UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

MAGISTRSKO DELO

ANALIZA USTREZNOSTI VARNOSTNIH MEHANIZMOV ZA UVEDBO V OBSTOJEČI INFORMACIJSKI SISTEM BANKE NLB, D.D.

Ljubljana, julij 2012 DAVID ČEBULAR

IZJAVA O AVTORSTVU

Spodaj podpisani David Čebular, študent Ekonomske fakultete Univerze v Ljubljani, izjavljam, da sem avtor magistrskega dela z naslovom ANALIZA USTREZNOSTI VARNOSTNIH MEHANIZMOV ZA UVEDBO V OBSTOJEČI INFORMACIJSKI SISTEM BANKE NLB, D.D., pripravljenega v sodelovanju s svetovalcem dr. Andrejem Kovačičem.

Izrecno izjavljam, da v skladu z določili Zakona o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami) dovolim objavo zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije na fakultetnih spletnih straneh.

S svojim podpisom zagotavljam, da

- je predloženo besedilo rezultat izključno mojega lastnega raziskovalnega dela;
- je predloženo besedilo jezikovno korektno in tehnično pripravljeno v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, kar pomeni, da sem
    - poskrbel, da so dela in mnenja drugih avtorjev oziroma avtoric, ki jih uporabljam v zaključni strokovni nalogi/diplomskem delu/specialističnem delu/magistrskem delu/doktorski disertaciji, citirana oziroma navedena v skladu z Navodili za izdelavo zaključnih nalog Ekonomske fakultete Univerze v Ljubljani, in
    - pridobil vsa dovoljenja za uporabo avtorskih del, ki so v celoti (v pisni ali grafični obliki) uporabljena v tekstu, in sem to v besedilu tudi jasno zapisal;
- se zavedam, da je plagiatorstvo – predstavljanje tujih del (v pisni ali grafični obliki) kot mojih lastnih – kaznivo po Zakonu o avtorskih in sorodnih pravicah (Ur. l. RS, št. 21/1995 s spremembami);
- se zavedam posledic, ki bi jih na osnovi predložene zaključne strokovne naloge/diplomskega dela/specialističnega dela/magistrskega dela/doktorske disertacije dokazano plagiatorstvo lahko predstavljalo za moj status na Ekonomski fakulteti Univerze v Ljubljani v skladu z relevantnim pravilnikom.

V Ljubljani, dne _____ Podpis avtorja:_____

KAZALO

KAZALO SLIK

KAZALO TABEL

UVOD

Internet je prinesel revolucijo že na mnoga področja in kljub temu, da ga poznamo že desetletja, še vedno velja za izredno hitro rastoče področje novih komunikacijskih storitev. Ko je internet dosegel banke, je v ta sektor prinesel nemalo pretresov in sprememb, ki so prinesle drugačen pogled na banke in bančništvo, kot smo ga bili vajeni do sedaj, in postal nepogrešljivo orodje za izvedbo elektronskega bančništva. Elektronsko bančništvo (v nadaljevanju e-bančništvo) se ni rodilo z razmahom interneta, saj smo že pred njim poslovali z bankomati in preko telefona, kar tudi sodi v kategorijo e-bančništva. Seveda pa se je internet izkazal kot idealen distribucijski kanal ali sredstvo komuniciranja med komitentom in banko. Tako so se pojavile prve rešitve elektronskega bančništva, ki potekajo preko interneta s pomočjo osebnega računalnika.

Velik napredek v informacijski tehnologiji nenehno spreminja način poslovanja med bankami in njihovimi strankami in nikjer ni to bolj očitno kot pri uporabi interneta kot sredstva za e-bančništvo in elektronsko poslovanje (Groznik, Trkman & Lindič, 2009, str. 60). Do sedaj je še vsako leto prineslo bistvene spremembe v svet e-bančništva in ponudilo številne nove storitve. Ko govorimo o e-bančništvu, ne moremo mimo varnosti in ranljivosti takega načina poslovanja. Seveda pa je tu poudarek na varnosti informacijskih tehnologij, ki omogočajo e-bančništvo. Elektronsko bančništvo na daljavo je ena najprivlačnejših tarč za internetne kriminalce, zato je potrebno zagotoviti cenovno učinkovite in delujoče varnostne rešitve za avtentikacijo uporabnikov ob vstopu v storitev ter verifikacijo vsebine transakcij, ki jih uporabniki izvajajo. Zaradi povezanosti sistemov lahko en sam vdor v bančni sistem pusti hude ali celo nepopravljive posledice. Zato se temu vprašanju upravičeno posveča velika pozornost.

Nova Ljubljanska banka je že vseskozi vodilna na področju nudenja storitev preko varnih elektronskih poti. Je ena izmed regijskih bank, ki je med prvimi omogočila spletno bančništvo tako podjetjem kot prebivalcem. NLB Mobo, prvo mobilno banko, je predstavila že leta 2002. Kljub temu, da je bila NLB Moba za tisti čas inovativna in tehnično napredna, pa je imela zaradi takratne tehnologije omejitve predvsem na področju funkcionalnosti (ComTrade, 2011).

Dinamičen in inovativen razvoj tehnologij, množica uporabniških naprav ter nove zahteve uporabnikov so narekovali nov korak v razvoju modernih bančnih storitev in nadgradnjo obstoječih. NLB je tako s svojim tehnološkim partnerjem, podjetjem, specializiranim za e-bančništvo, prenovila obstoječo spletno banko NLB Klik in jo nadgradila z možnostjo uporabe na mobilnem telefonu.

Ključna gradnika varnosti v NLB Kliku ostajata vzajemna avtentikacija strežnika in odjemalca s kvalificiranimi digitalnimi potrdili infrastrukture javnih ključev (angl. *Public Key Infrastructure* – PKI) ter šifriranje prenosa podatkov po standardu TLS (angl.

Transport Layer Security). TLS je standardizirana različica protokola SSL (angl. *Secure Socket Layer*).
K varnosti dodatno prispevajo:

- osebno statično geslo za dodatno avtentikacijo uporabnika ob vstopu v NLB Klik;
- osebno sporočilo uporabnika za dodatno avtentikacijo na vstopni strani NLB Klik;
- dodatno varnostno geslo za dodatno avtentikacijo uporabnika pri plačilih na nove račune in pri nekaterih drugih storitvah, kjer obstaja povečano tveganje zlorabe;
- nove varnostne možnosti – SMS sporočila in limiti porabe sredstev prek NLB Klika.

Rešitev je bila zasnovana ob upoštevanju dobrih praks za varnost spletnih aplikacij in neodvisno varnostno pregledana. Kljub varnostnim izboljšavam morajo uporabniki odgovorno skrbeti za varnost svojega računalnika v skladu z navodili, ki jih banka objavlja na spletnih straneh. Priporočljivo je, da uporabniki hranijo zasebne ključe svojega kvalificiranega digitalnega potrdila na PKI pametni kartici, PKI USB ključu ali podobni napravi, ki ustreza standardoma PKCS#11 in FIPS 140-2, raven 2 ali višji (Cryptographic Services, 2012).

Po zaključku prenove spletne banke Klik so se odgovorni za varnost v e-bančništvu odločili prenoviti tudi obstoječo infrastrukturo javnih ključev PKI, ki omogoča izdajanje digitalnih potrdil. Namreč v okviru banke NLB, d. d., deluje agencija za izdajo kvalificiranih digitalnih potrdil AC NLB. Agencija je registriran overitelj kvalificiranih digitalnih potrdil (certifikatov), vpisana v register overiteljev, njeno delovanje pa je skladno z Zakonom o elektronskem poslovanju in elektronskem podpisu. Glavna odgovornost overitelja kvalificiranih digitalnih potrdil je potrjevanje istovetnosti uporabnikov, kar je podobno izdajanju potnih listin ali osebnih izkaznic, le da digitalno potrdilo v papirni obliki ne obstaja.

S prenovo spletnega bančništva in agencije AC NLB pa banka še zdaleč ni naredila dovolj, da bi se zaščitila pred vsemi možnimi zlorabami in napadi na e-bančništvo. Integrirani varnostni mehanizmi še vedno ne preprečujejo udorov, kot so t. i. MiTM (angl. *Man in the Middle*) in MiTB (angl. *Man in the Browser*). Do zlorabe omenjenega varnostnega sistema pride lahko tudi v primeru izgube oz. kraje digitalnega potrdila. Zastavi se nam novo vprašanje o obstoju naprednejših tehnologij za zaščito pred vdori v e-bančništvo. Raziskovalci na Univerzi v Cambridgeu so nedavno ugotovili in tudi dokazali, da omenjene vdore in zlorabe v e-bančništvu do sedaj najbolje preprečujejo tehnologije, ki omogočajo potrjevanje transakcij po ločenem neodvisnem kanalu, ki ga napadalec ne more nadzorovati (Nordfjell, 2011). Sem sodijo potrditvena SMS sporočila, klic na znano telefonsko številko ... Vse bolj pogosto se banke odločajo za implementacijo varnostnih sistemov, katere predstavlja kombinacija uporabe novih EMV (angl. *Europay MasterCard and VISA*), CAP (angl. *Chip Authentication Program*) čip kartic in kartičnih čitalcev s funkcijo generiranja enkratnih gesel.

Še korak naprej v uspešnosti preprečevanja zlorab in vdorov pa je t. i. arhitektura JXCS. Arhitektura JXCS je bila predstavljena na zadnjem World computer Congress - Toulouse v Franciji. Omenjena arhitektura temelji na priporočilih svetovnega spletnega konzorcija (angl. *World Wide Web Consortium - W3C*) in standardih XMLDsig/XadES. Standarda opredeljujeta podpisovanje XML (angl. *Extensible Markup Language*) dokumentov z osebnim digitalnim potrdilom. Lahko rečemo, da je arhitektura JXCS tudi nadgradnja že prej omenjene infrastrukture javnih ključev PKI. Vsak dodatni varnostni ukrep v e-bančništvu ali v e-poslovanju pa zmanjšuje enostavnost uporabe sistema. Če je teh ukrepov preveč, je lahko to moteče za redno delo, prav tako pa z naraščanjem števila varnostnih ukrepov narašča kompleksnost sistema. Tako se poveča stopnja težavnosti za uporabnike in tudi za administratorje sistema. Po drugi strani pa je sistem brez varnostnih mehanizmov preveč ranljiv za vdore in druge zlorabe.

Namen magistrskega dela je izvesti študijo primera, izbire ustreznega varnostnega mehanizma e-bančništva v NLB, d. d. Z drugimi besedami, skušal bom poiskati optimalno ravnovesje med varnostjo, uporabnostjo, ceno in enostavnostjo vzdrževanja varnostnega mehanizma.

Cilj magistrskega dela je ugotoviti in argumentirati primernost varnostnih mehanizmov za implementacijo v informacijski sistem banke NLB, d. d.. Zaradi širokega spektra področij in tehnologij se bom osredotočil predvsem na varovanje e-bančništva fizičnih oseb (Klik). Sem sodi prenovljeni sistem infrastrukture javnih ključev PKI in ostali manj kompleksni sistemi, ki dopolnjujejo osrednji varnostni mehanizem. Ovrednotiti bom poskušal možnost nadgradnje PKI infrastrukture z XML podpisovanjem ter vpeljavo EMV kartic, za kar se je odločila največja banka skandinavskih držav z 11 milijoni komitentov fizičnih oseb in 700.000 komitentov pravnih oseb, Nordea Bank. Velika omejitev pri izbiri varnostnih mehanizmov so seveda tudi razpoložljiva finančna sredstva. Poleg same ustreznosti mehanizma in finančnih zmožnosti banke pa na izbiro varnostnega mehanizma vpliva tudi zakonodaja. Na ravni države je v Sloveniji v veljavi zakon o elektronskem poslovanju in elektronskem podpisu ZEPEP. ZEPEP ureja elektronsko poslovanje, ki zajema poslovanje v elektronski obliki z uporabo informacijske in komunikacijske tehnologije in uporabo elektronskega podpisa v pravnem prometu, kar vključuje tudi elektronsko poslovanje v bančnih, sodnih, upravnih in drugih podobnih postopkih. Cilj naloge je tudi, na podlagi regulativ v ostalih bolj razvitih evropskih državah, ugotoviti trend razvoja zakonodaje in argumentirati izbiro varnostnega mehanizma tudi s tega stališča.

V prvem delu magistrskega dela bo zajet poglobljen teoretično-analitični pregled strokovne literature, znanstvenih raziskav ter člankov domačih in tujih strokovnjakov, ki so gonilna sila razvoja v visokotehnoloških podjetjih s področja obravnavane teme. Poleg kritične analize strokovnoteoretičnih dognanj bodo zaradi lažjega razumevanja za ilustracijo navedeni tudi nekateri praktični primeri iz strokovne literature. Ta del magistrskega dela bo analiziran s pomočjo opisne metode, s katero bom združil spoznanja mnogih avtorjev,

predvsem s področja varnosti v e-bančništvu in elektronskem poslovanju nasploh. Drugi del magistrskega dela bo vseboval poglobljeno tehnološko predstavitev sistema infrastrukture javnih ključev, EMV CAP tehnologije ter XML podpisa s kvalificiranim digitalnim potrdilom. Na podlagi izkušenj bank uporabnic teh sistemov bom skušal ugotoviti stopnjo ranljivosti sistemov. V tretjem delu bom za lažjo predstavo na kratko predstavil arhitekturo informacijskega sistema NLB ter v njej skušal pozicionirati e-bančništvo in pripadajoči varnostni sistem. Skušal bom analizirati obstoječe stanje na področju varnosti e-bančništva NLB in s pomočjo analize SWOT predstaviti prednosti in slabosti obstoječega varnostnega mehanizma. V nadaljevanju magistrske naloge bom ugotovitve iz prvih dveh delov apliciral na primeru izbire varnostnega mehanizma v NLB, d. d.. S tehničnimi in ekonomskimi dognanji bom podkrepil izbiro varnostnega mehanizma, če bo analiza pokazala, da je to sploh potrebno, saj NLB, d. d., že ima implementirano in prenovljeno infrastrukturo javnih ključev. Pri izdelavi magistrskega dela bom uporabil tudi teoretična znanja, pridobljena v okviru podiplomskega študija, in znanje, ki sem ga pridobil iz praktičnih izkušenj kot sistemski inženir, zaposlen v oddelku za omrežja v NLB, d. d..

1 ELEKTRONSKO BANČNIŠTVO

V strokovni literaturi še ni zaznati enotne celovite opredelitve ali definicije elektronskega bančništva. Vendar se na splošno kažeta dve opredelitvi, in sicer ga nekateri poskušajo opredeliti po vrstah storitev, ki nam jih nudijo, drugi pa po lastnostih oziroma kriterijih, ki jim morajo zadoščati (Kovačič, 1998, str. 131).

Poskušajmo najprej opredeliti elektronsko bančništvo z vidika storitev, ki naj bi jih lahko opravljali preko elektronskega bančništva. Elektronsko bančništvo naj bi po tej opredelitvi omogočalo opravljanje osnovnih informacijskih in transakcijskih storitev, pri čemer bi te osnovne storitve opravljal komitent sam od doma ali od koder koli, kjer je možen dostop do interneta. Zahtevnejše oziroma nevsakdanje storitve pa naj bi še vedno opravljali na bančnih okencih. Med informacijske storitve, ki naj bi jih lahko po tej opredelitvi opravljali peko elektronskega bančništva, sodijo informacije o:

- stanjih in transakcijah na računih,
- dogajanjih na kapitalskih trgih,
- obrestnih merah,
- pogojih za pridobitev posojil,
- potrebni dokumentaciji za odobritev posojila ipd.

Med transakcijske storitve, ki naj bi jih lahko po tej opredelitvi opravljali preko elektronskega bančništva, štejemo vse storitve, ki vključujejo plačilne instrumente. Le-te lahko v grobem razdelimo v tri skupine, in sicer elektronski denar, sistemi, ki zahtevajo vodenje računov, in storitve plačevanja s plačilnimi karticami (Hernaus, 1997, 143).

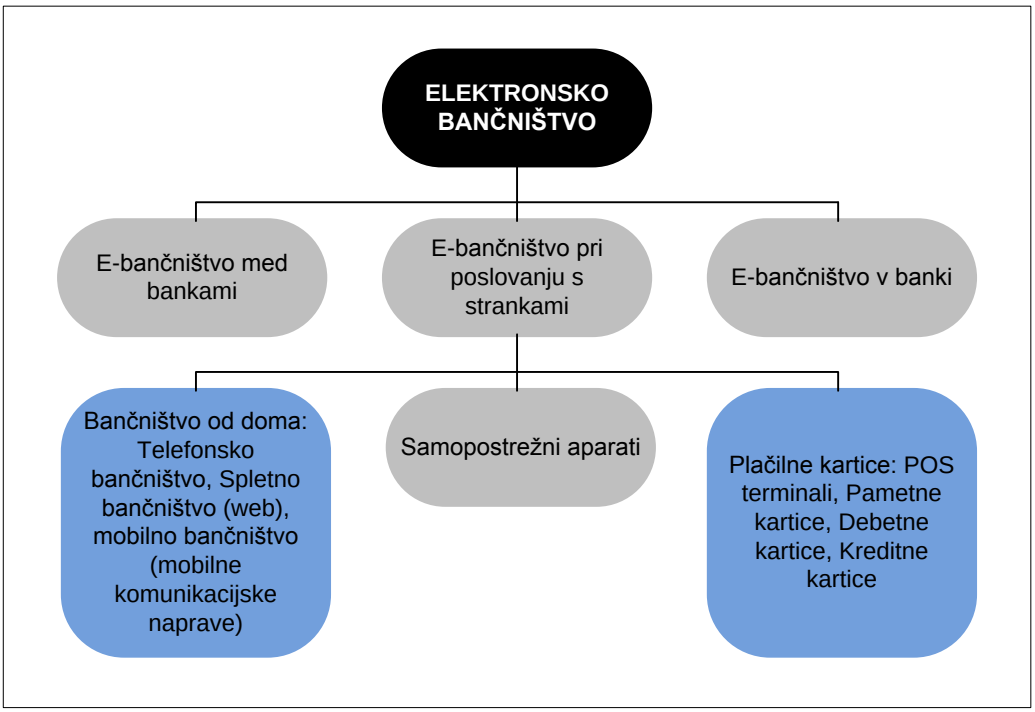
Če opredelimo elektronsko bančništvo z vidika lastnosti storitev, ki zadostijo pomenu elektronsko bančništvo, morajo storitve po Kovačiču (1998, 131) imeti naslednje lastnosti:

- dosegljivost 24 ur na dan, 7 dni v tednu,
- dosegljive morajo biti od koder koli,
- popolna avtomatizacija nudenja storitev in
- opravljene morajo biti varno.

1.1 Oblike elektronskega bančništva

Elektronsko bančništvo med bankami se razvija že zelo dolgo, pri čemer so na tem področju dosegli velike uspehe predvsem pri standardizaciji tehničnih rešitev in medsebojnem povezovanju. Vrhunec tega predstavlja uveljavitev mednarodnega informacijskega sistema za izvajanje plačilnega prometa SWIFT. (angl. *Society to Worldwide Interbank Financial Transaction*), brez katerega si mednarodnega poslovanja ni več mogoče zamišljati. Elektronsko bančništvo znotraj banke je prepuščeno vsaki banki zase. Večino napora banke vlagajo v razvoj aplikacij, ki bi avtomatizirale posamezne rutinske procese in tako zmanjšale stroške. Slika 1 prikazuje oblike elektronskega bančništva in nadaljnjo delitev e-bančništva pri poslovanju s strankami (SWIFT, 2012).

Slika 1: Oblike elektronskega bančništva



Vir: M. Svojšak, Elektronsko bančništvo, 1999.

Elektronsko bančništvo pri poslovanju s strankami pa lahko opredelimo kot kakršenkoli način poslovanja stranke z banko, ki je neodvisen od poslovalnic bank in temelji na informacijski tehnologiji in elektronskih medijih. Ob hitrem napredku interneta in

tehnologiji za varno poslovanje je večina bank vpeljala sisteme za poslovanje na daljavo. Plačevanje položnic se s tem ni spremenilo v užitek, je pa postalo vsaj malce bolj znosno (Gabrijelčič, 2006).

1.2 Storitve elektronskega bančništva

Storitve elektronskega bančništva so popolnoma avtomatizirane in dosegljive 24 ur na dan in vse dni v tednu. Preko sistemov elektronskega bančništva lahko banke ponudijo številne storitve, ki so uporabnikom na voljo preko različnih komunikacijskih naprav. Pomembno je predvsem to, da je opravljanje storitev varno. Za ustrezno zaščito mora poskrbeti banka.

1.2.1 Bankomati

Bankomat je računalniška telekomunikacijska naprava, ki omogoča komitentu finančne institucije dostop do finančnih transakcij v javnem prostoru brez prisotnosti bančnega uslužbenca. Na novejših bankomatih se komitent identificira s plačilno kartico in osebno identifikacijsko številko (angl. *Personal identification number – PIN*). Bankomati v Sloveniji omogočajo komitentom opravljanje naslednjih storitev (Bankomati, 2011):

- avtomatski polog gotovine,
- naročilo za polog gotovine,
- elektronsko plačilo posebnih položnic,
- naročilo za plačilo posebnih položnic,
- hitri dvig gotovine,
- dvig zneska po izbiri,
- vpogled v stanje,
- sprememba identifikacijskih številk,
- nakup GSM kartic in
- vpogled v stanje na kreditnih karticah.

