od nas npr. zahtevek za transakcijo denarja. Najbolj znani primeri so kraje številk kreditnih kartic, čeprav so informacije zašifrirane. Kreditne kartice so najbolj problematične, saj je njihovo strukturo možno prestreči. Potujejo namreč preko delov omrežja, ki niso pod nadzorom.).
- *Pretvarjanje* (da se nekdo prek interneta identificira kot uporabnik. Za to zadostuje že številka kreditne kartice.).

Število poskusov, vdorov, goljufij in zlorab se vsako leto povečuje, saj je elektronski denar izredno hiter in nesledljiv. Strežniki večjih bank se dnevno ukvarjajo z napadi hekerjev, ki pa jih največkrat tudi uspešno ustavijo.

6.1 Nezanesljiva strojna oprema

Najpomembnejši del strojne opreme so bančni strežniki in njihovi trdi diski, saj morajo delovati neprekinjeno in brezhibno. Zato je potrebno izdelovati varnostne kopije podatkov, da se v primeru izgube lahko vzpostavi prvotno stanje.

6.2 Virusi

Virusi lahko povzročijo v sistemih bank in podjetij ogromno škodo, saj se hitro širijo in imajo uničujoče posledice. Obstaja ogromno različnih vrst virusov. Nekateri kradejo številke kreditnih kartic, če so shranjene v datoteki, spet drugi bodo prisluškovali početju na računalniku, čakajoč na uporabniška imena in gesla…

Večina ljudi se zaveda tega problema, saj jih ima večina nameščen kakšen program za odkrivanje virusov.

6.3 Lažne banke

Te banke pogosto obstajajo samo na internetu (na domenah majhnih otočkov v samostojnih državicah, s povsem svojo zakonodajo) in z namenom, da se izognejo radovednim državnim organom. Neprevidni poslovneži so na primer nasedli European Union Bank iz Antigue ali Rotschild International Ltd. iz Kajmanskih otokov, ki so kliente ogoljufale za velike vsote denarja, in na hitro poniknile.

7 Zaključek

E-bančništvo mora v grobem zadoščati trem pomembnim funkcijam. Biti mora preprosto, tako da služi tudi ljudem, ki se ne spoznajo na internet in računalnike. Posnemati mora storitve navadne banke ter jih celo izboljšati. In nenazadnje mora biti varno, da ohrani zaščito transakcij in osebnih podatkov.

Slovenija je trenutno nad povprečjem držav Evropske Unije na področju izdaje pametne kartice in digitalnih certifikatov. Večina evropskih držav namreč še vedno uporablja manj zanesljivo tehnologijo z enkratnimi gesli.

V prihodnosti se bo varnost elektronskega poslovanja še povečala, pri čemer bo poudarek pri dostopu uporabnika in identifikaciji. Temeljila bo na biometriki, ki se nanaša na poznavanje in razlikovanje fizičnih karakteristik osebe. Uporabljala se bo tehnologija prepoznavanja obraza, prstnih odtisov ali zenice.

Banka sicer poskrbi za varnostne mehanizme. Še vedno pa se vdori v računalniške sisteme lahko zgodijo zaradi napak samih uporabnikov. Vsak uporabnik bi moral poskrbeti, da ima nameščeno najnovejšo različico protivirusnega programa, geslo oziroma PIN številko pametne kartice ohranjeno v tajnosti, uporabljati pa bi moral najnovejšo različico operacijskega sistema.

8 Viri in literatura

1. Black Uyless: Internet Security Protocols, Protecting IP Traffic. Upper Saddle River, New Yersey, 2000.
2. Elektronsko poslovanje v bankah, ZBS – Združenje bank Slovenije.
3. Idzig Štefan: Projekt varne uporabe interneta v podjetju. Win.ini, Maribor, 8 (1999), št. 7-8. Str. 66-71.
4. Jerman Blažič Borka et al.: Elektronsko poslovanje na internetu. Ljubljana GV založba, 2001. Str. 206.
5. Jerman Blažič Borka, Turk Tomaž: Internet. Ljubljana: Novi forum, 1996. Str. 87.
6. Jurišič Aleksandar, Tonejc Jernej: Pametne kartice in varnost. Monitor, Ljubljana, 11 (2001), št. 6. Str. 66-75.
7. Kovačič Matevž: Storitve elektronskega bančništva. Banke in tveganja. Zbornik III. Strokovnega posvetovanja o bančništvu. Portorož: Zveza ekonomistov Slovenije, 1997. Str. 131-142.
8. Lesjak Igor: E-podpis. Sistem, priloga revije Monitor, Ljubljana 13 (2003), št.10. Str. 12-13.
9. Mele Jaka: Zaščita podatkov na informacijski avtocesti. Moj mikro, Ljubljana, 2004, št.12. Str. 88-91.
10. Navodila za uporabnike Poslovnega Bank@Neta - aplikacije EPP.
11. (Citirano 3.2.2005). Dostopno na internetnem naslovu Nove Ljubljanske banke d.d.. [https://klik.nlb.si/].
12. Risen James: Sept. 11 Hijackers Said to Fake Data on Bank Accounts. New York Times, New York, 10.6.2002. Str.3.
13. (Citirano 16.1.2005). Dostopno na internetni strani Siol novice. [http://www.siol.net/novice/default.asp?page_id=9&article_id=1903071017263668].
14. Trampuš Matej: Zmeda okoli trojanskega konja "Lažni podpis". Moj mikro, Ljubljana, 2002, št.11.

9 Zahvala

Za pomoč pri raziskovalni nalogi se zahvaljujem svoji mentorici Karmen Kotnik ter vsem drugim, ki so mi pomagali pri iskanju virov in literature.