1.2.2 Kartično poslovanje

Plačevanje s plačilnimi karticami je čedalje pogostejši način plačevanja blaga in storitev tako doma kot v tujini. Prednost poslovanja s karticami je v tem, da nam omogočajo poslovanje brez gotovine ali zamudnega pisanja čekov. Plačilne kartice sodijo med elektronske plačilne instrumente, kjer je mogoče plačilo opraviti le s pomočjo elektronskih terminalov, preko katerih se nalog za plačilo v elektronskem omrežju posreduje do banke, pri kateri ima imetnik plačilne kartice deponirana sredstva. Tako banka na podlagi prejetega zahtevka izvede plačilo na ciljni račun. S plačilnimi karticami lahko dvigujemo gotovino na bankomatih in plačujemo storitve ali izdelke, ki jih kupujemo preko spleta (NLB, 2012).

Imetniki lahko izbirajo med:

- **debetno kartico**, kjer ob vsakem opravljenem plačilu banka imetniku sproti bremeni račun,
- **kartico z odloženim plačilom ali kreditno kartico**, kjer nastale obveznosti imetnik poravna enkrat mesečno v celoti (Activa, Visa, Karanta, Eurocard, Diners Club ...) in
- **posojilno kartico**, kjer del porabljenega zneska imetnik poravna mesečno, preostanek dolga pa se obrestuje in se odplačuje v več obrokih (posojilna Visa).

Kartica s takojšnjim plačilom je kartica BA in Maestro, pri kateri izdatki sproti bremenijo imetnikov osebni račun tako kot ob plačilu s čekom ali dvigu gotovine pri bankomatih. Kartice z odloženim plačilom so Karanta, MasterCard, Visa, Visa-Electron, Eurocard itd. Odloženo plačilo pomeni, da izdajatelj kartice imetniku kreditira nakup, enkrat mesečno pa se ta dolg poravna. Posojilne kartice omogočajo delno poravnavanje mesečnih obveznosti. Vsak mesec se tako poplača le določen odstotek skupnega zneska porabe na posojilni kartici.

1.2.3 Telefonsko bančništvo

Telefonsko bančništvo je poslovanje komitenta z njegovo banko preko telefona. Telefonsko bančništvo ima različne pojavne oblike. Najbolj enostavna oblika telefonskega bančništva je avtomatski odzivnik. Zaradi zagotavljanja varnosti moramo pred opravljanjem transakcij sporočiti bodisi številčno bodisi glasovno geslo. Storitve, ki jih nudi telefonsko bančništvo, so odvisne od banke.
Običajne storitve so (NLB, 2012):

- informacije o bančni mreži in vseh storitvah,
- informacije o stanju in prometu na bančnem računu,
- vloga za otvoritev/spremembo limita,
- blokacije bančnih kartic in čekov,
- otvoritev/sprememba/ukinitev trajnega naloga,
- naročanje čekovnih blanketov na naslov,
- naročilo potovalnih čekov,
- naročilo dviga gotovine,
- zamenjava valut v okviru osebnega računa,
- naročilo pošiljanja promocijskega gradiva,
- vezava depozita v domači in tuji valuti,
- prenos sredstev na bančne račune,
- nakazilo sredstev na naslov,
- plačilo položnic in računov, tudi z valuto vnaprej,
- telefonsko nakazilo,
- nakazilo prek Western Uniona,
- naročilo za uporabo avtomatskegaodzivnika,
- naročilo potrdil.

1.2.4 Spletno bančništvo

Internet oz. splet (tudi medmrežje, skrajšano iz angleške besede *inter-network*) je v splošnem smislu računalniško omrežje, ki povezuje več omrežij. Sistem uporablja način paketno preklopljivih komunikacijskih protokolov TCP/IP. Kot lastno ime je Internet javno razpoložljiv mednarodno povezan sistem računalnikov skupaj z informacijami in storitvami za uporabnike. Spretnost povezovanja omrežij na ta način se imenuje internetno delovanje. V razširjenem izražanju se *internet* velikokrat nanaša na storitve, kot so svetovni splet (WWW), elektronska pošta in neposredni klepet (angl. *online chat)* (Online banking, 2011). Ena iz med storitev svetovnega spleta pa je tudi spletno bančništvo.

Spletno bančništvo oziroma opravljanje bančnih storitev preko računalnika (brskalnika) ali mobilnega telefona ter interneta se je uveljavilo predvsem zaradi dveh razlogov:

- Banke so na ta način želele zmanjšati vrste, znižati stroške in množične vsakdanje posle prenesti iz poslovalnic (tako da so se bančni uslužbenci lahko bolj posvetili svetovanju strankam in zahtevnejšim storitvam).
- Banke so morale oziroma želele ugoditi strankam, ki so izrazile željo po takšni vrsti poslovanja.

Prednosti, ki jih spletno bančništvo prinaša bankam, so večja varnost in zasebnost, večja hitrost, obseg prenosa podatkov ipd. Storitve, ki jih lahko opravljamo preko elektronskega bančništva, so vpogled v stanje na računih, prenos med bančnimi računi, plačevanje računov, sklenitev in prekinitev varčevanja, naročila za kartice, kredite ipd.

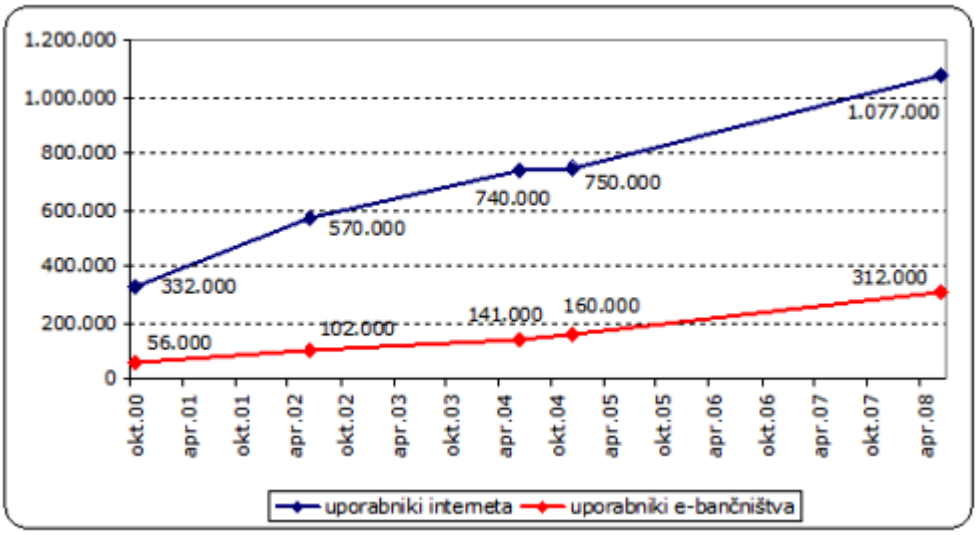
1.3 Razvoj elektronskega bančništva v Sloveniji

Po raziskavah RIS, ki so bile narejene v letu 2010, je slabe tri četrtine (74 %) uporabnikov interneta rednih, torej takšnih, ki so internet uporabljali v zadnjih 3 mesecih, dobre štiri petine (81 %) internet uporablja vsak dan ali skoraj vsak dan. Precej podoben pa je tudi delež rabe e-bančnih storitev.

E-bančništvo se je v zadnjem desetletju izkazalo za eno najbolj dobičkonosnih spletnih storitev. Glede na vedno večjo ponudbo storitev preko spleta je za ponudnike ključnega pomena pridobitev kakovostne splošne slike o panogi. Glavni dejavniki, ki vplivajo na uporabo (in raven uporabe) e-bančništva po podatkih RIS, so predvsem skrb za varnost oz. zasebnost, finančna tveganja, način dojemanja prednosti, uporabnosti storitve ter odnos do spletnih storitev nasploh. Ponudba e-bančništva bo v prihodnje eden izmed ključnih momentov pri odločanju za izbiro banke, spletne storitve bodo postale ključni faktor pri ohranjanju oz. pridobivanju ali izgubi tržnega deleža med komitenti. Slika 2 prikazuje, kako z naraščanjem števila uporabnikov interneta raste tudi število uporabnikov e-bančništva. Graf prikazuje rast števila uporabnikov interneta in e-bančništva od leta 2000

do leta 2008. Opazimo pa lahko tudi malenkostno hitrejšo rast števila uporabnikov interneta od rasti uporabnikov e-bančništva.

Slika 2: Rast uporabnikov interneta in e-bančništva v preteklem desetletju v Sloveniji



Vir: RIS, Raba interneta v Sloveniji, 2011.

Leta 2004 je RIS napovedal letno rast uporabnikov e-bančništva za 15 %, kar v absolutnem pomeni letno rast v povprečju za 20.000 uporabnikov. Napovedi so se v celoti uresničile, vendar pa se za prihodnja leta kaže počasnejši trend rasti. Ob sedanjem trendu rasti za EU15 oz. EU27 lahko v EU do leta 2020 v povprečju pričakujemo današnjo raven skandinavskih držav (okoli 60 ali 70 % uporabnikov e-bančništva v populaciji 16–75 let). Ob sedanjem trendu rasti v Sloveniji pa lahko takšno raven v Sloveniji pričakujemo šele do leta 2035. Slovenija s trenutnimi trendi ne zmanjšuje razkoraka za razvitejšimi evropskimi državami. Banke bodo morale v prihodnjih letih oblikovati ponudbo, ki bo zadržala obstoječe uporabnike ter privabila nove. Kakšna so gibanja na strani ponudbe (tržni deleži, število in razporeditev ponudnikov) in povpraševanja – npr. kdo so (ne)uporabniki, zadovoljstvo in lojalnost komitentov – bodo za obstoječe in nove ponudnike ključna vprašanja v naslednjih nekaj letih intenzivne ekspanzije.

2 VARNOST V ELEKTRONSKEM BANČNIŠTVU

Bankam internet predstavlja vrata do milijonov potencialnih strank. Selitev bančnega poslovanja iz poslovalnic na internet predstavlja komitentom lažji in udobnejši dostop do banke, za banke pa ogromen prihranek. Sodobni bančni kanali zagotovo večajo zadovoljstvo uporabnikov in omogočajo banki hitrejšo in cenejšo rast, pomenijo pa tudi potencialno veliko varnostno tveganje in neosebno obravnavanje bančnih komitentov. Ko so banke omogočile partnerjem in strankam poslovanje preko interneta, je postala varnost nujnost. Pri poslovanju z bankami prihaja do prenosa občutljivih informacij, kot so denarne

transakcije, podatki o računih, osebni podatki o komitentih itd. Da do sodelovanja sploh pride, si morajo banke pridobiti zaupanje partnerjev, komitentov in to zaupanje tudi vzdrževati. V današnjem okolju, kjer so kraje identitet in udori v poslovne informacijske sisteme zelo pogosti, je nujno, da podjetja, predvsem pa banke, zagotavljajo varno izvajanje spletnih transakcij. S takim načinom si banke ne le pridobijo zaupanje komitentov, temveč z dodajanjem novih storitev na splet povečajo tudi dobiček. Banka pa tako postane tudi odgovorna za to, da so ogromne količine občutljivih podatkov varne pred vdori in zlorabo (Securing Digital Identities & Information, 2011).

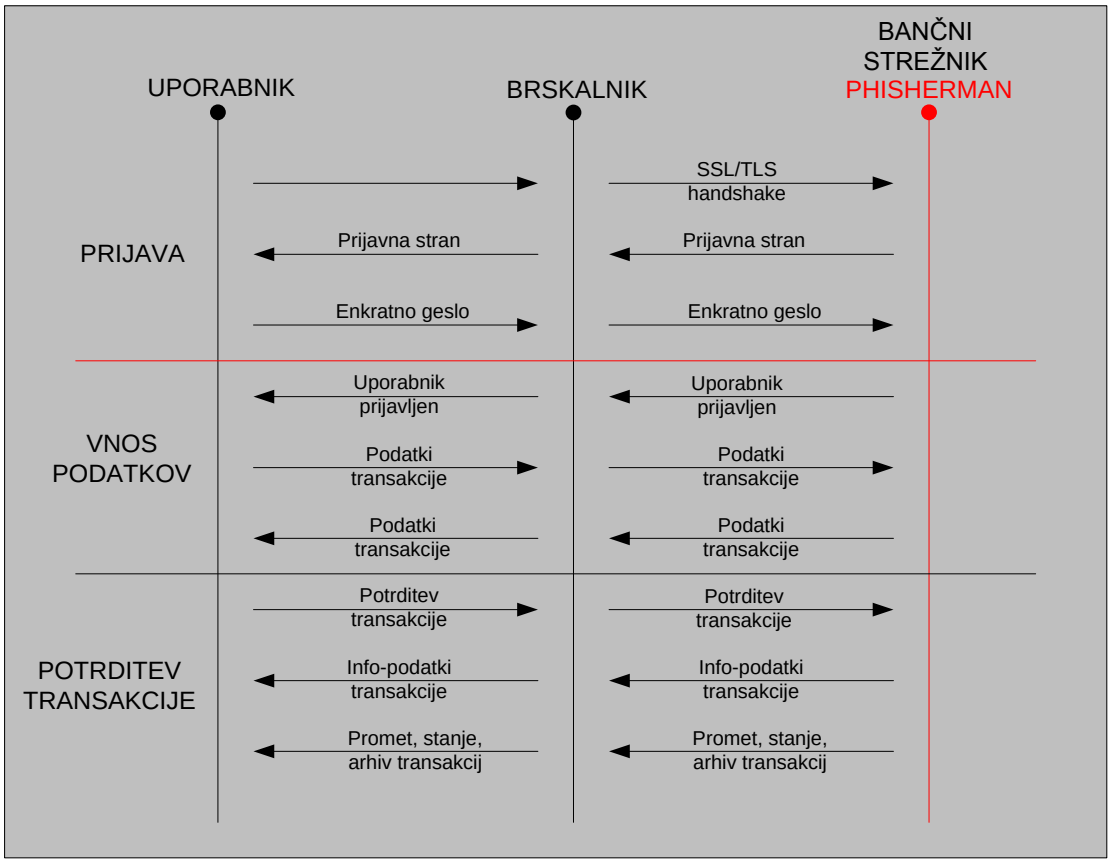
2.1 Grožnje in zlorabe v elektronskem bančništvu

Poleg vseh prednosti, ki jih prinaša elektronsko bančništvo, je z vse večjo uporabo prišlo tudi do porasta zlorab. Gre za novejšo obliko organiziranega kriminala, proti kateremu pa nismo nemočni. Če želimo povečati zanesljivost preprečevanja zlorab, se moramo osredotočiti na varovanje transakcij in ne zgolj na varovanje uporabnikove prijave v storitev. Pri tem pa se ne smemo zanašati na varnost uporabnikovega računalnika. Potem ko smo se uporabniki le zavedeli, da moramo varovati svoja gesla in digitalna potrdila (certifikate) ter paziti na lažne spletne strani, prek katerih zlikovci ribarijo dragocene podatke (angl. *phishing*), so se začeli pojavljati novi načini napadov. Zdaj se skušajo goljufi in tatovi vriniti kar v komunikacijski kanal med uporabnikom e-banke in bančnim strežnikom ter spreminjati podatke o transakcijah. Obramba pred tovrstnimi napadi obstaja, toda tako uporabniki kot banke bodo morali biti v prihodnje še bolj pozorni in ažurni (Bric, 2010).

2.1.1 Ribarjenje (Phishing)

Najobičajnejša metoda je ribarjenje gesel z lažnimi spletnimi stranmi. O tem je bilo že veliko zapisanega, spomnimo se, kako je naša največja banka obveščala o pojavu lažnih strani. Metoda napada je proces identifikacije uporabnika – pridobivanje gesel in digitalnih potrdil. Podobno delujejo tudi programi za beleženje tipk (angl. *keylogger*), ki pridobljene podatke takoj pošiljajo v sistem neposrednega sporočanja. Hekerska infrastruktura je močno razvita, tako da kriminalec pravočasno pridobi potrebne podatke. Nato se prijavi kot uporabnik in če ni dodatnih varnostnih mehanizmov pri potrjevanju transakcije, lahko počne, kar se mu zljubi. Pozoren uporabnik bo prepoznal lažno stran, ne bo brez razmišljanja kliknil vsako zahtevo, ki se prikaže na zaslonu, in če bo njegov računalnik dovolj varovan pred okužbami, lahko sam največ stori za svojo varnost (Vodopivec, 2010). Slika 3 prikazuje potek vdora s pomočjo ribarjenja. Rdeča vertikalna črta predstavlja bančni strežnik in obenem mesto, kjer je nameščena lažna aplikacija oz. ribič, ki lovi občutljive podatke.

Slika 3: Potek vdora Ribarjenje »Phishing«

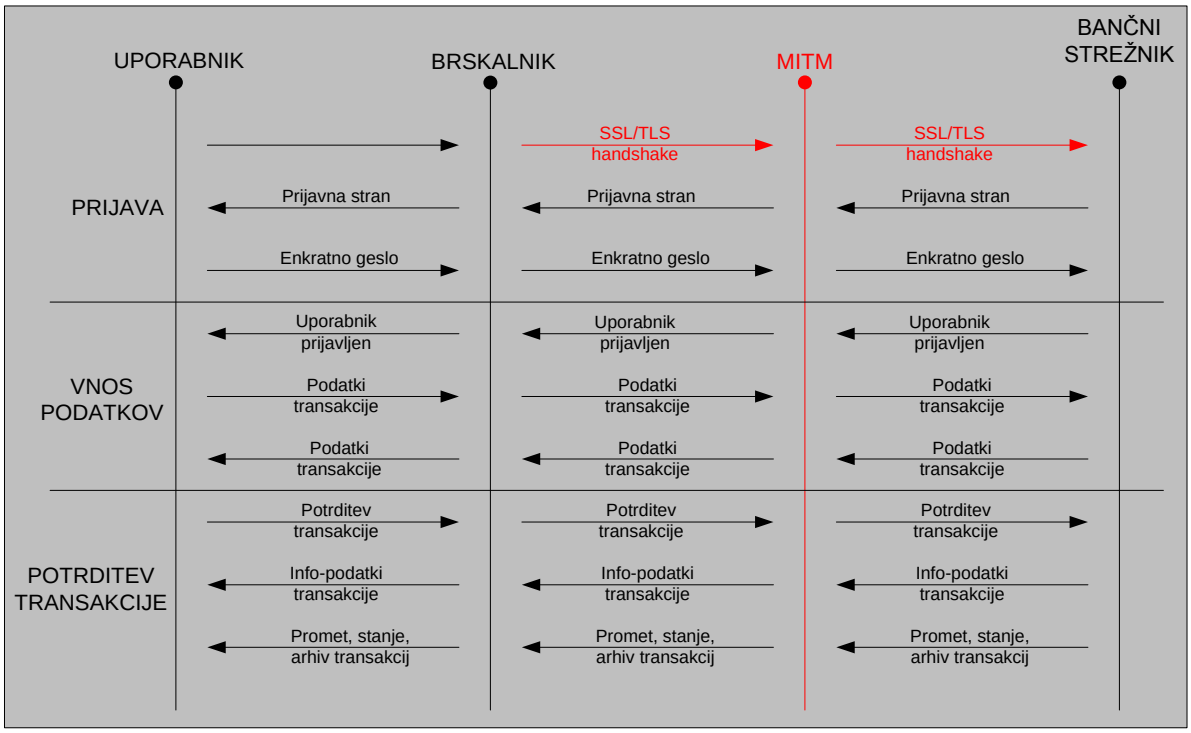


Vir: T. Vodopivec, Kdo se boji črnega moža, 2010.

2.1.2 Mož v sredini (MiTM)

Napad »mož v sredini« (angl. *Man in the middle* – MiTM) je metoda, kjer se napadalec vrine v komunikacijski kanal na sredini in ne samo, da nadzira komunikacijo, ampak jo tudi prilagaja. Na primer: pošiljatelj pošlje črko A, sprejme jo napadalec, doda črko B in niz AB pošlje naprej. Ne uporabnik ne prejemnik ne vesta, da je bilo sporočilo spremenjeno. Pošiljatelj misli, da je prejemnik dobil črko A, prejemnik pa, da mu je pošiljatelj poslal niz AB. S spreminjanjem podatkov transakcije lahko napadalec poviša znesek in spremeni račun, na katerega želi uporabnik nakazati denar. Gre za manj verjeten scenarij napada, saj se je težje vključiti na sredini komunikacije, čeprav varnostna luknja protokola TLS, ki je bila odkrita lanskega novembra, to omogoča. Veliko varnostno grožnjo za ta tip napada pomenijo tudi poceni domači usmerjevalniki s prenizko stopnjo zaščite (Vodopivec, 2010). Slika 4 prikazuje potek vdora mož v sredini. Vertikalna rdeča črta med bančnim strežnikom in uporabnikovim brskalnikom predstavlja mesto, kjer je skrit napadalec in prestreza podatke.

Slika 4: Potek udora MiTM »Man in the middle«

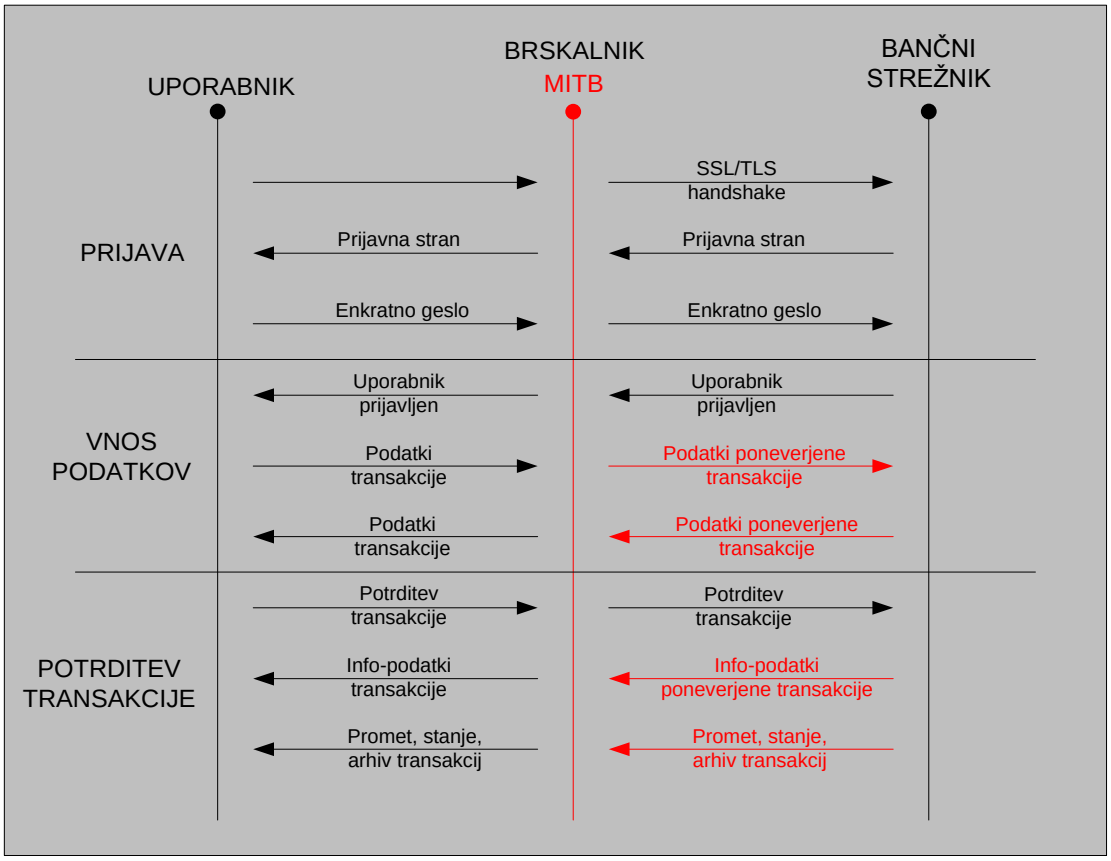


Vir: T. Vodopivec, Kdo se boji črnega moža, 2010.

2.1.3 Mož v brskalniku (MiTB)

Podoben, a veliko nevarnejši, je napad »mož v brskalniku« (angl. *Man in the browser* – MiTB), kjer trojanski konj okuži brskalnik, tako da je ta pod njegovim nadzorom. Ko uporabnik vstopi v sistem spletnega bančništva, napadalec v obliki samodejne nevarne kode čaka, da ta začne izvajati transakcijo plačevanja. Na primer vpiše znesek in številko računa, na katerega bi rad nakazal denar. Takrat lahko program poveča znesek in spremeni številko računa, a na zaslonu brskalnika je vse videti kot prej. Uporabnik potrdi plačilo, misli, da je poslal banki podatke, ki jih vidi na zaslonu, čeprav je banka dobila popolnoma drugačna navodila. Ker program »sedi« v brskalniku, je zmožen sproti prilagajati vse izpise, tako da uporabnik še dolgo ne ve, da je prišlo do zlorabe. Slika 5 prikazuje potek vdora mož v brskalniku. Vertikalna rdeča črta v sredini predstavlja uporabnikov brskalnik in mesto, kjer je skrit napadalec, ki prestreza podatke.

Slika 5: Potek udora MiTB »Man in the browser«



Vir: T. Vodopivec, Kdo se boji črnega moža, 2010.

2.2 Opredelitev varnostnih komponent e-bančništva

V zgornjih poglavjih sem navedel samo nekaj naprednejših nevarnosti, ki ogrožajo varnost e-bančništva, poudariti pa je potrebno, da je teh nevarnosti še veliko več ter da se njihovo število z vse večjim razmahom interneta tudi nenehno povečuje. Glede zagotavljanja varnosti e-bančništva iz naslova navedenih groženj sklepamo, da ni popolne zaščite, ki bi odpravila vse grožnje, je pa varnost v največji meri odvisna od človeškega faktorja. Za uspešno delovanje sistema varnosti je nujna ustrezna razporeditev vlog in odgovornosti od vodstva organizacije – banke – na najvišjem nivoju, vseh zaposlenih na najnižjem nivoju do strank uporabnikov elektronskega bančništva (Gradišar, 2003, str. 51).

Za zagotavljanje varnosti e-bančništva je pri tem pomembno upoštevati priporočila za pripravo varnostne politike, ki vključuje naslednja področja:

- sistem upravljanja z varnostjo,
- človeške vire,
- zagotavljanje varnega okolja,
- upravljanje z informacijskimi sistemi,
- obvladovanje dostopov,

- razvijanje, naročanje, prevzemanje in vzdrževanje programske opreme,
- načrtovanje neprekinjenega poslovanja,
- naročanje storitev pri zunanjih izvajalcih.

Priporočila so zasnovana tako, da obsegajo vsa pomembna področja informacijske varnosti ter poskušajo identificirati vsa morebitna tveganja ter hkrati ponuditi praktične in hitro izvedljive pravne, organizacijske in tehnološke ukrepe za zmanjševanje teh tveganj (Gradišar, 2003, 51).

2.2.1 Kriptografija

Poleg varnostnih mehanizmov, kot so požarne pregrade, protivirusne zaščite, programi za odkrivanje udorov, je osnova za zagotavljanje varnosti poslovanja banke kriptiranje izmenjave informacij – prometa med banko, poslovnimi partnerji in komitenti. Kriptologija je veda o tajnosti, šifriranju, zakrivanju sporočil (kriptografija) in o razkrivanju šifriranih podatkov (kriptoanaliza). Uporabljata se še pojma enkripcija (šifriranje) in dekripcija. Osnovno sporočilo po navadi imenujemo čistopis (angl. *cleartext, plaintext*), zašifrirano pa šifropis ali tajnopis (angl. *kriptogram, ciphertext*). Sporočilo po nekem postopku (algoritmu, metodi) spremenimo v kriptirano sporočilo, pri tem uporabimo določene vrednosti za parametre v algoritmu, ki jim rečemo ključi. Sogovornika se morata torej dogovoriti o algoritmu in ključu, da si lahko pošiljata šifrirana sporočila. Ločimo dve vrsti kriptosistemov – simetrične in asimetrični (Kriptografija, 2011).

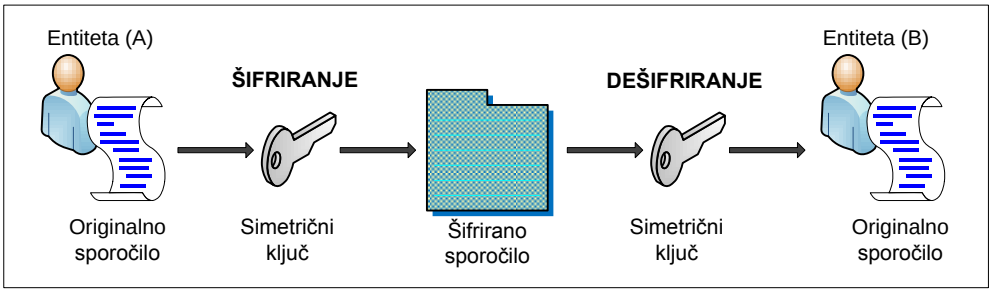
2.2.1.1 Simetrični kriptosistemi

V simetričnih kriptosistemih uporabljamo za šifriranje in dešifriranje isti ključ. Simetrični kriptosistem zagotavlja določeno mero pristnosti, saj informacija, šifrirana z enim simetričnim ključem, ne more biti dešifrirana s kakšnim drugim ključem. Torej, dokler je simetrični ključ varno shranjen, je lahko vsaka stran, ki je vključena v izmenjavo podatkov, popolnoma prepričana, da komunicira s pravo stranko na drugi strani. Dešifrirano sporočilo ima pri tem vedno nek pomen. Če nekdo drug odkrije ključ, je prekinjena tako varnost kot pristnost sporočila. Oseba z nedovoljeno uporabo simetričnega ključa lahko poleg tega, da dešifrira sporočilo, ki je bilo poslano s tem ključem, tudi šifrira novo sporočilo in ga pošlje, kot da bi prišlo od osebe, ki originalno uporablja ta ključ.

Za šifriranje podatkov v elektronskem poslovanju so na voljo številni simetrični algoritmi. Najbolj znan je DES (angl. *Data Encryption Standard*), ki sta ga razvila NIST (angl. *National Institute of Standards and Technology*) ter IBM. Omenjeni standard danes zaradi prekratkih ključev ni več priporočljivo uporabljati. Pomembnejši preizkušeni in splošno znani algoritmi so še IDEA (angl. *International Data Encryption Algorithm*), trojni 3DES,

RC2, RC4, Blowfish[1] in CAST (Smith, 2002). Spodnja Slika 6 prikazuje potek simetričnega šifriranja nekega sporočila. Entiteta A s simetričnim ključem šifrira sporočilo in ga pošlje entiteti B. Entiteta B lahko prejeto šifrirano sporočilo odšifrira samo s ključem, s katerim je bilo sporočilo predhodno šifrirano s strani entitete A.

Slika 6: Simetrična kriptografija



Vir: Cryptography Research, 2012.

Ameriška organizacija za standarde NIST je septembra 1997 razpisala natečaj za naslednika algoritma DES, ki naj bi bil močnejši in hitrejši od 3DES, odporen proti vsem zdaj znanim napadom, s 128- in 256-bitnimi ključi ter ne bi smel biti patentiran. Izmed 15 kandidatov so se v finale uvrstili naslednji algoritmi, ki so vsi uspešno prestali testiranja:

- **MARS**[2] (IBM),
- **RC6** (RSA Laboratories),
- **Rijndael**[3] (Joan Daemen, Vincent Rijmen),
- **Serpent**[4] (Ross Anderson, Eli Biham, Lars Knudsen),
- **Twofish**[5] (Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson).

Postopek za izbiro "algoritma za 21. stoletje" (angl. *Advanced Encryption Standard* – AES) je bil zaključen 2. oktobra 2000, ko je bil izbran algoritem Rijndael (Kriptografija, 2011).

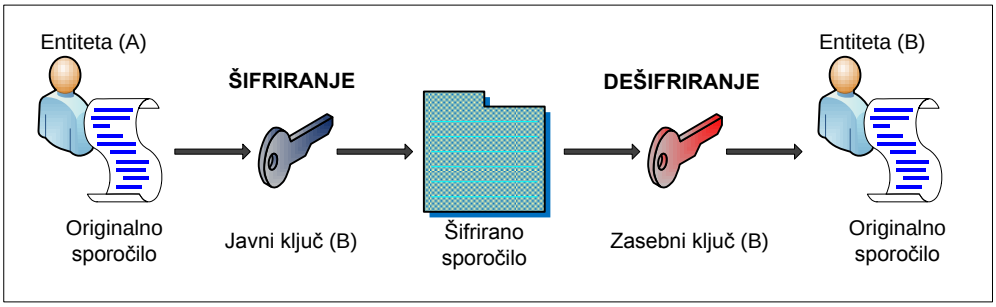
2.2.1.2 Asimetrični kriptosistemi

Drugačen pristop kot v tradicionalni, simetrični kriptografiji je od leta 1976 na voljo v asimetričnih kriptosistemih oziroma kriptosistemu javnih ključev, ki sta ga leta 1975 predstavila Whitfield Diffie in Martin Hellman – *The Diffie-Hellman key agreement protocol.* Kot že ime pove, to ni algoritem za šifriranje podatkov, temveč postopek za kreiranje in izmenjavo skritega ključa po javnem omrežju. Pri asimetričnih kriptosistemih ključa za šifriranje in dešifriranje nista enaka. Ključi nastopajo v parih, najpomembnejša

[1] Blowfish je ime šifrirnega algoritma Bruca Schneierja.
[2] MARS je ime za napredni šifrirni algoritem podjetja IBM.
[3] Rijndael je ime za šifrirni algoritem. 2. oktobra je bil izbran za naslednika DES algoritma.
[4] Serpent je ime za simetrični šifrirni algoritem, ki je drugi naslednjk DES algoritma
[5] Twofish je ravno tako ime za simetrični šifrirni algoritem, ki pa ni bil izbran kot standardiziran algoritem.

lastnost takih kriptosistemov pa je, da iz enega ključa, brez poznavanja dodatnih informacij, ni mogoče določiti preostalega. En ključ lahko zato javno objavimo. Tak ključ imenujemo javni ključ, drugi ključ iz para, ki ga mora lastnik varno shraniti, pa zasebni ključ. Kdorkoli nam želi poslati zaupno sporočilo, ga šifrira z našim javnim ključem. Samo mi, ki edini poznamo ustrezni zasebni ključ, pa lahko šifrirano sporočilo dešifriramo (Jerman-Blažič, 2001, str. 102–106).

Slika 7: Asimetrična kriptografija



Vir: Cryptography Research, 2012.

Danes je najpogosteje uporabljani asimetrični kriptografski algoritem algoritem RSA, imenovan po začetnicah priimkov njegovih avtorjev: Rivestu, Sharnirju in Adlemanu. Metoda je v ZDA patentirana, patent je potekel septembra 2000. Do tedaj je bilo potrebno za uporabo v ZDA plačevati licenčnino, zato algoritem ni bil vključen v nekatere produkte. Zaradi vse lažjega razbitja krajših RSA ključev (512, 768 bitov) smo prisiljeni uporabljati vedno daljše ključe. Tako bo potrebno opustiti 1024-bitne ključe in začeti uporabljati 2048 bitov, za pomembne operacije pa vsaj 3072 bitov (npr. za ključe overiteljev oziroma certifikatskih agencij). Za zdaj nihče ne bo šel razbijat ključa običajnega uporabnika, ker je na voljo veliko lažjih načinov, kako priti do njegovih podatkov (luknje v operacijskih sistemih, trojanski konji, phishing ...). Po drugi strani pa imajo zlikovci na voljo vojske ugrabljenih računalnikov (botnetov), ki bi jih v prihodnosti lahko uporabili tudi za take naloge. V zadnjem času dobivajo vse večjo veljavo algoritmi na podlagi eliptičnih krivulj (angl. *Elliptic curve cryptosystems* – ECC). Največ je na tem področju naredilo kanadsko podjetje Certicom. Njihova prednost pred RSA je manjša dolžina ključev in večja hitrost pri isti stopnji varnosti, zato so posebej primerni za aplikacije, pri katerih je problem velikost pomnilnika računalnika, na primer pri pametnih karticah. Jasno je, da se bodo ti algoritmi v prihodnosti uporabljali vedno več. Da se že sedaj bolj ne uporabljajo, pa je kriva patentna zaščita (Kriptografija, 2011).

Tabela 1: Dolžine kriptografskih ključev ECC in RSA

Dolžina ključa ECC	Dolžina ključa RSA
106 bitov	512 bitov
132 bitov	768 bitov
160 bitov	1024 bitov
191 bitov	1536 bitov
211 bitov	2048 bitov

Vir: Cryptography Research, 2012.

Asimetrični algoritmi se uporabljajo za izmenjavo skupnih ključev in za digitalno podpisovanje, za masovno šifriranje podatkov pa ne, ker so počasnejši od simetričnih algoritmov. Spodnja Tabela 2 prikazuje matematično osnovo, namen ter uporabo Diffie-Hellman, ElGamal, RSA in ECC ključev.

Tabela 2: Uporaba ključev Diffie-Hellman, ElGamal, RSA in ECC

Ime	**Matematična osnova**	**Namen**	**Uporaba**
Diffie-Hellman	diskretni logaritmi	izmenjava skritega ključa	V protokolih IPSEC, SSL
ElGamal	diskretni logaritmi	digitalni podpis, enkripcija	za digitalni podpis v DSS
RSA	faktoriranje velikih števil	digitalni podpis, enkripcija	za zdaj najbolj pogosto uporabljen asim. algoritem
ECC	Eliptične funkcije	digitalni podpis, enkripcija	naslednik RSA?

Vir: Cryptography Research, 2012.

2.2.1.3 Zgoščevalna funkcija

Zgoščevalna funkcija je matematična operacija, ki preslika poljubno dolg niz znakov v blok konstantne dolžine, ki je nekakšen prstni odtis oziroma povzetek vhodnega niza (message digest, message fingerprint). Od zgoščevalne funkcije pričakujemo, da (Cryptography Research, 2012):

- je nemogoče najti dve različni sporočili, ki bi ju preslikala v isti blok;
- isto sporočilo vedno preslika v enak blok;
- iz zgoščevalnega bloka ni mogoče restavrirati sporočila (od tu ime one-way hash function);
- vsaka sprememba v sporočilu povzroči spremembo zgoščevalnega bloka.

Pri ocenjevanju zgoščevalnih funkcij se uporabljajo izrazi (Cryptography Research, 2012):

- ***Collision resistance***
  Temu, da dvema različnima vhodnima datotekama ustreza enak povzetek, rečemo kolizija. Jasno je, da za vsako zgoščevalno funkcijo obstajajo kolizije, ker imamo neskončno mnogo možnih vhodov, ki jih preslikamo v končno mnogo izhodov.

Zahtevana lastnost zgoščevalne funkcije je, da se kolizij s sedanjo tehnologijo ne da najti dovolj hitro.

- ***Preimage resistance***
  To je lastnost, da je v primernem času nemogoče najti vhod, ki se preslika v vnaprej določen izhod.
- ***Second preimage resistance***
  To je lastnost, da je v primernem času nemogoče najti drugi vhod, ki se preslika v enak izhod kot vnaprej določen vhod.

Rezultat mora torej enolično identificirati datoteko. Zaradi te lastnosti so povzetki postali nepogrešljivi pri digitalnem podpisovanju, kjer zašifriramo samo povzetek, in pa kot indikatorji nespremenjenosti podatkov v postopkih za prenos podatkov. Ne smemo pa teh funkcij zamenjevati s kompresijskimi postopki (zip in podobnimi), kjer vedno lahko iz zgoščene datoteke dobimo nazaj prvotno datoteko. Postopek se začne tako, da vhodno datoteko razdelimo na bloke konstantne dolžine in konec dopolnimo do polnega bloka (padding). Potem zaporedoma obdelujemo bloke. Ena od možnosti je, da za zgoščevalno funkcijo uporabimo katerega od simetričnih algoritmov: vhodno datoteko razbijemo na bloke take dolžine, kot ustrezajo algoritmu, prvi blok zašifriramo s ključem, vsak naslednji blok seštejemo (XOR) z zašifriranim povzetkom prejšnjega bloka. Vendar se za zdaj v glavnem uporabljajo posebej za to razviti algoritmi (MD5, SHA-1), ker so hitrejši (Cryptography Research, 2012).

Najbolj znane zgoščevalne funkcije so (Kriptografija, 2011):

- **MD5** (MD je okrajšava za Message Digest)

Razvil jo je Ronald Rivest leta 1991. Opisana je v RFC 1321. Sporočilu v binarni obliki doda toliko bitov, da je skupno število deljivo s 512, in sicer je zadnjih 64 bitov rezerviranih za zapis dolžine sporočila. Prostor med koncem sporočila in temi 64 biti pa napolni tako, da najprej doda 1, potem pa same 0. Potem zaporedoma obdeluje bloke po 512 bitov. Blok razdeli na 16 besed po 32 bitov, ki jih obdeluje v štirih 32-bitnih registrih. Postopek ima štiri različne zanke. Povzetek je tisto, kar na koncu dobimo v registrih, torej je dolg 128 bitov. Njena uporaba ni več priporočljiva.

- **SHA** (Secure Hash Algorithm) – zdaj verzija SHA-1

Razvili sta jo organizaciji NIST in NSA in je objavljena kot standard FIPS PUB 180-1 (1995). Ravno tako kot MD5 obdeluje bloke po 512 bitov. Obdeluje jih v petih registrih po 32 bitov, kar da 160-bitni rezultat. Leta 2002 je NIST objavil standard FIPS PUB 180-2, ki določa SHA-256 z 256-bitnimi povzetki, SHA-384 s 384-bitnimi povzetki in SHA-512 s 512-bitnimi povzetki.

- **HAVAL**

To je verzija MD5, ki so jo razvili Yuliang Zheng, Josef Pieprzyk in Jennifer Seberry. Lahko se izbere število ponovitev algoritma in dolžino rezultata (od 92 do 256 bitov).

- **RIPEMD-160**

Zgoščevalno funkcijo so leta 1996 razvili Hans Dobbertin, Antoon Bosselaers in Bart Preneel v sklopu evropskega projekta RIPE. Obdeluje 512-bitne bloke v petih zankah, rezultat je 160-biten. Na konferenci Crypto 2005 je bilo 16. avgusta na predavanju z naslovom "New collision search for SHA-1" povedano, da je skupina profesorice Xiaoyun Wang našla način najti kolizije za SHA-1 v 2^{63} poskusih. To za enkrat še ne pomeni konec elektronskega poslovanja (2^{63} operacij je ogromna številka), je pa jasno, da bo treba SHA-1 nadomestiti z varnejšo funkcijo prej, kot smo mislili pred nekaj leti. NIST priporoča naslednje korake:

- prehod na SHA-2 (torej na SHA-224, SHA-256, SHA-384 ali SHA-512); čeprav gre za isto vrsto algoritmov kot SHA-1, so toliko močnejši, da bi morali biti nezlomljivi še eno desetletje,
- pospešiti raziskave zgoščevalnih funkcij;
- priprava izbora za novo zgoščevalno funkcijo na način, kot so ga izvedli za naslednika DES.

2.2.1.4 Primerjava kriptosistemov

Tako simetrično kot asimetrično kriptiranje imata dobre in slabe lastnosti. Slabosti simetričnih kriptosistemov so:

- izmenjava velikega števila ključev v velikih omrežjih,
- izmenjava tajnih ključev zahteva zaupanje obeh subjektov, zato je potrebno poznati vsako stran, s katero želimo varno komunicirati,
- zahteva po varnem kanalu za distribucijo ključev.

Če bi želeli imeti z vsakim subjektom, s katerim si pošiljamo zaupna sporočila, svoj skupni ključ, bi potrebovali toliko ključev, kot je subjektov. Za razliko imamo v asimetričnih kriptosistemih ne glede na število vseh uporabnikov le en par ključev. Slabosti asimetričnih kriptosistemov v primerjavi s simetričnimi sta predvsem hitrost šifriranja in dešifriranja. Asimetrični kriptoalgoritmi so veliko počasnejši od simetričnih, zato jih le redko uporabljamo za šifriranje daljših sporočil. Pri hibridnem načinu šifriramo podatke s simetričnimi kriptoalgoritmi, ključe za te algoritme pa z asimetričnimi.

Kriptosisteme javnih ključev torej uporabljamo pri šifriranju večinoma le za razdeljevanje ključev. Splošna predpostavka je, da najbolj znani in preizkušeni simetrični kriptografski algoritmi ne vsebujejo nikakršnih varnostnih lukenj, zato se lahko napadalec loti dešifriranja le tako, da preizkusi vse možne ključe. Zaželeno je, da pri šifriranju

uporabljamo le preizkušene simetrične algoritme, kjer je velikost ključev vsaj 72 bitov. Za razbitje asimetričnega kriptografskega algoritma, kakršen je RSA, ki temelji na matematičnem problemu velikih praštevil, obstajajo tudi druge metode, ne le preizkušanje vseh možnih ključev, čeprav je število teh ključev še vedno najpomembnejša informacija. Zato je pomembno, da velikosti ključev za simetrične in asimetrične postopke ne primerjamo slepo med seboj (Cryptography Research, 2012).

2.2.1.5 Dolžine ključev

Dolžine ključev so seveda najprej odvisne od vrste algoritma. Pri simetričnih (RC2, RC4, IDEA, DES, trojni DES, CAST, GOST, Rijndael ...) moramo za dešifriranje najti pravo kombinacijo bitov ključa. Če predpostavimo, da algoritem nima varnostnih lukenj, je v povprečju treba preizkusiti pol od vseh možnih kombinacij bitov, da najdemo pravo kombinacijo. Pri 40-bitnem ključu je treba preiskati 2^{39} kombinacij, kar je približno 10^{12} . Če imamo računalnik, ki preizkusi milijon kombinacij na sekundo, bo potreboval milijon sekund, kar je več kot 11 dni. V literaturi lahko najdemo tabele, ki navajajo te čase v odvisnosti od cene opreme, ki jo imamo.

Tabela 3: Časi preizkušanja glede na dolžino ključa in ceno opreme

Cena opreme	40 bitov	56 bitov	112 bitov	128 bitov
100.000 USD	2 sek	35 ur	10^{14} let	10^{19} let
10.000.000 USD	0.02 sek	21 min	10^{12} let	10^{17} let

Vir: Cryptographic Key Lenght Recommendation, 2012.

Za asimetrične algoritme (RSA, Diffie-Hellman), kjer je treba faktorirati veliko praštevilo ali pa poiskati diskretni logaritem, smo do nedavnega uporabljali ključ, omejen na 512 bitov, sedaj pa smo zaradi varnosti prisiljeni uporabljati daljše ključe, kar v praksi pomeni, da uporabljamo 1024- in 2048-bitne ključe.

V Tabeli 4 so prikazana priporočila dolžine ključev organizacije NIST, ki bi zadoščale zadovoljivi stopnji varnosti za obdobje med 2010 in 2060. Vse dolžine so navedene v bitih (Cryptographic Key Lenght Recommendation, 2012).

Tabela 4: Priporočila dolžine ključev za obdobje od 2010 do 2030 in naprej

Obdobje	Simetrični kriptosistemi	Asimetrični kriptosistemi	Diskretni ključi	Eliptične krivulje	Zgoščevalna funkcija (A)	Zgoščevalna funkcija (B)
2010	80	1024	160	160	**SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	**SHA-1** SHA-224 SHA-256 SHA-384 SHA-512
2011-2030	112	2048	224	224	**SHA-1** SHA-224 SHA-256 SHA-384 SHA-512	**SHA-1** SHA-224 SHA-256 SHA-384 SHA-512
>2030	128	3072	256	256	SHA-256 SHA-384 SHA-512	SHA-256 SHA-384 SHA-512
>>2030	192	7680	384	384	SHA-384 SHA-512	SHA-384 SHA-512
>>>2030	256	15360	512	512	SHA-512	SHA-512

Vir: Cryptographic Key Lenght Recommendation, 2012.

2.2.2 SSL/TLS komunikacija

Kratica SSL (angl. *Secure Sockets Layer*) predstavlja protokol, ki omogoča šifriranje komunikacije med strežnikom in odjemalcem. V večini primerov sta to spletni strežnik in brskalnik, v primeru elektronskega bančništva pa je to bančni spletni strežnik, kjer teče aplikacija spletnega bančništva in brskalnik komitenta. Varnostni protokol SSL je leta 1995 razvilo podjetje Netscape. Glavni cilj podjetja pri razvoju protokola je bil zagotoviti varnost in zasebnost komunikacije, poleg tega pa so si prizadevali doseči tudi:

- odprtost – možnost implementacije protokola v druge sisteme,
- skalabilnost – možnost nadgrajevanja z novimi kriptografskimi algoritmi,
- učinkovitost – parametri, izmenjani s pomočjo asimetričnih algoritmov, ki so dosti počasnejši od simetričnih, se nekaj časa hranijo zato, da se asimetrični algoritmi izvajajo manjkrat.

Protokol SSL vsebuje vse omenjene lastnosti, zato je bil izbran kot de facto standard. Njegov naslednik TLS (angl. *Transport Layer Security*), opisan v standardu RFC 2246, ki ga je pripravila organizacija IETF, se od SSL le malo razlikuje. Seveda pa se razvoj tukaj ni ustavil. Junija 2003 je bil objavljen standard RFC 3546, ki dopolnjuje RFC 2246. Dopolnitev izboljšuje učinkovitost protokola TLS. Naslednje dopolnitve so naštete v RFC 4366, tu gre predvsem za izboljšave pri uporabi protokola pri mobilnih telefonih oziroma manj zmogljivih klientih (Kriptografija, 2011).

Po OSI modelu (angl. *Open Systems Interconnection*) komunikacijskih protokolov je umeščen med transportni in aplikacijski nivo. Preverjanje vrstnega reda ali sprememb v izmenjanih blokih prepušča niže ležečemu protokolu, zato mora biti ta zanesljiv (TCP in ne UDP). Omogoča zaščito za vse aplikacijske protokole nad TCP (HTTP, smtp, news, pop3, ldap ...). Iz do sedaj omenjenega je razvidno, da samo šifriranje blokov podatkov še ne bi

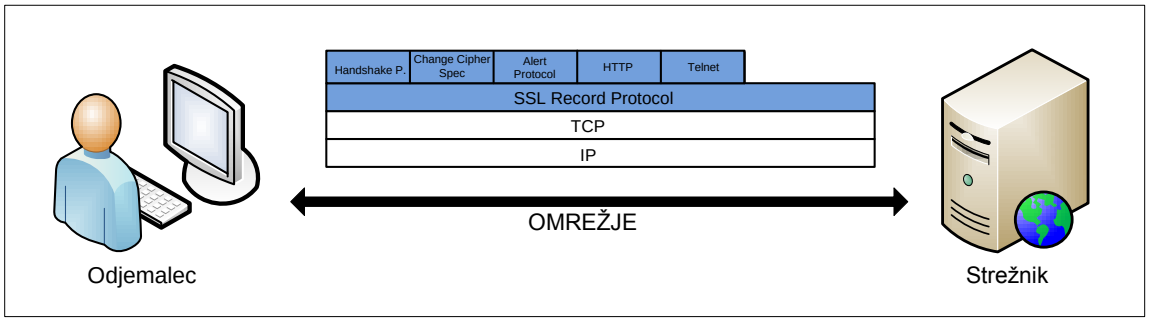
omogočilo varne komunikacije, prav tako pomembno je preverjanje nespremenjenosti podatkov (angl. *integrity*) ter preverjanje avtentičnosti obeh strani (*authentication*) in vse to vključuje SSL.

Protokol SSL sestavljata dva sloja:

1) SSL Handshake Protocol omogoča usklajevanje algoritmov, overjanje strežnika in odjemalca, prenos digitalnih certifikatov in določitev skupnega ključa za simetrični kriptoalgoritem,
2) SSL Record Protocol definira osnovni format izmenjanih podatkov, zagotavlja neokrnjenost in šifriranje.

Slika 8 prikazuje varno SSL povezavo med odjemalcem in strežnikom. Strežnik in odjemalec pri vzpostavitvi povezave najprej na podlagi prvega protokola preverita identiteto drug drugega, uskladita kriptografske algoritme in si varno izmenjata ključ ter ostale podatke, ki so potrebni za poznejše šifriranje. Za šifriranje skrbi SSL Record Protocol. Iz slike pa je razvidno, da oba omenjena protokola slonita na protokolnem skladu TCP/IP.

Slika 8: SSL povezava



Vir: Secure Sockets Layer (SSL), 2011.

Glede medsebojnega overjanja so možne naslednje kombinacije:

- ni overjanja,
- anonimni odjemalec preveri certifikat strežnika,
- vsak preveri certifikat sogovornika.

Prva možnost je seveda najslabša, podatki se sicer izmenjujejo v šifrirani obliki, vendar jih lahko kdo prestreže in spremeni (man-in-the-middle attack). Nabor algoritmov in velikost ključev lahko določi uporabnik sam pri nastavitvi SSL parametrov v brskalniku. Preverjanje identitete, ki poteka večinoma s pomočjo elektronskih potrdil, je lahko tudi enosmerno. V tem primeru preveri identiteto strežnika le odjemalec, ne pa tudi obratno. Ko je postopek preverjanja, usklajevanja kriptografskih algoritmov, ki jih bosta uporabljala, ter izmenjave ključa za simetrično šifriranje končan, lahko s pomočjo drugega dela protokola začneta s pošiljanjem podatkov. Podatkom je vedno zagotovljena neokrnjenost,

lahko pa so tudi šifrirani, če je treba zagotoviti zaupnost (Secure Sockets Layer (SSL), 2011).

SSL loči podatke seje (angl. *Session*), ki se hranijo dalj časa, in podatke povezave (angl. *Connection*). S sejo označujemo neprekinjeno izmenjavo podatkov – koristne informacije med odjemalcem in strežnikom. Vsaki seji pa lahko pripada več povezav (*connections*), tudi istočasnih, npr. za prenos slike poleg teksta. Seji pripadajo naslednji podatki, ki si jih oba zapomnita in s tem skrajšata naslednja dogovarjanja:

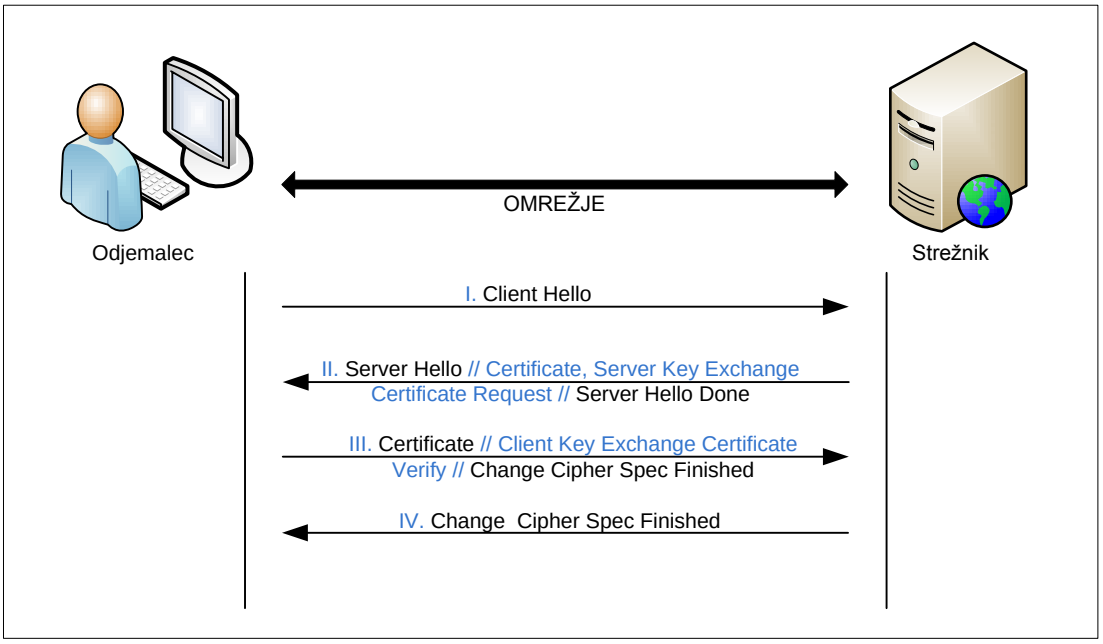
- oznaka seje – 32 bajtov,
- certifikat sogovornika (če ga ima oziroma če je tako določeno),
- simetrični algoritem za šifriranje podatkov,
- zgostitveni algoritem za računanje MAC (angl. *Message Authentication Code*),
- postopek za komprimiranje,
- Master Secret – 48 bajtov (osnova za izračun simetričnega ključa in drugih parametrov),
- is_resumable Flag (če je to stikalo vključeno, bosta za naslednjo povezavo te seje uporabila iste pravkar naštete parametre).

Za povezavo (*connection)* pa so značilni naslednji podatki:

- Client Challenge (32-bajtno naključno generirano število),
- Server Challenge (32-bajtno naključno generirano število),
- zaporedna številka poslanega paketa,
- zaporedna številka dobljenega paketa,
- števila, ki jih izračunata iz Master Secret,
- simetrični ključ odjemalca,
- simetrični ključ strežnika,
- overitveno število odjemalca (MAC secret),
- overitveno število strežnika,
- začetni vektor za odjemalca (če je potreben),
- začetni vektor za strežnik (če je potreben).

Za vsako povezavo si izmenjata drugo osnovo za ključ (*Challenge*), zato s ključem ene povezave ne moremo dešifrirati podatkov druge povezave – poznati bi morali 48-bajtni Master Secret. Dolžina ene seje je po protokolu omejena na 24 ur (če je seveda odjemalec in strežnik prej ne prekineta), kar bi veljalo skrajšati na nekaj ur. Na Sliki 9 je podrobno predstavljeno izvajanje SSL Handshake protokola med odjemalcem in strežnikom. Prikazani so vsi štirje koraki, ki so potrebni za izmenjavo ključa in pripravo na izvedbo šifriranja prenosnih podatkov.

Slika 9: Izvajanje Handshake protokola



Vir: Secure Sockets Layer (SSL), 2011.

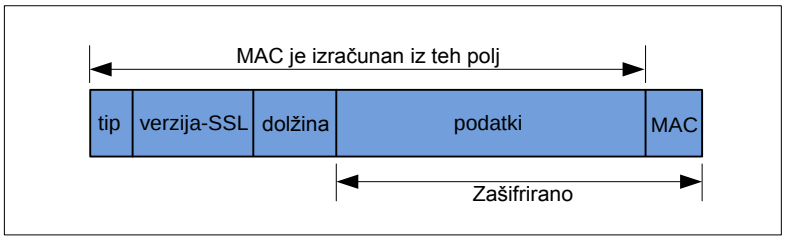
SSL Record Protocol poskrbi, da se sporočila prenašajo šifrirano tako, kot je bilo dogovorjeno na višjem SSL Handshake protokolu. Podatke razbije na bloke, dolge do 2^{14} bajtov (16 Kb). V verziji 3 je predvideno komprimiranje podatkov pred šifriranjem. Bloku podatkov doda zaporedno številko sporočila, tip zapisa (ki loči dejanske podatke od kontrolnih sporočil SSL z višjega nivoja) ter dolžino bloka podatkov. Iz tega izračuna MAC, ki omogoča kontrolo nespremenjenosti podatkov in overovitev pošiljatelja:

MAC = hash (MAC-p + pad2 + hash(MAC-p + pad1 + zap.št. + tip + dolžina bloka podatkov + podatki))

MAC-p = overitveno število pošiljatelja, izračunano iz podatkov, izmenjanih na višjem nivoju SSL
pad1 = 48 znakov 0x36 pri MD5 ter 40 znakov 0x36 pri SHA
pad2 = 48 znakov 0x5c pri MD5 ter 40 znakov 0x5c pri SHA

Slika10 prikazuje potek SSL Record Protocol-a oz. postopek šifriranja prenosnih podatkov.

Slika 10: SSL Record Protocol



Vir: Secure Sockets Layer (SSL), 2011.

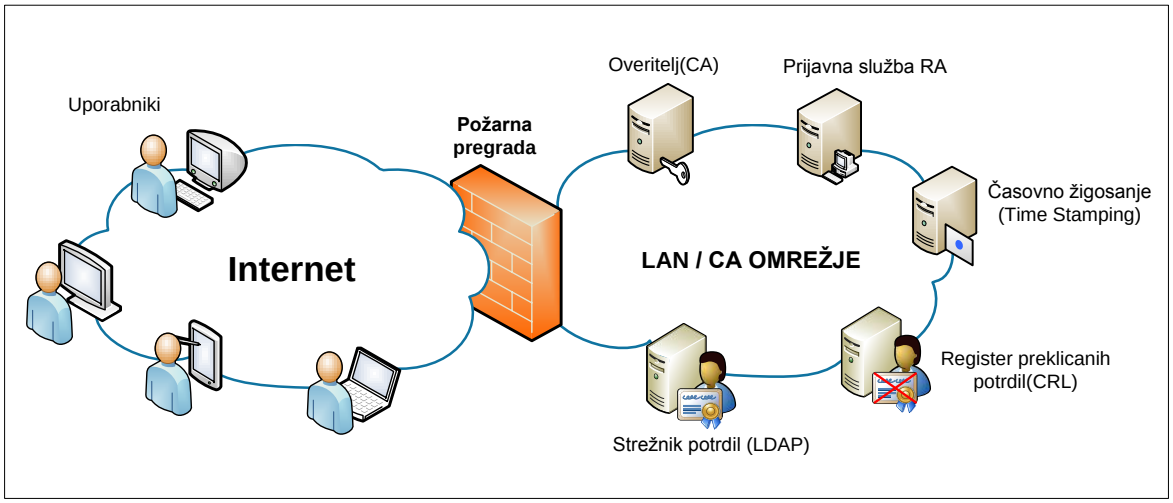
Protokol MAC podatke zašifrira z dogovorjenim ključem za to povezavo in zapis preda transportnemu nivoju pod seboj (oziroma pri sprejemu dešifrira, izračuna MAC in ga primerja s prejetim MAC ter zapis preda višjemu nivoju).

2.3 Infrastruktura javnih ključev PKI

Celoten sistem za uporabo asimetrične kriptografije v elektronskem poslovanju imenujemo infrastruktura javnih ključev (angl. *Public Key Cryptography Infrastructure - PKI*). Vključuje organizacijsko, tehnično in pravno infrastrukturo za izdajo, upravljanje in preklic digitalnih potrdil. Je zbirka programske in strojne opreme, procesov, pravil in tehnologij kriptografije javnih ključev. PKI infrastruktura določa protokole in storitve pri upravljanju z javnimi ključi.

PKI infrastrukturo sestavlja več komponent: overitelj digitalnih potrdil (angl. *Certification authority* – CA), prijavna služba (angl. *Registration authority* – RA), strežnik potrdil ali imenik (angl. *directory*), register preklicanih potrdil (angl. *Certificate Revocation List* – CRL) in časovno žigosanje (angl. *Time Stamping*). K naštetim elementom moramo dodati še končnega uporabnika oz. končno entiteto (angl. *End entity*). Končna entiteta je lahko uporabnik z računalnikom s kriptografsko programsko opremo, spletni strežnik ali pa tudi pametni mobilni telefon, ki zmore procesirati digitalna potrdila (Internet Security and Encryption, 2012). Slika 11 prikazuje vse potrebne entitete, ki morajo biti v omrežju prisotne za delovanje PKI infrastrukture.

Slika 11: PKI infrastruktura



Vir: Public key infrastructure, 2011.

Osnovna naloga PKI je omogočiti varno elektronsko poslovanje med podjetji, ki so svoje storitve preselila na splet, in seveda uporabniki teh storitev, npr. elektronsko bančništvo – komitent. PKI temelji na elektronskih potrdilih, s katerimi potrdimo uporabnikov elektronski podpis in njegov javni ključ, hkrati pa z njimi šifriramo podatke, ki si jih izmenjujeta komitent in banka. PKI lahko v elektronskem poslovanju združuje naslednje subjekte in dokumente (Public key infrastructure, 2011):

- overitelj,
- prijavna služba,
- politika overitelja,
- sistem distribucije potrdil,
- dokument o ravnanju s potrdili.

2.3.1 Digitalna potrdila (Certifikati)

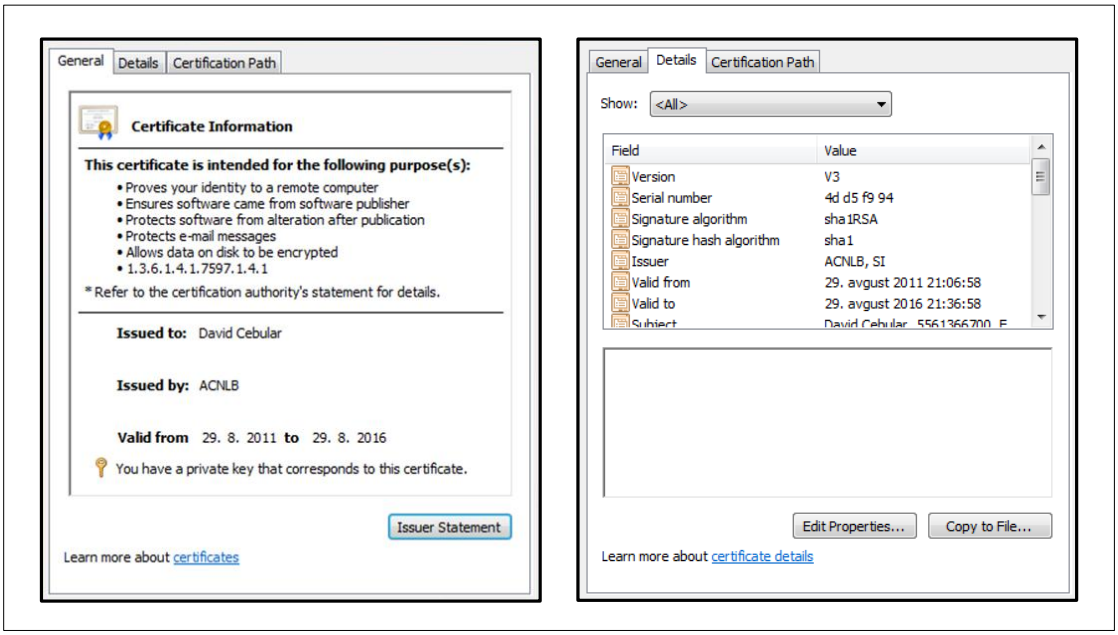
Že v prejšnjem poglavju smo ugotovili, da šifriranje prometa brez medsebojnega overjanja komunikacijskih entitet ni dovolj za zagotavljanje zadostne varnosti. Najbolj primerno sredstvo za overjanje komunikacijskih entitet je digitalna osebna izkaznica ali digitalno potrdilo (angl. *Digital Certificate*), pogovorno ga poimenujemo tudi certifikat. Digitalno potrdilo predstavlja enolično povezavo med imetnikom potrdila in javnim ključem. Potrdilo vsebuje vse osnovne podatke o imetniku in javni ključ. Stopnjo odgovornosti in tveganja v elektronskem poslovanju lahko uporabniki rešujejo s kvalificiranimi ali nekvalificiranimi digitalnimi potrdili.

Nekvalificirana potrdila temeljijo na pogodbenem razmerju strank, kjer gre za dogovor med strankami, ki poslujejo po že utečenih poteh. Pri elektronskem poslovanju strank, ki še niso poslovale ena z drugo, pa je smiselna vključitev tretje osebe, ki izdaja kvalificirana potrdila. Kvalificirana potrdila temeljijo na natančno predpisanem uradnem postopku identifikacije imetnika. Možnost zlorabe je minimalna, saj je podan prepričljiv dokaz o

identiteti podpisnika. Takšno identifikacijo lahko izvajajo overitelji in pa v njihovem imenu tudi pooblaščene prijavne službe. Kvalificirana digitalna potrdila lahko izdaja tudi overitelj ACNLB, ki deluje v sklopu NLB, a o tem več v poglavju 3.4.1.

Digitalno potrdilo je tako imetnikova osebna izkaznica v elektronskem bančništvu ali elektronskem poslovanju nasploh. Če ne gre za zaprt sistem uporabnikov, so digitalna potrdila javno objavljena, kar omogoča ugotovitev ter preverjanje identitete podpisnika na osnovi njegovega javnega ključa (HalcomCA, 2011). Slika 12 prikazuje osebno digitalno potrdilo za fizične osebe, izdano od overitelja ACNLB. Na prvem zavihku lahko vidimo navedene splošne pogoje uporabe, za koga je bilo digitalno potrdilo izdano, kdo ga je izdal in obdobje veljavnosti. Na zavihku podrobnosti pa lahko vidimo še ostale potrebne parametre digitalnega potrdila.

Slika 12: Osebno digitalno potrdilo za fizične osebe



2.3.1.1 Osebno digitalno potrdilo za fizične osebe

Iz vidika sistemske informatike je digitalno potrdilo računalniški zapis, sestavljen iz dveh delov, ki vsebujeta naslednje podatke (Internet X.509 Public Key Infrastructure, 2005):

Podatkovni del:

- različico formata po priporočilu X.509[6],
- enolično serijsko številko potrdila v okviru izdanih potrdil overitelja (angl. *Certification Authority - CA*),
- neobvezni polji, ki omogočata ponovno uporabo le dodeljenih razločevalnih imen overitelja ali lastnika javnega ključa,

[6] Oznaka X.509 predstavlja ITU-T standard, ki opredeljuje infrastrukturo javnih ključev (PKI).

- razločevalno ime lastnika javnega ključa, javni ključ in identifikator algoritma, v katerem se ključ uporablja,
- obdobje veljavnosti overitelja,
- razločevalno ime overitelja, ki je izdal potrdilo,
- neobvezne razširitve, ki vsebujejo dodatne informacije o javnem ključu in politikah overjanja, imetniku in izdajatelju potrdila ter različnih omejitvah.

Del elektronskega podpisa:
- identifikator algoritma, s katerim je bilo podpisano potrdilo,
- elektronski podpis overitelja.

Osnovni format potrdila, ki ga označujemo kot format različice 1, je bil prvič objavljen leta 1998. Leta 1993 je bil razširjen z dvema neobveznima poljema (različica 2 z oznako v2), leta 1997 pa so mu bile dodane še neobvezne razširitve (različica 3 z oznako v3) (Internet X.509 Public Key Infrastructure, 2005).

2.3.1.2 Šifrirni algoritmi, formati podatkov in protokoli

Primer ACNLB

- za podpisovanje potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,

- za šifriranje podatkov algoritme Triple DES, CAST-128 in RC2 (standardi FIPS PUB 186-2, ANSI X9.30 (1), IEEE P1363 in ISO/IEC 14888-3),

- zgostitvene algoritme SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),

- način uporabe algoritma RSA za upravljanje s ključi RSA (RFC 1421 in RFC 1423(PEM) in PKCS#1),

- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997 ter X.509 ver. 3 (v3),

- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z verzijo 2 (v2),

- oblika RSA enoličnih razločevalnih imen ter format javnega ključa ustrezajo priporočilu RFC 1422 in 1423 (PEM) in PKCS#1,
- protokol LDAP ustreza priporočilu RFC 1777 in RFC 2559,

- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,

- komunikacija med programsko opremo na strani imetnika in infrastrukturo NLB CA poteka po protokolu SEP (angl. *Secure Exchange Protocol*), ki temelji na standardu GULS (angl. *Generic Upper Layers Security*), ki ustreza priporočilom ITU-T za X.830,

- za podpisovanje X.831, X.832 in ISO/IEC 11586-1, 11586-2 in 11586-3 ali protokolu PKIX-CMP, ki temelji na priporočilu RFC 2510.

Overitelji izdajajo več vrst certifikatov in za različne potrebe. V primeru agencije AC NLB razlikujemo digitalna potrdila za fizične in pravne osebe, napredna digitalna potrdila (Enterprise), strežniška digitalna potrdila in potrdila za naprave (angl. *code signing*). V Tabeli 5 je zajeta struktura digitalnega potrdila za fizične osebe, overitelja AC NLB.

Tabela 5: Struktura digitalnega potrdila za fizične osebe

Podatek	**Vrednost oz. pomen**
Verzija X.509, angl. *Version*	3
Identifikacijska oznaka, angl. *Serial Numb*er	<enolična interna številka potrdila>
Algoritem za podpis potrdila, angl. *Signature Algorithm*	sha1WithRSAEncryption
Ime izdajatelja, angl. *Issuer*	c=si, o=NLB, ou=Fizizne osebe
Začetek in konec veljavnosti potrdila, angl. *Validity*	Not Before: <začetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>
Imetnik, angl. *Subject*	<razločevalno ime imetnika, ki vključuje naziv imetnika, serijsko številko potrdila, v primeru osebnih potrdil tudi institucijo oz. področje ...>
Alternativno ime, angl. *Subject Alternative Name*	*<elektronski naslov imetnika oz. splošnega naziva oz. strežnika>*
Imetnikov javni ključ, ki pripada ustreznemu paru ključev, angl. *RSA Public Key (2048 bit)*	<javni ključ, šifriran z algoritmom RSA, dolžine 2048 bitov>
Identiteta imetnikovega ključa, angl. *Subject Key Identifier*	<odtis imetnikovega javnega ključa>

Se nadaljuje

Nadaljevanje

Identiteta registra preklicanih potrdil, angl. *CRL Distribution Points*	CN=CRL483 O=ACNLB C=SI URL=ldap://acldap.nlb.si/o=ACNLB,c=SI?certificateRevocationList URL=http://acldap.nlb.si/crl/acnlbcrl.crl
Podpis izdajatelja ACNLB	<podpis potrdila s strani izdajatelja ACNLB>
Identiteta ključa izdajatelja ACNLB, angl. *Authority Key Identifier* (SHA1)	0456 F23D 1E9C 43AE CB0D 807F 1C06 4755 1A05 F456

Vir: AC NLB, Politika AC NLB Javni del notranjih pravil, 2011.

2.3.1.3 Lastnosti osebnega digitalnega potrdila

Vsak imetnik osebnega potrdila ima dva ločena para ključev – za digitalno podpisovanje/overjanje in za šifriranje/dešifriranje podatkov. Oba para imata en zasebni in en javni ključ (AC NLB, 2011).
Par ključev za digitalno podpisovanje/overjanje sestavlja:

- zasebni ključ za podpisovanje ter
- javni ključ za overjanje podpisa.

Par ključev za šifriranje/dešifriranje sestavlja:

- zasebni ključ za dešifriranje ter
- javni ključ za šifriranje.

Par ključev za podpisovanje/overjanje se tvori z imetnikovo programsko opremo. Overitelj nikoli ne hrani in tudi nima dostopa do ključa za podpisovanje. Ključ za overjanje podpisa se pošlje overitelju, ki izda osebno potrdilo za verifikacijo podpisa, katerega sestavni del je ključ za overjanje podpisa. Osebno potrdilo za verifikacijo podpisa se shrani pri imetniku. Par ključev za šifriranje/dešifriranje se tvori na strani overitelja. Ključ za dešifriranje hrani imetnik. Zaradi možnega dostopa (dešifriranja) do pomembnih zašifriranih podatkov, če ključ za dešifriranje iz kakršnihkoli vzrokov ni več dostopen, se ta ključ po posebnem režimu, ki je določen z interno politiko overitelja, varno hrani tudi v arhivu overitelja. Overitelj izda osebno potrdilo za šifriranje, katerega sestavni del je ključ za šifriranje. Osebno potrdilo za šifriranje se objavi v javnem imeniku potrdil. Veljavnost osebnega potrdila je odvisna od overitelja, po navadi je to od 3 do 5 let od prevzema. Podaljšanje veljavnih potrdil in generiranje novih parov ključev se izvaja avtomatsko pred iztekom roka, določenim za veljavnost potrdila. Veljavnost ključa za overjanje digitalnega podpisa je tudi odvisna od politike overitelja, po navadi do 5 let od prevzema. Nov ključ za overjanje podpisa se generira avtomatsko pred iztekom roka, določenim za veljavnost potrdila.

Poleg osnovnih podatkov iz Tabele 5 osebno potrdilo za šifriranje, objavljeno v javnem imeniku, vključuje še podatke, navedene v Tabeli 6.

Tabela 6: Vključeni podatki pri osebnem potrdilu za šifriranje

Podatek	**Vrednost oz. pomen (osebno - za šifriranje)**
Namen uporabe, angl. *Key Usage*	Key Encipherment
Začetek in konec veljavnosti ključa za dešifriranje, angl. *Private Key Usage Period*	Not Before: <začetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>
Politika, pod katero je bilo izdano potrdilo (OID) in iz katere je razvidno tudi, da gre za kvalificirano potrdilo. Spletni naslov za dostop do politike, angl. *Certificate Policies*	Policy: 3.6.1.4.1.7597.1.4.1 CPS: http://www.nlb.si/ac-nlb-notranja-pravila

Vir: AC NLB, Politika AC NLB Javni del notranjih pravil, 2011.

Poleg osnovnih podatkov iz Tabele 5 osebno potrdilo za verifikacijo podpisa, ki ga hrani imetnik, vključuje še podatke, navedene v Tabeli 7.

Tabela 7: Vključeni podatki pri osebnem potrdilu za verifikacijo podpisa

Podatek	**Vrednost oz. pomen (osebno -** za verifikacijo podpisa**)**
Namen uporabe, angl. *Key Usage*	Digital Signature
Začetek in konec veljavnosti ključa za dešifriranje, angl. *Private Key Usage Period*	Not Before: <začetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>
Politika, pod katero je bilo izdano potrdilo (OID) in iz katere je razvidno tudi, da gre za kvalificirano potrdilo. Spletni naslov za dostop do politike, angl. *Certificate Policies*	Policy: 3.6.1.4.1.7597.1.4.1 CPS: http://www.nlb.si/ac-nlb-notranja-pravila

Vir: AC NLB, Politika AC NLB Javni del notranjih pravil, 2011.

2.3.1.4 Lastnosti spletnega SSL potrdila

Vsak imetnik SSL potrdila ima en par ključev, ki ga sestavlja zasebni in javni ključ. Par ključev se tvori z imetnikovo programsko opremo. Zasebni ključ ima samo imetnik. Overitelj nikoli ne hrani in tudi nima dostopa do imetnikovega zasebnega ključa. Javni ključ se pošlje overitelju, ki izda in objavi SSL potrdilo z javnim ključem kot sestavnim

delom potrdila. Veljavnost spletnih potrdil je odvisna od overitelja, po navadi do 5 let od prevzema. Poleg osnovnih podatkov iz Tabele 5 vključuje SSL potrdilo še podatke, navedene v Tabeli 8.

Tabela 8: Vključeni podatki pri SSL potrdilu

Podatek	**Vrednost (spletno)**	**Vrednost (spletno-strežnik)**
Namen uporabe, angl. *Key Usage*	Digital Signature, Key Encipherment	
Pričetek in konec veljavnosti ključa za dešifriranje, angl. *Private Key Usage Period*	Not Before: <pričetek veljavnosti po GMT> Not After: <konec veljavnosti po GMT>	
Vrsta potrdila, angl. *Netscape Cert Type*	SSLClient, S/MIME	SSL Server
Politika, pod katero je bilo izdano potrdilo (OID), in iz katere je razvidno tudi, da gre za kvalificirano potrdilo. Spletni naslov za dostop do politike, angl. *Certificate Policies*	Policy: 3.6.1.4.1.7597.1.4.1 CPS: http://www.nlb.si/ac-nlb-notranja-pravila	

Vir: AC NLB, Politika AC NLB Javni del notranjih pravil, 2011.

2.3.2 Overitelj digitalnih potrdil

Overitelj digitalnih potrdil (CA – *Certification Authority, Certification Agency*) je organizacija, ki izdaja digitalna potrdila ali opravlja ostale storitve v zvezi z overjanjem ali elektronskimi podpisi. Organizaciji pravimo tudi agencija za certificiranje ali urad za overjanje. Overitelj igra osrednjo vlogo v infrastrukturi javnih ključev. V sklopu izdajanja potrdil overitelj nudi naslednje storitve (Public key infrastructure, 2011):

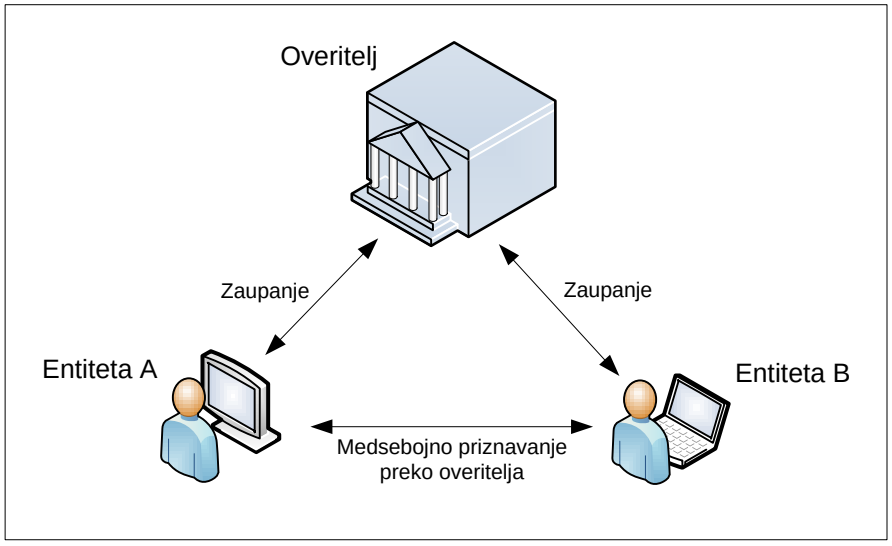
- sprejemanje naročil za izvajanje postopkov nad digitalnimi potrdili,
- izvajanje identifikacije entitete,
- objavljanje in vzdrževanje informacije o stanju digitalnih potrdil,
- preklicevanje potrdil,
- izdajanje časovnih žigov.

Infrastrukturo overitelja sestavljajo (Public key infrastructure, 2011):

- močno varovani notranji prostori,
- strojna in programska oprema, ki jo overitelj uporablja za upravljanje s potrdili ali za opravljanje drugih storitev v zvezi z elektronskim podpisovanjem,
- osebje ter
- metode in postopki pri upravljanju s potrdili in drugih storitvah v zvezi z elektronskim podpisovanjem.

Uporabniki bi si digitalno potrdilo lahko izdali tudi sami in z njim medsebojno poslovali. Pri tem pa bi obstajala možnost, da se uporabnik izdaja za drugega. Zato je potrebno vpeljati tretjo osebo (overitelj), ki ji zaupajo vsi uporabniki v infrastrukturi in ki skrbi za izdajo potrdil na podlagi predhodne identifikacije imetnika. Overitelj odpravi problem lažne identitete in problem zanikanja identitete. Overitelj torej predstavlja ustanovo, ki ji imetniki digitalnih potrdil zaupajo in jo pooblaščajo, da upravlja z njihovimi digitalnimi potrdili (Public key infrastructure, 2011). Na Sliki 13 sta prikazani entiteti A in B, ki zaupata overitelju. Overitelj pa obema na podlagi predhodne identifikacije podeli digitalna potrdila.

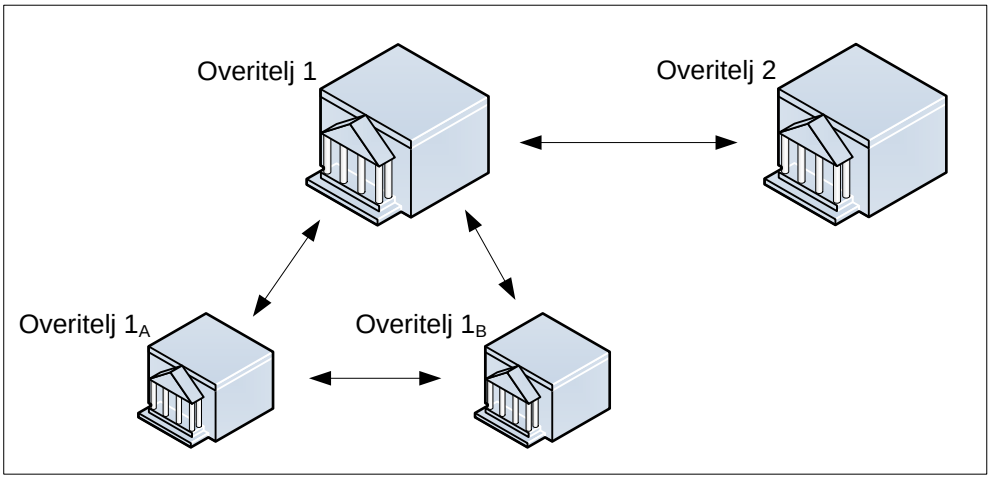
Slika 13: Medsebojno priznavanje uporabnikov preko overitelja



Vir: Public key infrastructure, 2011.

Na ravni države se lahko formira več overiteljev. Ti lahko delujejo povsem neodvisno ali pa se medsebojno priznavajo. V primeru priznavanja so lahko med seboj enakopravni ali pa drug drugemu podrejeni. Slika 14 prikazuje primer horizontalnega povezovanja, kjer se overitelja medsebojno overita in s tem omogočata varno in zanesljivo komunikacijo med lastniki digitalnih potrdil obeh overiteljev. Prikazan je tudi primer vertikalne povezave overiteljev. V tem primeru gre za formiranje hierarhične strukture overiteljev z obrnjeno drevesno strukturo, kjer vrhovni (angl. *Root*) overitelj elektronsko podpisuje digitalna potrdila za nižji nivo overiteljev. Tako se formira veriga zaupanja (angl. *Chain of trust*).

Slika 14: Medsebojno priznavanje overiteljev



Vir: Public key infrastructure, 2011.

V Sloveniji overitelji kvalificiranih potrdil izdajajo potrdila državljanom Republike Slovenije oz. tujcem s stalnim ali začasnim prebivališčem v Republiki Sloveniji. Prvi overitelj v Sloveniji, SI-CA (*Slovenian Certification Authority*), je bil vzpostavljen leta 1995. SI-CA je tudi del panevropske mreže overiteljev EuroPKI. Slovenski prostor tako pokrivajo SI-CA overitelja Ministrstva za javno upravo (SIGEN-CA in SIGOV-CA), overitelj podjetja Halcom d.d. HALCOM-CA, overitelj Pošte Slovenije d.d. POŠTA-CA, svojo agencijo pa ima tudi Nova Ljubljanska Banka ACNLB. V EuroPKI je tako vključen samo en Slovenski overitelj. EuroPKI je krovna infrastruktura javnih ključev, ki je namenjena združevanju overiteljev iz vseh evropskih držav. Prednost vključenosti v evropsko infrastrukturo javnih ključev je predvsem v medsebojnem priznavanju potrdil. Uporabniki morajo tako zaupati samo enemu vrhovnemu overitelju in ni potrebe po križnem certificiranju (angl. *Cross-certification*) (Public key infrastructure, 2011).

V skupino overiteljev Ministrstva za javno upravo pa spada tudi zaprt sistem CSCA-SI (*Country Signing Certificate Authority Slovenia*). CSCA-SI izdaja digitalna potrdila izključno za sisteme za podpisovanje podatkov za potrebe biometričnih potnih listin. Potni listi državljanov Republike Slovenije so bili nadgrajeni z biometričnimi zaščitnimi elementi. Biometrični podatki so zapisani na brezkontaktnem čipu, ki je vgrajen v potni list, ti podatki pa morajo biti elektronsko podpisani. Vsaka država naj bi za te namene ustanovila svojega overitelja (Public key infrastructure, 2011).

2.3.3 Notranja pravila – politike

V PKI infrastrukturi je poglavitnega pomena zaupanje. Po zakonu mora overitelj objaviti svoja notranja pravila (politiko), s katerimi si lahko pridobi zaupanje do strank. To je skupek pravil, ki opredeljuje uporabnost digitalnega potrdila. Notranja pravila vsebujejo javni in zaupni del. V tujini analogijo javnemu delu notranjih pravil predstavljata podobna dokumenta, ki se imenujeta CP (angl. *Certification Policy*) in CPS (angl. *Certification*

Practice Statement). Overitelj v notranjih pravilih izraža predvsem svoj interes in razloge za zaupanja vredno organizacijo. V javnem delu so med drugim opisani procesi, kadri, ki jih zaposluje, postopki nad digitalnimi potrdili in njihovo vzdrževanje, pa tudi obveznosti uporabnikov ob razkritju ključa za podpisovanje ali ob zlorabi potrdila. Navedeni so algoritmi in standardi, na katerih temelji izdaja potrdil oz. njihovih ključev in preklicevanje. V zaupnem delu pa so še natančno podane značilnosti računalniške opreme, fizičnega varovanja, protipožarnega sistema, varovanja računalniškega omrežja, sistema proti izlitju vode, sistema prezračevanja in neprekinjenega napajanja. Na vpogled uporabnikom je možen samo javni del, zaupni del pa je shranjen pri samem overitelju in se smatra kot poslovna skrivnost (AC NLB, 2011).

Uporabnik se mora strinjati z javnim delom notranjih pravil overitelja, ko odda vlogo za izdajo digitalnega potrdila oz. najkasneje, ko prevzema digitalno potrdilo. Notranja pravila so neke vrste splošni pogoji poslovanja. Notranja pravila so enolično določena z mednarodno številko CPOID (angl. *Certification Policy Object IDentifier*). CPOID izhaja iz OID, ki ga je predstavila organizacija ISO. OID ali objektni identifikator je unikaten niz številk, ki so zgrajene hierarhično. Vsi interni identifikatorji se začnejo z 1.3.6.1. Vsako notranje pravilo ima tudi svoje ime (CPName – Certification Policy Name) in je enolično povezano s CPOID. Digitalno potrdilo X.509v3 v polju »Certificate Policies« oz. »certifikatni pravilniki« vsebuje enolično mednarodno številko notranjega pravila (CPOID), pod katerim je izdano potrdilo in spletni naslov za dostop do tega notranjega pravila (AC NLB, 2011).

2.3.4 Prijavne službe RA

V večini primerov overitelji pokrivajo večja geografska območja. Ta območja pa so prevelika, da bi jih kadrovsko pokrivali sami, zato sodelujejo s prijavno službo (*Registration Authority* – RA) ali agencijo za registracijo. Overitelji tako izdajajo digitalna potrdila na podlagi podatkov prijavne službe. Prijavna služba vključuje osebje, procese in orodja za podporo delovanja overitelja in je odgovorna za (AC NLB, 2011):

- pravilno identifikacijo imetnikov potrdil,
- komunikacijo z uporabniki,
- posredovanje podatkov overitelju v dogovorjeni obliki,
- sodelovanje in obveščanje overitelja,
- pravočasno obveščanje overitelja o preklicu,
- hrambo vlog za izdajo, spremembe in preklic (telefonskih, papirnih) ter
- vnos vlog v sistem overitelja.

Prijavna služba opravlja naloge po pooblastilu in navodilih overitelja, hkrati pa mora biti njihovo delovanje skladno z zakonom ZEPEP.

Svojo prijavno službo ima tako tudi agencija ACNLB, kar pomeni, da je v vsaki poslovalnici NLB vsaj ena oseba usposobljena opravljati naloge prijavne službe. Slovenski prostor pokrivajo še prijavne službe drugih overiteljev:

- upravne enote (za fizične osebe), DURS (za poslovne subjekte), slovenske ambasade in diplomatska konzularna predstavništva overitelja SIGEN-CA,
- poštne poslovalnice pri POŠTARCA.

Komitentom, katerih banke nimajo svojega overitelja kot NLB, pa storitve overiteljev in prijavnih služb nudi komercialni overitelj HALCOM-CA.

2.4 Varnostni mehanizem EMV CAP

Ob zadnjih metodah napadov (MiTM, MiTB) se je izkazalo, da je poleg šifriranja prometa ter avtentikacije uporabnikov zelo pomembna tudi avtorizacija oziroma podpis transakcije. Takšen varnostni element je uvedla tudi NLB, saj morajo uporabniki njene spletne banke pri izvajanju nakazil na račune, kamor do tedaj še niso nakazovali, vpisati dodatno varnostno geslo iz nabora znakov, ki so jih prejeli po pošti. Med take mehanizme spadajo bralci bančnih kartic EMV CAP (angl. *Chip Authentication Program*), ki so sposobni na podlagi pametne kartice ter transakcijskih podatkov generirati enkratno geslo (angl. *One time password* – OTP). Enkratno geslo lahko služi kot avtentikacijsko sredstvo ali za podpis transakcije, predstavlja pa dodatno varnostno komponento varovanja e-bančnih sistemov. Enkratno geslo je bolj smiselno uporabljati za avtorizacijo transakcije, saj je za avtentikacijo uporabnikov veliko bolj primerno osebno digitalno potrdilo. Banke pa bi morale iti še korak naprej in uvesti potrjevanje transakcij po neodvisnem kanalu, torej kanalu, ki ga napadalec ne more nadzorovati. Med take mehanizme spadata potrditveno sporočilo sms ter klic na znano telefonsko številko. Zavedati pa se moramo, da vsaka dodatna varnostna komponenta povzroča tudi manj udobno e-bančno storitev.

2.4.1 Standardi kartičnih sistemov Europay Mastercard Visa (EMV)

Europay International, MasterCard International in Visa International so zaradi vedno večjega števila zlorab kartic z magnetnimi zapisi že pred časom ustanovili konzorcij EMVCo LLC, da bi upravljali, vzdrževali in nadgradili standard EMV za zagotavljanje združljivosti plačilnih sistemov, ki temeljijo na plačilnih karticah z vgrajenim čipom (angl. *Intergrated Circuit Cards* – ICC). Zaradi večje procesorske zmogljivosti in posledično hitrejše obdelave podatkov pravimo omenjenim čip karticam tudi pametne kartice. Danes konzorcij EMVCo LLC zaradi lastniških sprememb vodijo JCB International, MasterCard Worldwide in Visa (A guide to EMV, 2012).

Organizacija EMVCo je do danes izdala več različic standarda EMV, ki zagotavlja povezljivost kartic s čipom in naprav na fizični, podatkovni, električni in programski ravni ne glede na mesto uporabe, finančne ustanove ali proizvajalca.

EMV standard je nastal leta 1993 kot rezultat skupnega dela vodilnih plačilnih institucij; Europaya, Mastercarda in Vise, po katerem je standard tudi dobil ime. Glavni cilj konzorcija je bil definirati skupek standardov za plačilne aplikacije, ki bodo temeljile na pametnih karticah. Ti standardi omogočajo varno komunikacijo med karticami in bralnimi enotami CAD terminali (angl. *Card Acceptance Device*) in predpisujejo načine medsebojne komunikacije (A guide to EMV, 2012):

- Pametne kartice in terminali (bančni avtomati, EFTPOS plačilni terminali, PC čitalniki) morajo znati komunicirati po standardnih platformah.
- Način komunikacije pametne kartice in terminala mora ustrezati minimalnim varnostnim zahtevam.
- Pametne kartice morajo biti interoperabilne in kompatibilne povsod po svetu.

Tako kot na drugih tehničnih področjih tudi za pametne kartice obstajajo standardi, ki opisujejo njihove lastnosti. Pomanjkanje standardov na začetku razvoja se odraža predvsem v nezdružljivosti kartic in terminalov posameznih proizvajalcev, vendar se stanje zadnja leta izboljšuje (Smart Card Alliance Financial Resources, 2012):

Najpomembnejši standardi, ki so povezani s pametnimi karticami:

- ANSI X9: Skupina standardov, ki opisuje kriptografijo z javnimi ključi v finančni industriji. Izdal jih je American National Standard Institute, najpomembnejši med njimi pa so X9.30-2, opis zgoščevalne funkcije SHA-1(angl. *Secure Hash Algorithm*), X9.62 ECDSA (angl. *The Elliptic Curve Digital Signature Algorithm*) in X9.63 (angl. *Eliptic Curve Key Agreement and Transport Protocols*).
- ISO 7810: Opisuje najpomembnejše fizične lastnosti identifikacijskih kartic brez čipa, med drugim tudi velikost kartic.
- ISO 7811: Opisuje postopke zapisovanja podatkov na magnetni trak kartice.
- GSM 11.11: Global System for Mobile Communications, ki vsebuje popoln opis vmesnika med pametno kartico in mobilnim aparatom. Vključuje tudi opis velikosti pametne kartice ter položaj kontaktov, podatkovne strukture in električne karakteristike pametne kartice.
- ISO 10536: Standard za brezkontaktne pametne kartice z dometom do 10 cm.
- ISO 14443: Standard za brezkontaktne pametne kartice z dometom več kot 10 cm.
- ISO 7816: Standard za kontaktne pametne kartice. V standardu je določen položaj čipa in kontaktov ter opis protokolov in ukazov.
- ISO 13491: Standard opisuje koncepte in ocenjevalne metode za varne kriptografske naprave v bančništvu.
- ISO 9798: Standard opisuje kriptografske postopke za preverjanje istovetnosti.
- ISO 10373: Standard opisuje metode za preizkušanje magnetnih, optičnih kontaktnih in brezkontaktnih kartic.
- SET: Secure Electronic Transaction – Skupina standardov za plačila s plačilnimi karticami prek omrežja s številko kartice. SET so skupno razvili CyberCash, GTE, IBM, MasterCard, Microsoft, Netscape in Visa.

- Javacard: Industrijski standard, ki je osnova za Javo na pametnih karticah. Objavilo ga je podjetje Sun Microsystems.
- IEEE P1363: Standard za javno kriptografijo.
- PKCS 11: Mednarodni standard za API, ki uporablja kriptografske funkcije. API se imenuje Cryptoki, vsebuje pa funkcije, kot so RC2, RC4, RC5, MD5, SHA-1, DES, 3DES, IDEA, RSA, DSA.
- EMV: Skupina standardov, ki so jih razvili mednarodni kartični sistemi Europay, MasterCard in Visa, opisuje čipne pametne kartice za uporabo v sistemih plačilnih kartic. Napisani so tako, da omogočajo uporabo kartic različnih bank na istem bankomatu, ne da bi morala banka pri tem razkriti interni sistem plačevanja.

EMV tehnične zahteve temeljijo na ISO standardu, standardu za mikroprocesorske čipe, kartice in terminale. Specifikacije EMV standarda spadajo v podsklop ISO 7816 standarda in so izdane v štirih knjigah (A guide to EMV, 2012):

1. knjiga: Zahteve za uporabo neodvisnega vmesnika med ICC in terminalom (Application Independent ICC to Terminal Interface Requirement)
2. knjiga: Upravljanje s ključem in varnostjo (Security and Key Management)
3. knjiga: Specifikacije za programsko opremo (Application Specification)
4. knjiga: Zahteve za vmesnike lastnikov kartic bančnih posrednikov in prejemnikov plačil (Cardholder, Attendant and Acquirer Interface Requirements)

Zadnja verzija standarda EMV 4.3 je bila izdana novembra 2011.

2.4.2 SEPA in EMV

Evropa je po uvedbi enotne valute evra vstopila v novo fazo usklajevanj. Evropska komisija je od bank zahtevala, da oblikujejo enoten evropski plačilni sistem, ki bo postopoma zamenjal posamezne nacionalne plačilne sisteme. Pred uvedbo enotnega sistema so se načini elektronskih plačil med evropskimi državami razlikovali – vsaka država je imela pri tem svoje specifične navade, zakonodajo in menjalne okvire. SEPA je angleška kratica za enotno območje plačil v evrih. Območje SEPA vključuje 13 držav evroobmočja, 14 preostalih držav EU, Islandijo, Norveško, Liechtenstein, Švico in devet območij, ki so pod upravo držav EU. Na tem območju lahko potrošniki, gospodarske družbe in drugi uporabniki plačilnih storitev plačujejo in sprejemajo plačila v evrih pod enakimi osnovnimi pogoji, z enakimi pravicami in obveznostmi tako znotraj posamezne države EU kot med državami EU.

Pravila in standardi SEPA (sheme) ne pomenijo le izboljšanja učinkovitosti in standardizacije čezmejnega plačilnega prometa, temveč posegajo tudi na področje plačilnega prometa v evrih znotraj nacionalnih meja. Popolna uveljavitev plačilnih shem SEPA pomeni uskladitev tako enega kot drugega z enakimi podlagami, standardi in

postopki izvršitve ne glede na to, prek katere plačilne infrastrukture se takšna plačila izvajajo in ne glede na to, v kateri državi znotraj območja SEPA ima stranka transakcijski račun oziroma prek katerega izvajalca opravlja plačilni promet (SEPA, 2011).

Na področju kartičnega poslovanja v območju SEPA pa lahko posamezniki s karticami plačujejo v celotnem območju SEPA in pri večini trgovskih družb, in sicer z enako stopnjo varnosti, kot jo predpisuje sedanji standard EMV. Temeljna zahteva SEPA na področju kartičnega poslovanja je vzpostavitev poslovanja po načelih čipne tehnologije. Ta tehnologija zagotavlja večjo varnost pri izvajanju transakcij in večjo zaščito pred morebitnimi zlorabami ter pomeni nadgradnjo klasičnih kartic. To pomeni, da bodo podatki o imetnikih kartice poleg magnetnega zapisa zapisani tudi na čipu, ki bo postopoma vgrajen na vse plačilne kartice, ki se bodo uporabljale v območju SEPA. S tem bo poslovanje prek kartičnega čipa postalo standard vse Evrope, vseh izdanih kartic, POS terminalov in bankomatov.

SEPA je na kartičnem področju nadalje zahtevala:

- EMV čipna tehnologija (čip) je morala biti na vseh karticah, POS terminalih in bankomatih nameščena do 1. januarja 2011;
- transakcije s kartico so se morale najkasneje po 1. januarju 2011 izvajati le ob uporabi PIN številke, to pomeni, da se bo nakup s kartico potrjeval le še z vnosom PIN številke, podpis kot avtorizacijski element pa bo izginil. Posledično bodo tudi kartice, skladne s SEPA, opremljene le s čipom, magnetna steza pa bo s kartic počasi izginila (Združenje bank Slovenije, 2007).

2.4.3 Večfunkcionalnost EMV tehnologije

Glavni namen doseganja večfunkcionalnosti je vzpostavitev globalne kartične sheme, ki omogoča, da naša kartica deluje ne glede na geografske meje ter doseganje zadostnega nivoja varnosti. Večfunkcionalnost zajema še dva pomembna vidika. Z vidika proizvajalca kartične infrastrukture to pomeni, da njihova naprava lahko procesira kartice različnih kartičnih shem. Izdajatelj kartice pa pričakuje, da bo njegova kartica delovala na kateremkoli prodajnem mestu ali čitalcu po svetu, ki je opremljen z logotipom blagovne znamke kartice, ne glede na vrsto kartice in tehnologijo sprejemnih naprav – terminalov. Tako plačevanje vključuje čezmejne transakcije, zato mora kartica delovati po vsem svetu, pri tem pa morajo biti zagotovljene varnost, priročnost in preprostost za imetnika plačilne kartice, tako kot je vajen v domačem okolju (Smart Card Alliance Financial Resources, 2012). Za čipne plačilne kartice velja enaka predanost standardom, kot so jo izdajatelji kartic ter izdelovalci kartične opreme dosegli že z globalno večfunkcionalnostjo pri karticah z magnetnim trakom, ko so razvili in začeli uporabljati industrijske standarde. Za nadaljevanje večfunkcionalnosti na čipnih karticah je potrebna enaka zavezanost standardom.

EMV-standard dosega večfunkcionalnost med kartico in sprejemno napravo skozi dva mehanizma. Prvi opredeljuje minimalne zahteve, ki jih morata imeti čipna kartica in sprejemna naprava, da lahko med seboj komunicirata. Te zahteve zagotavljajo, da sprejemna naprava ne poškoduje kartice. Imenujemo jih skupek procedur EMV Level 1. Skupek nadaljnjih procedur se imenuje EMV Level 2 in opredeljuje, kako se bo transakcija na kartici izvedla, ko se opravi fizični stik med čipom kartice in sprejemno napravo. Oba skupka procedur, tako EMV-Level 1 kot EMV-Level 2, morata biti zagotovljena, če želimo ohraniti raven večfunkcionalnosti, medtem ko prehajamo s kartic z magnetnim trakom na kartice s čipi (A guide to EMV, 2012).

2.4.3.1 Zahteve EMV Level 1:

Prva stopnja EMV-standarda zagotavlja osnovne zahteve za vse čipne kartice, vključno s fizičnimi in elektromehanskimi karakteristikami, logičnimi vmesniki in prenosniškimi protokoli za zagotavljanje osnovne večfunkcionalnosti. Definira se osnovne elemente, ki omogočajo čipnim karticam in sprejemnim napravam, da komunicirajo med seboj. To pomeni, da morata biti kartica in sprejemna naprava zmožni fizične povezave in morata zagotoviti prenos informacij. Kartica mora ustrezati specifikacijam, kot so velikosti in oblika kartice, pozicija čipa na kartici, kontakti čipa pa morajo biti postavljeni v skladu z EMV-specifikacijami. Sprejemna naprava mora imeti odprtino za kartico ustreznih dimenzij (tako da kartica lepo sede v ležišče sprejemne naprave), kontakti za branje s čipa pa morajo biti usklajeni s kontakti na kartici, da omogočajo dober fizični kontakt med samo napravo in kartico. EMV Level 1 prav tako določa, na kakšni napetosti deluje interakcija med sprejemno napravo in čipom na kartici za nemoten ter varen prenos podatkov. Druge zahteve EMV Level 1 vsebujejo definicijo komunikacijskih protokolov za prenašanje podatkov med čipno kartico in sprejemno napravo, kot so zaporedje, v katerem so poslani znaki, hitrost prenosa podatkov in število znakov, poslanih v časovni enoti (A guide to EMV, 2012).

2.4.3.2 Zahteve EMV Level 2:

Priporočila EMV Level 2 opredeljujejo specifikacije za izvršitev funkcij, povezanih z debetnimi transakcijami in tistimi z odloženim plačilom. Med vključene funkcije štejemo izbiro aplikacije (debetno ali z odlogom plačila), individualne podatkovne elemente, ukaze in varnost. Po vzpostavitvi povezave med kartico in sprejemno napravo EMV Level 2 ob upoštevanju EMV Level 1 specificira mehanizme, ki dovolijo kartici in sprejemni napravi, da ugotovita, ali se komunikacija lahko nadaljuje. Sprejemna naprava pridobi informacije s kartice, katere aplikacije so na njej. Če čip omogoča več aplikacij in sprejemna naprava omogoča njihovo prepoznavo, je možna izbira določene aplikacije (npr. posojilna funkcija plačila nakupa, takojšnja bremenitev računa ipd.). Izbiro odločitve imenujemo izbira

aplikacije. Konkretneje, imetnik kartice vstavi čipno kartico v sprejemno napravo, sprejemna naprava prek vseh svojih notranjih postopkov prikaže imetniku kartice možne aplikacije, ki so skupne čipni kartici in sprejemni napravi (debetna z odlogom plačila – do meseca dni ali na obroke na podlagi posojila, bonitetna shema ipd.) ter omogoča imetniku kartice, da sam izbere želeno aplikacijo (A guide to EMV, 2012).

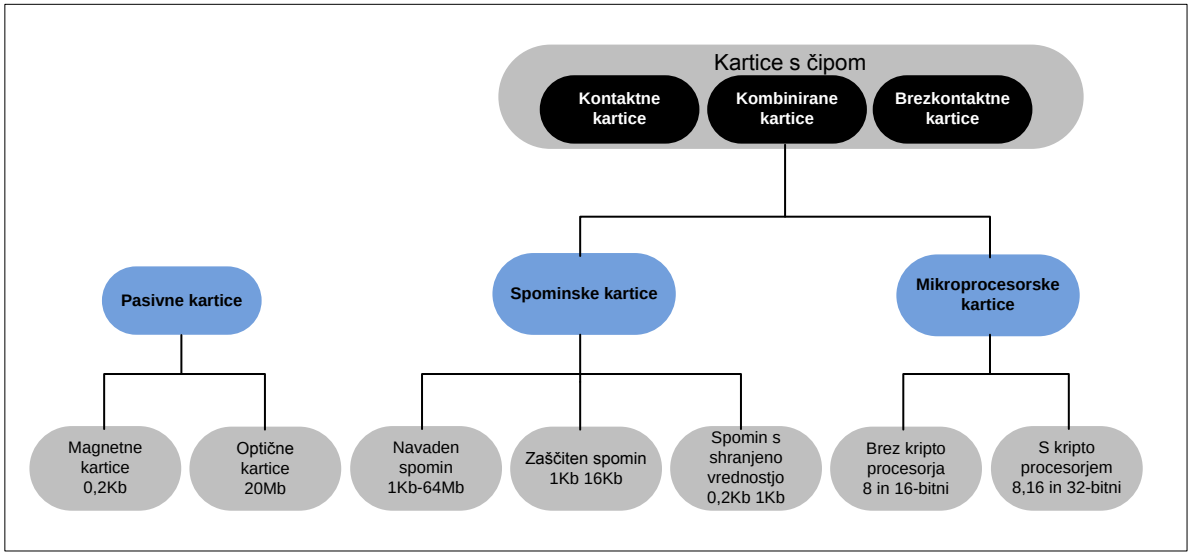
2.4.4 Klasifikacija in primerjava pametnih kartic

V splošnem lahko danes na karticah zasledimo več mehanizmov hranjenja in dostopa do podatkov:

- »mehanske«,
- magnetne ali optične in
- kartice s čipom.

V prvem primeru je nosilec podatka nazobčana površina. Magnetne kartice ponujajo shrambo podatkov s pomočjo magnetenja magnetnega traku, kartice s čipom pa ponujajo pravi računalniški dostop do podatkov. Procesorje za pametne kartice izdelujejo tako rekoč vsi pomembnejši proizvajalci namenskih integriranih vezij (NEC, Samsung, Hitachi, Infeon, Philips …). Danes ti procesorji delujejo s frekvencami tja do 40 MHz, na voljo imajo do 5 kB delovnega pomnilnika, 136 KB bralnega pomnilnika in 32 kB trajnega pomnilnika. Zagotavljajo elektronsko podpisovanje in varnost, kot je določena z množico kriptografskih algoritmov, ki smo jih spoznali v prejšnjem poglavju o kriptografiji. Operacije so dokaj hitre, velikostnega reda nekaj ms (Smart Cards, 2011).

Slika 15: Klasifikacija spominskih kartic in kartic s čipom



Vir: Typs of Smart Cards, 2012.

2.4.4.1 Kartice s čipom

Pomnilniške kartice zaznamuje neprisotnost lastnega procesorja in s tem nezmožnost obdelave podatkov. Kartice z navadnim pomnilnikom so namenjene zgolj shranjevanju podatkov. Pojavljajo se lahko tudi kot kartice s čipom in pomnilnikom EEPROM ali v obliki kartic s pomnilniki flash. Kartice z zaščitenim pomnilnikom imajo vgrajena preprosta logična vezja, ki nadzirajo dostop do podatkov. Uporabne so tam, kjer visoka varnost ni zelo pomemben kriterij; denimo pri raznih karticah ugodnosti, varovanih s PIN kodo. Kartice s shranjeno vrednostjo so namenjene shranjevanju vrednosti za enkratno ali večkratno uporabo. Tipičen predstavnik so kartice v telefoniji, darilne kartice itd.

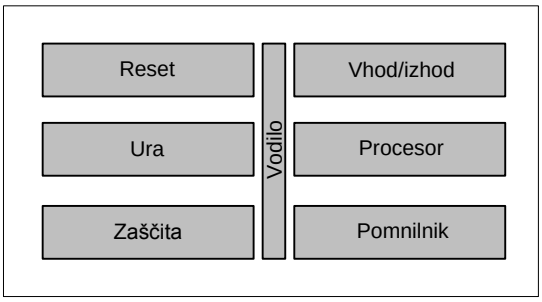
Mikroprocesorske kartice ali pametne kartice so sposobne dinamične obdelave podatkov. Brezkontaktne kartice se od kontaktnih razlikujejo le v načinu prenosa podatkov med čitalnikom in kartico. Pri brezkontaktnih karticah ima antena v kartici obliko tuljave. Skupaj z integriranim vezjem je lahko zalita v kartice, gumbe, obeske, ključe, ure in podobno, saj stroga kartična oblika ni več potrebna. Te kartice prejmejo potrebno energijo za delovanje iz elektromagnetnega polja čitalnika. Takšna »kartica« je zelo robustna in ima zelo dolgo življenjsko dobo. Glede na razdaljo branja jih ločimo na kartice, sposobne komunikacije na razdalji (ISO 7816-4, 2011):

- do 2 cm (še vedno potrebujemo neke vrste režni čitalnik),
- 2 do 15 cm (tukaj lahko kartico identificiramo že med približevanjem),
- do 1 m (uporabno za prenašanje v žepih in podobno) ter
- večje razdalje (uporabno za aktivne kartice – z vgrajeno baterijo življenjske dobe 3–10 let).

Kot je že bilo omenjeno, je pametna kartica popolnoma pravi kartični računalnik. Po obliki in mehanskih lastnostih so pametne kartice enake spominskim, razlika je le v kompleksnosti integriranega vezja. Zgradbo pametne kartice narekuje danes najbolj uveljavljen Von Neumannov model računalnika. Kartice vsebujejo procesor, vhodno-izhodno enoto ter več vrst pomnilnika. Trenutno se uporabljajo 8-, 16- in 32-bitni procesorji, v povprečju imajo 64 kB ROM-a, 16 do 32 kB EEPROM-a ter 3 kB RAM-a, vhodno-izhodna enota pa dosega prenose 9,6–115 kB na sekundo (pri čemer je možen samo polovični – dupleksni – način). Po računski moči so primerljive s prvotnim računalnikom IBM-XT, kartice s kripto-soprocesorjem pa v nekaterih opravilih prekašajo celo 50 MHz računalnik 486. Čas vpisovanja enega bita informacije v posamezno celico znaša za RAM 70 ns, za EEPROM pa 3–10 ms. Celice ROM lahko samo beremo. Večina proizvajalcev zagotavlja shranjevanje podatkov v EEPROM-u do 10 let. Po tem času se zaradi zgradbe EEPROM celice lahko zgodi, da le-ta ne shrani več vrednosti, ki je bila vanjo vpisana. Zato moramo podatke obnavljati, če jih potrebujemo več kakor 10 let. Mnogo današnjih mikroprocesorskih kartic ima kripto-soprocesor. Zmožne so generiranja in preverjanja digitalnih podpisov ter šifriranja podatkov s simetričnim ključem. Podatki so organizirani v datotečnem sistemu, do katerega ima procesor dostop s kartičnim

operacijskim sistemom (COS). Uporabljajo se v telefonih GSM (kartica SIM), za avtentikacijo, shranjevanje občutljivih podatkov (npr. zasebnih ključev, certifikatov). Blokovno predstavo logične zgradbe vidimo na Sliki 16.

Slika 16: Logična zgradba pametne kartice



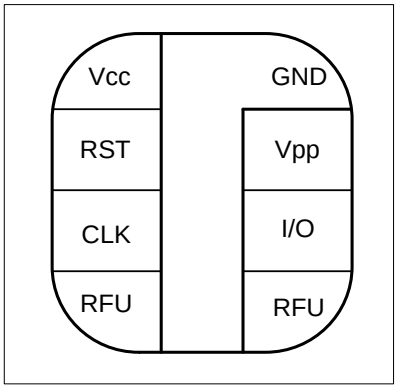
Vir: Smart Cards, 2012.

Vhodno-izhodne enote berejo in pišejo podatke v pomnilniku s pomočjo centralne procesne enote, ki zagotavlja ustrezno varnost. Na vodilo so poleg tega povezani še poseben modul za zaščito, urin signal in signal za reset. Takšno zgradbo, ki potrebuje samo 8 kontaktov, predpisuje standard ISO 7810 (ISO 7816-4, 2011).

Pomnilnik v pametni kartici je razdeljen na tri dele:

- samo bralni pomnilnik (ROM, OTP ali FLASH),
- trajni bralno-pisalni pomnilnik (EEPROM ali FRAM) in
- delovni pomnilnik SRAM.

Slika 17: Kontaktna površina pametne kartice



Vir: Smart Cards, 2012.

2.4.4.2 Integracija kartičnih operacijskih sistemov

Kot pri večini računalniških komponent je tudi pri pametnih karticah osnova programske opreme operacijski sistem. V praksi obstajata dve vrsti kartičnih operacijskih sistemov:

- fiksne datotečne strukture in
- dinamično aplikacijski operacijski sistem.

Izbira operacijskega sistema, ki bo osnova uporabniškim aplikacijam, je odvisna od tipa kartice in samega namena uporabe kartice. Izbira tipa operacijskega sistema je odvisna tudi od potrebe po kriptografskih sposobnostih kartičnih čipov. V primeru, da bo ena izmed funkcij pametne kartice tudi hramba digitalnega potrdila, mora čip na kartici vsebovati tudi tako imenovani kripto modul. Kripto modul omogoča generiranje privatnega ključa na kartico in varno hrambo le-tega. Glede na potrebe šifrirnih algoritmov morajo biti v čip arhitekturi zajete tudi ustrezne knjižnice (PKCS#11).

Pametne kartice s prednaloženim operacijskim sistemom fiksnih datotečnih struktur predstavljajo varno računalniško komponento, ki je predvsem namenjena shranjevanju podatkov. Podatki in pravice dostopa do teh podatkov so navadno delegirane že s strani proizvajalca pametnih kartic. Ta tip operacijskih sistemov je primeren v okoljih, kjer se podatkovne strukture in funkcionalnost programske opreme na krajši rok ne spreminjajo. Najpogosteje se tak tip funkcionalnosti uporablja v zdravstvu za shranjevanje zdravstvenih kartonov, za shranjevanje biometričnih osebnih podatkov, ki so namenjeni avtentikaciji uporabnikov v različne sisteme ipd. V svetu je v uporabi omenjeni tip pametnih kartic najbolj pogost (Smart Cards, 2011).

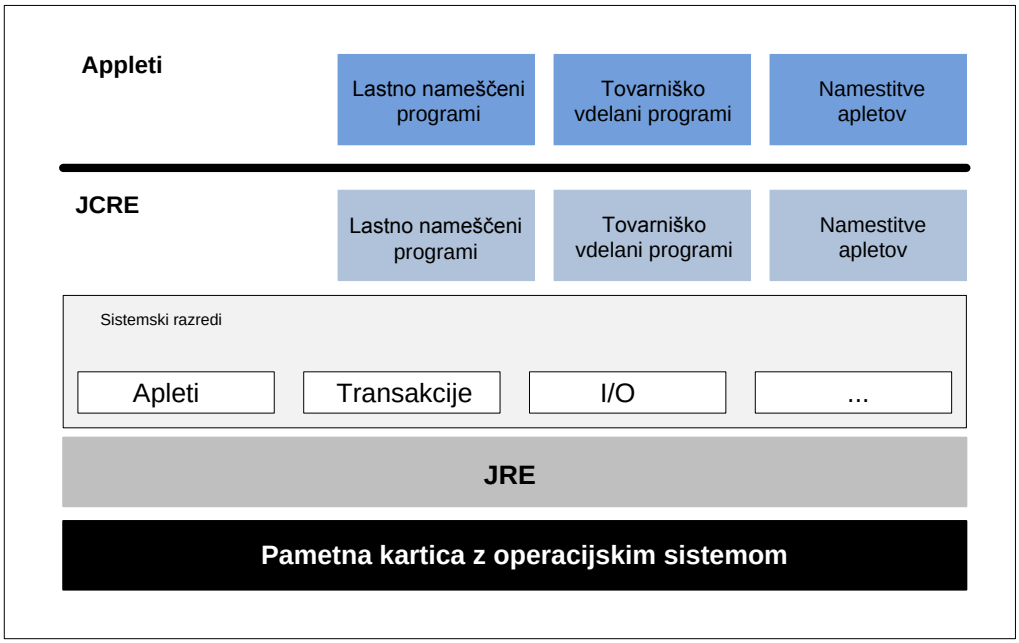
Dinamično aplikacijski operacijski sistemi pa vključujejo JavaCard in MULTOS[7] razvojna okolja, ki razvijalcem omogočata razvoj, testiranje in nameščanje različnih uporabniških aplikacij na mikroprocesorske čipe pametnih kartic. Ker so aplikacije in kartični operacijski sistemi ločeni, se lahko aplikacije posodabljajo dinamično brez globljega posega v prednaložen sistem proizvajalca. Lep primer take arhitekture so SIM kartice za GSM mobilne aparate, kjer se podatki med kartico in telefonskim aparatom pretakajo dinamično in zelo pogosto. Ta vrsta pametnih kartic predvideva nenehno posodabljanje in prilagajanje aplikacij, kar pomeni, da mora biti čip kot strojna oprema dimenzionirana in nagnjena k hitri rasti potreb po sistemskih zmogljivostih. Trenutno sta glavna standarda, ki opredeljujeta kartične operacijske sisteme JavaCard in MULTOS. JavaCard podpira Visa, MULTOS pa je podprt s strani MasterCard-a. V začetku je bila platforma JavaCard razvita kot posledica vse hitrejšega razvoja Java aplikacij, medtem ko je bil MULTOS razvit kot operacijski sistem za elektronske blagajne, temeljil pa je na visoki varnosti finančnih transakcij. Leta 2004 je standard OSCIE potrdil kot možnost za dizajniranje arhitekture pametnih kartic samo JavaCard in MULTOS (Smart Cards, 2011).

[7] MULTOS je vodilni proizvajalec rešitev za operacijske sisteme pametnih kartic.

2.4.4.3 JavaCard tehnologije

S pomočjo tehnologije JavaCard je možno pisati lastne programe, ki tečejo na pametnih karticah. Za kaj takega so potrebni definirani vmesniki za razvoj takšnih programov. Široko uporabnost zagotavlja podpora mednarodnim standardom (denimo ISO 7816) kot tudi širše priznanim industrijskim standardom (denimo Europay/Master Card/Visa – EMV in PKI – standard za identifikacijo z elektronskim podpisom). Za razvoj JavaCard aplikacij ne potrebujemo posebnih orodij, samo prevajalnik, ki razredne datoteke (.class) prevede v ustrezno prilagojene razredne datoteke, ki so pripravljene za izvajanje na pametni kartici. Ustrezna tehnologija je na voljo tudi za razvoj aplikacij na strani čitalnika: tam uporabimo OpenCard Framework. Na Sliki 18 vidimo podrobnejšo logično zgradbo izvajalnega okolja JavaCard (JavaCard Technology, 2011).

Slika 18: JavaCard okolje



Vir: JavaCard Technology, 2011.

2.4.4.4 MULTOS OS

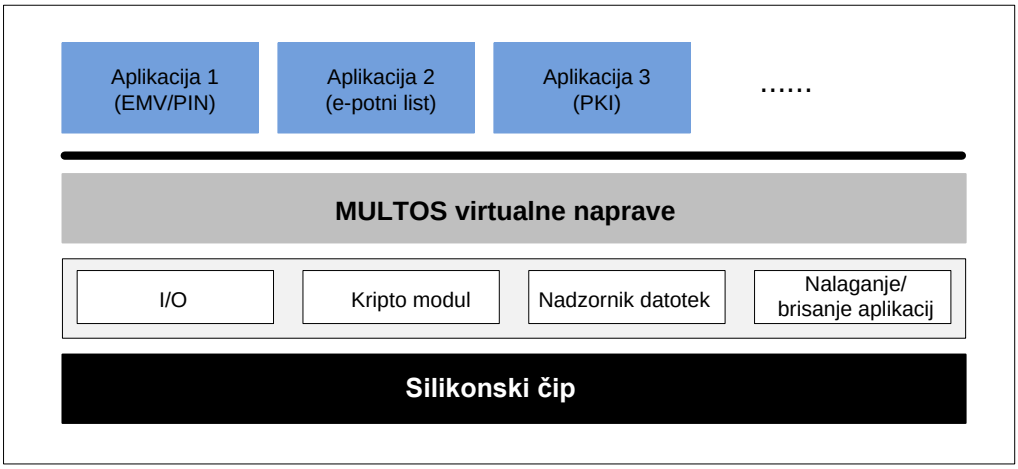
MULTOS je večaplikativni kartični operacijski sistem, ki omogoča pametnim karticam izvajanje več aplikacij. V mislih imamo seveda čip&PIN aplikacijo za izvajanje avtentikacije pri elektronskem bančništvu, kripto modul za prevzem digitalnega potrdila, aplikacijo za ujemanje biometričnih podatkov za secure ID in e-potni list, aplikacijo za plačevanje javnega prometa in druge podobne aplikacije.

MULTOS je odprti standard, katerega razvoj nadzoruje konzorcij MULTOS. Konzorcij MULTOS sestavljajo podjetja, ki jim je v interesu izboljšati kartični operacijski sistem in s tem razširiti uporabo pametnih kartic. To so podjetja, ki delujejo na področju razvoja shem plačilnih kartic, silicijevih čipov, kartične programske opreme, in razna podjetja, ki nudijo

storitve kartičnega poslovanja. Ena od ključnih razlik od ostalih kartičnih operacijskih sistemov je ta, da MULTOS vzdržuje varno in zaupanja vredno okolje, preko katerega izdajatelj nadzoruje vse izdane kartice in skrbi za njihove posodobitve. Ta nadzor se izvaja z uporabo KMA (angl. *Key Management Authority*) protokola. KMA omogoča izdajateljem kartic posredovanje posodobitev za izdane kartice. Te posodobitve so lahko novi kripto algoritmi, inicializacija-aktivacija kartic za njihovo uporabo, dodeljevanje ali odvzemanje pravic za nameščanje novih aplikacij ... MULTOS implementacija omogoča operacijski sistem, na katerem gostujejo ločene virtualne naprave (MULTOS, 2012). Virtualne naprave pa omogočajo:

- aplikativno delavno okolje,
- upravljanje s spominom in
- nalaganje ter brisanje aplikacij.

Slika 19: MULTOS okolje



Vir: MULTOS, Guide to Generating Application Load Unit, 2012.

Za potrebe kartičnega poslovanja, internetne avtentikacije, izkazovanja identitete z digitalnim potrdilom, e-potnih listov z biometričnimi zapisi, zdravstva in vojske je bilo s strani bank in vladnih organizacij po vsem svetu izdanih že na milijone MULTOS pametnih kartic, število pa še vedno strmo narašča (MULTOS, 2012).

2.4.5 EMV CAP avtorizacija transakcije

Varovalne mehanizme za avtorizacijo transakcij v e-bančništvu lahko delimo glede na število uporabljenih avtorizacijskih faktorjev:

- uporaba enostopenjskega avtorizacijskega faktorja (uveljavitev statičnega ali dinamičnega gesla za izvedbo avtorizacije transakcije),
- uporaba dvostopenjskega avtorizacijskega faktorja (avtorizacijski podatki za izvedbo avtorizacije transakcije so sestavljeni iz dela transakcijskih podatkov in dela

avtorizacijskih podatkov). Opisani postopek (sestavljeni parameter) lahko izvedemo na več načinov:

- za vsako transakcijo se preko neodvisnega kanala končnemu uporabniku s strani banke pošlje SMS z avtorizacijsko kodo,
- končni uporabnik na ločeni, za napadalca nedostopni, napravi (npr. čitalec pametnih kartic, v katerega vstavi bančno kartico) vnese PIN in potrdi znesek transakcije. Naprava iz zneska transakcije in PIN-a generira enolično identifikacijsko številko, ki jo uporabnik vnese v spletno banko.

Bistvena lastnost dvostopenjskih avtorizacijskih faktorjev je, da je vsaka posamezna transakcija predhodno overjena in avtorizirana (npr. z vnosom sestavljenega PIN-a ali digitalnega podpisa transakcije). Druga pomembna lastnost dvostopenjske avtorizacije je, da napadalec zgolj s krajo avtentikacijskih podatkov ne more izvajati plačil, saj je geslo časovno omejeno, poleg tega za izvedbo napada potrebuje še aktivno sejo in elemente avtorizacije. Pri dvojni avtorizaciji gre običajno tudi za več uporabljenih mehanizmov, nekaj, kar uporabnik ve, in nekaj, kar uporabnik ima, torej uporabnik ve svoje PIN geslo in ima svojo bančno EMV kartico (OTP One Time Password, 2012).

V bankah zahodnoevropskih držav so se v zadnjih letih razširile rešitve, ki uporabljajo t. i. EMV CAP (angl. *Chip authentication Program*) tehnologijo. CAP imetnikom kartic s tehnologijo EMV in osebnim čitalnikom kartic omogoča preverjanje verodostojnosti storitev. Čitalnik generira geslo za enkratno uporabo, ki se uporabi za prijavo v elektronsko banko ali za avtorizacijo transakcij elektronskega bančništva. V Evropi so rešitve dobile komercialno ime OTP (angl. *One time password*) generatorji. To so posebne od računalnika neodvisne naprave, v katere uporabnik vstavi EMV čip kartico, na tipkovnici kartičnega bralca pa odtipka PIN geslo. Čitalec generira OTP enkratno geslo, s katerim se uporabnik prijavi v elektronsko banko. Geslo je veljavno samo za enkratno prijavo in je lahko tudi časovno omejeno. V primeru avtorizacije transakcije pa mora uporabnik v čitalec vstaviti kartico, vnesti PIN, nato pa napravo približati dinamični grafiki na zaslonu, ki napravi pošlje informacijo o znesku transakcije. V primeru, da bralci ne podpirajo optičnega odčitavanja, mora uporabnik v čitalec sam vnesti znesek transakcije. V naslednjem koraku čitalec generira OTP enkratno geslo, ki je enolično sestavljeno iz osebnega PIN-a in zneska transakcije. Geslo OTP uporabnik nato vnese v spletno mesto e-banke, ki predstavlja avorizacijsko kodo transakcije (Multi-Factor Authentication, 2012).

2.4.6 Avtorizacija transakcije pri mobilnem e-bančništvu

MasterCard je leta 2009 predstavil inovativno rešitev, t. i. program za preverjanje pristnosti z integriranim vezjem (angl. *Chip Authentication Program* – CAP) na mobilnih telefonih. Rešitev omogoča, da uporabnik na mobilnem telefonu ustvari dinamično geslo (unikatni podpis za vsako transakcijo), ki je sestavljeno iz dela transakcije in PIN-a. Na mobilnih telefonih sta možna dva načina izvedbe. Pri prvi različici se dinamično geslo s pomočjo

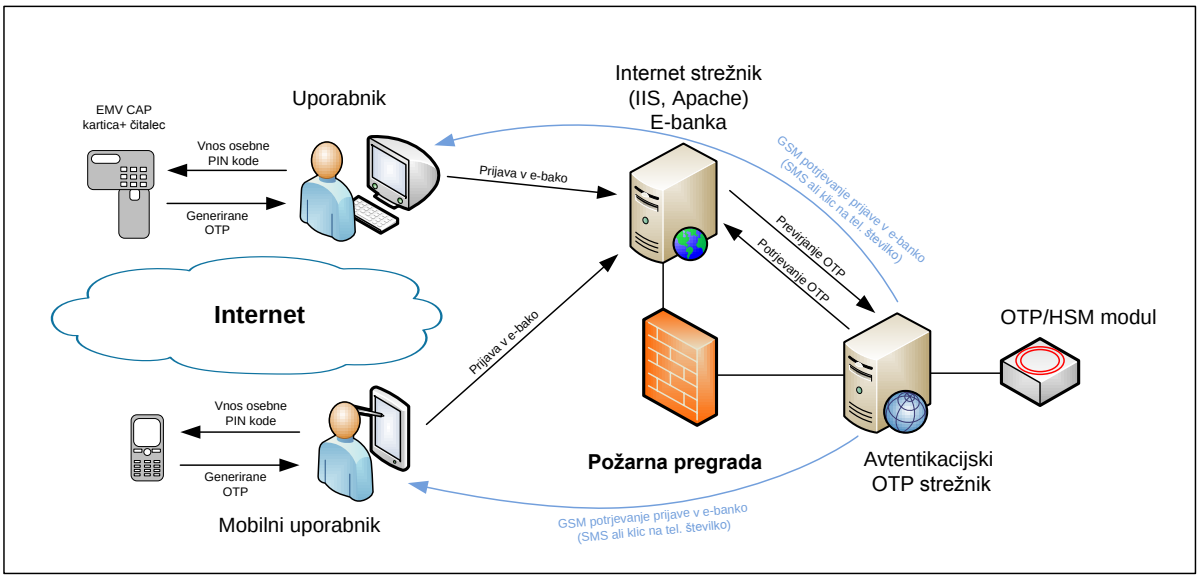
CAP programa generira na strežniku in s sporočilom SMS pošlje imetniku kartice. Imetnik kartice pridobljeno geslo v nadaljevanju uporabi za prijavo v e-banko ali avtorizacijo bančne transakcije. Rešitev SMS-CAP deluje na vseh mobilnih aparatih. Druga različica uporablja program, ki deluje na mobilnem telefonu in od imetnika kartice zahteva vnos osebne identifikacijske številke (PIN). Na zaslonu telefona se nato prikaže CAP geslo, ki ga uporabnik vpiše v aplikacijo mobilne banke. Ta različica deluje le na pametnih telefonih ali telefonih, združljivih s programskim jezikom Java. Postopek za uporabnika je pri tem zelo podoben tistemu pri preverjanju pristnosti s čitalnikom kartic. Ker obe rešitvi temeljita na istih tehnoloških osnovah, lahko banke izberejo, ali želijo uporabljati čitalnike kartic, mobilne telefone ali oboje. Bančni komitent lahko, na primer za preverjanje pristnosti, doma uporablja čitalnik kartic, drugje pa mobilni telefon (Mobile Banking, 2012).

Z uvedeno rešitvijo v igro varnega mobilnega bančništva konkurenčno vstopajo tudi mobilni aparati. Intel je lansko leto oktobra objavil novico, da bo IIPT (angl. *Intel Identity protection technology*) čipe vgrajeval tudi na matične plošče prenosnih računalnikov. Realizacija dvostopenjske avtorizacije transakcije je poleg uvedbe OTP generatorjev (bodisi na EMV CAP bralcu ali mobilnem telefonu), lahko izvedena še z vpeljavo potrditvenega SMS sporočila ali potrditvenega telefonskega klica. Preverjanje transakcije po glasovnem kanalu s klicem na znano telefonsko številko uporabnika (angl. *Out of band - voice channel transaction verification*) zanesljivo ščiti pred MiTB napadi (Mobile Banking, 2012).

2.4.7 Primer avtentikacije/avtorizacije stacionarnih in mobilnih uporabnikov

Kot je bilo rečeno že v prejšnjih poglavjih, je varnostni mehanizem EMV CAP zelo učinkovit pri avtorizacijah uporabnikovih transakcij, dejstvo pa je, da ta mehanizem ni nič manj učinkovit pri avtentikaciji oz. prijavi uporabnika ob vstopu v bančno spletno aplikacijo. Tudi pri avtentikaciji uporabnikov lahko govorimo o dvostopenjski avtentikaciji, kar pomeni, da sta za vstop uporabnika v spletno aplikacijo potrebna dva faktorja. Prvi faktor predstavlja nekaj, kar uporabnik ima (bančna kartica), drugi faktor pa predstavlja nekaj, kar uporabnik ve (osebno PIN geslo). V primeru, da k avtentikaciji in avtorizaciji uporabnika dodamo še preverjanje preko neodvisnega kanala, pa lahko govorimo že o tristopenjskem preverjanju ali večfaktorski avtentikaciji/avtorizaciji uporabnika. V tem dodatnem preverjanju avtentikacijski ali avtorizacijski strežnik ob prijavi ali izvedbi transakcije uporabniku pošlje na GSM številko potrdilo, da se je prijava ali transakcija res zgodila.

Slika 20: EMV CAP arhitektura/avtentikacija ali prijava v e-banko

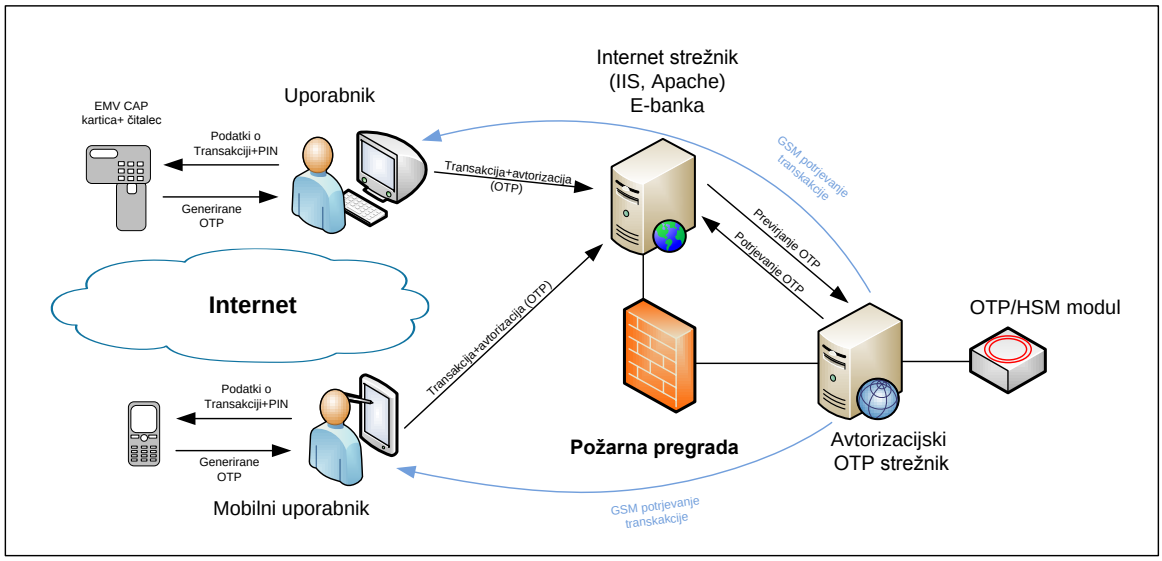


Vir: Multi-Factor Authentication, 2012.

Na Sliki 20 je prikazan postopek prijave uporabnika v spletno banko s pomočjo OTP enkratnega gesla. Prikazana je tako prijava uporabnika, ki se prijavlja z domačo delovno postajo, kot prijava mobilnega uporabnika, ki se prijavlja s pametnim mobilnim telefonom ali tabličnim računalnikom. V prvem primeru uporabnik vstavi pametno kartico v čitalec in vnese osebno geslo PIN. Čitalec generira enkratno geslo, s katerim se uporabnik prijavi v spletno aplikacijo. Na strani banke spletni strežnik prejeto OTP geslo posreduje OTP avtentikacijskemu strežniku, ta pa v svoji bazi, ki je lahko zaradi varnosti shranjena na HSM (angl. *Hardware Security Modul*) modulu preveri ali se OTP geslo res ujema z uporabnikom ali ne. V primeru, da je geslo pravo, avtentikacijski strežnik sporoči bančni aplikaciji, da je uporabnik preverjen in da mu lahko omogoči storitve elektronskega bančništva. V drugem primeru, ko se uporabnik prijavlja v spletno banko z mobilnim telefonom, pa je postopek podoben, le da namesto bralca OTP na podlagi PIN osebnega gesla generira mobilni telefon. Vendar tukaj obstajata dve možnosti. V primeru, da uporabnik uporablja pametni telefon, lahko predhodno nameščena Java aplikacija (Soft OTP token) kar sama generira OTP geslo. V primeru uporabe navadnega telefona pa uporabnik preko npr. tabličnega računalnika odda banki zahtevo za OTP geslo, avtentikacijski/avtorizacijski strežnik pa ga pošlje v obliki SMS sporočila uporabniku.

Pri avtorizaciji uporabnikove transakcije pa je proces identičen, le da mora uporabnik za generiranje enkratnega OTP gesla, s katerim bo potrdil transakcijo, poleg osebnega PIN gesla v čitalec ali mobilni telefon vnesti tudi višino oz. znesek transakcije. Uporabnik želeno transakcijo potrdi z generiranim OTP geslom, na strani banke pa je proces preverjanja povezovanja OTP gesla in uporabnika enak kot pri avtentikaciji uporabnika.

Slika 21: EMV CAP arhitektura/avtorizacija transakcije



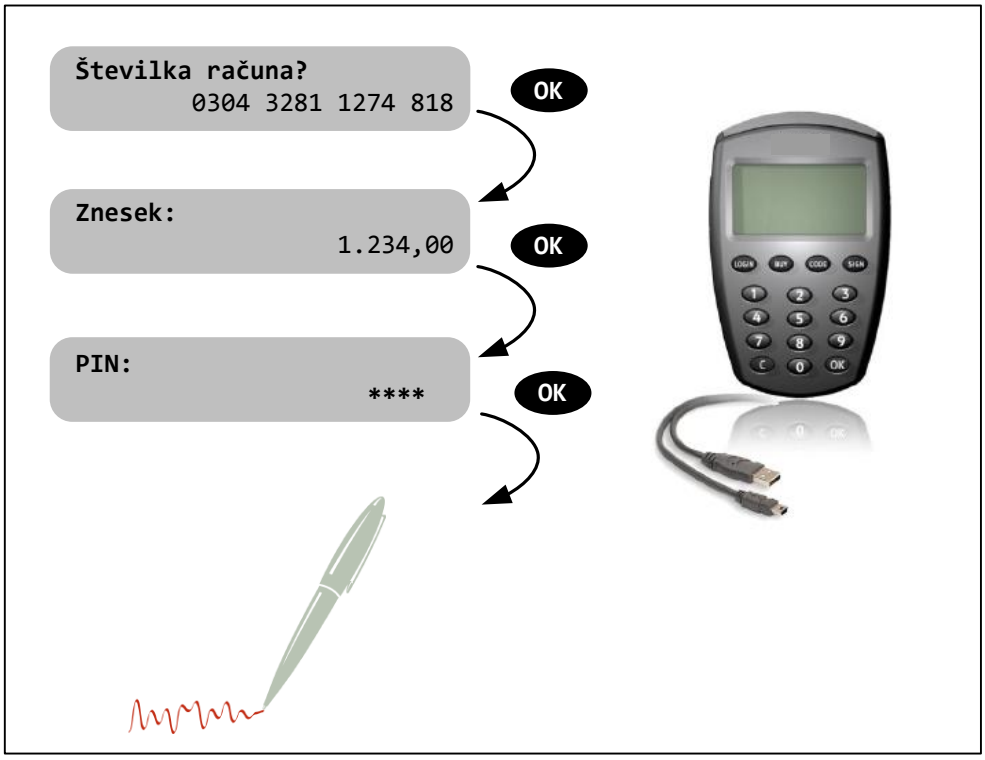
Vir: Multi-Factor Authentication, 2012.

Tretje preverjanje uporabnika po neodvisnem kanalu, SMS sporočilo ali klic na znano GSM številko, pa je tudi enak v obeh primerih, pri avtentikaciji/avtorizaciji, dostopu s stacionarne delovne postaje in mobilnem dostopu.

2.5 Digitalno podpisovanje transakcij v varnem okolju

V prejšnjem poglavju je bil predstavljen varnostni mehanizem elektronskega bančništva, kjer je uporabnik z enkratnim geslom OTP lahko podpisal transakcijo in s tem precej zmanjšal možnost napada na transakcijo oz. poneverbo le-te. Za še bolj varno izvajanje transakcij se je izkazal princip podpisovanja, ki so ga inženirji Nils Gruschka, Florian Reuter in Norbert Luttenberger predstavili avgusta 2004 na konferenci Sixt Smart Card Research and Advanced Application IFIP Conference v Toulouseu. Princip podpisovanja temelji na podpisu XML dokumenta z digitalnim potrdilom v varnem okolju. Varno okolje v tem primeru predstavlja Java pametna kartica, na kateri je varno shranjeno digitalno potrdilo in pa kartični čitalec razreda 3 ali 4, ki premore zaslon za prikazovanje vsebine XML dokumenta, tipkovnico za vnos glavnih parametrov vsebine ter izvedbo digitalnega podpisa. Za razliko od vsem dobro poznanega podpisovanja XML dokumenta, izvedenega v brskalniku ali podobni internetni aplikaciji na računalniku, se podpis in samo preverjanje pomembnih parametrov dokumenta izvede na Java pametni kartici in bralcu, ki pa sta za napadalca nedostopna. V naslednjem koraku je podpisan dokument, na katerem so podatki, na primer višina transakcije, ciljni račun in ostali podatki, poslani e-bančni aplikaciji. (Gruschka, Reuter & Luttenberger, 2004, str. 1–15).

Slika 22: Princip elektronskega podpisa transakcije



Vir:P. Gullberg, Remote Authentication for Everyone Everywhere, 2011.

Omenjeni princip podpisovanja obvaruje bančno transakcijo tako pred MiTM kot MiTB napadom, obenem pa rešuje tudi problem ¨kar je videno je nekaj, kar je podpisano¨ (angl. *What you see is what you sign*).

2.5.1 Digitalno podpisovanje XML dokumenta

Eden glavnih izzivov digitalnega podpisovanja dokumentov je zagotavljanje preverjanja vsebine pred podpisom. Dokument nam napadalec lahko spremeni še po našem pregledu, kar pomeni, da smo podpisali nekaj, ne da bi sploh vedeli, kaj. Takemu primeru rečemo problem ″what you see is what you sign″. XML kot meta kodirani računalniški jezik ponuja nove možnosti za reševanje tega problema. Varnost procesa podpisovanja dokumentov lahko izboljšamo, če zagotovimo možnost preverjanja temeljnih lastnosti kodiranih XML dokumentov, to je formiranost in veljavnost (angl. *well-formed-ness, validity*) dokumenta.

V tem delu naloge bo predstavljena arhitektura, ki omogoča omenjen pregled in elektronski podpis XML dokumenta na Java pametni kartici v ločenem in za napadalce nedostopnem okolju. Omenjena arhitektura je bila uspešno implementirana v mednarodni transakcijski sistem FinTS, ki v celoti temelji na kartičnem elektronskem poslovanju.

Digitalno podpisovanje na pametni kartici je trenutno vrhunec tehnologije, počasi pa prehaja tudi v dobro prakso pri implementacijah bančnih elektronskih plačilnih mehanizmov. Arhitektura je posledica dejstva, da imajo danes pametne kartice dovolj

procesorske moči in spomina za shranjevanje digitalnih potrdil ter generiranje digitalnih podpisov. Način podpisovanja, kjer javni ključ uporabnika nikoli ne zapusti varnega okolja, še dodatno ščiti uporabnika pred zlorabo podpisa. Privatni ključ uporabnika je od generacije na kartico shranjen samo na kartici in ni potrebe, da se ga izvaža na katerikoli drug medij ali nosilec. Vendar, če proces podpisovanja pogledamo bližje, ugotovimo, da nam še vedno ostaja problem znan kot ″what you see is what you sign″. Preden uporabnik elektronsko podpiše XML dokument (transakcijo), želi preveriti formiranost dokumenta in seveda vsebino oz. parametre XML dokumenta.

Če primerjamo digitalni podpis z ročnim podpisom nekega besedila na listu papirja, lahko hitro ugotovimo, da pri podpisu s svinčnikom nimamo takih težav kot pri digitalnem podpisu. Ko besedilo na listu papirja preberemo, preverimo veljavnost in pravilnost vsebine, lahko še istočasno papir podpišemo in smo povsem prepričani, da teksta v tem času, ko smo ga imeli pred očmi in do podpisa ni nihče spreminjal. Povsem drugače pa je pri digitalnem podpisu. Namreč pri tovrstnem podpisu sta preverjanje dokumenta in generiranje podpisa izvedena v dveh povsem ločenih okoljih s povsem različnimi značilnostmi, tako s stališča varnosti kot s stališča virov (procesor, spomin, prikazovalnik vsebine). Pri običajnem elektronskem podpisu aplikacija za podpisovanje iz dokumenta, s pomočjo enosmerne zgoščevalne funkcije (angl. *hash*), zgosti vsebino, nato pa dobljen zgoščen izvleček pošlje pametni kartici. Operacijski sistem čip kartice poskrbi, da se vsebina šifrira s privatnim ključem, shranjenim na čipu kartice. Dobljeni rezultat je digitalni podpis dokumenta, ki je nato spet poslan nazaj aplikaciji za podpisovanje. Uporabnik tako nima možnosti preverjanja sintakse dokumenta (v primeru XML dokumenta: preverjanje formiranosti in veljavnosti) niti pravilnosti ustreznih parametrov. Kar je v resnici podpisano, je skrito uporabnikovim očem in izven njegove kontrole. Tudi če kartica predstavlja varno okolje, je računalnik, in aplikacije na njem, lahko okužen in vsiljivec lahko spremeni dokument, še predno je bil ta podpisan. Podpis je v tem primeru sicer lahko veljaven in nesporen z vidika podpisovalca, vprašanje pa je le, kaj je bilo podpisano.

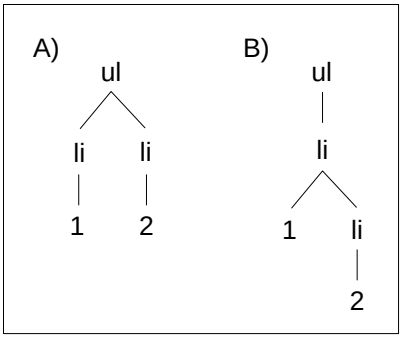
Trojček inženirjev je na konferenci v Toulouseu predstavil rešitev tega problema. Ta problem rešuje tako imenovana JXCS arhitektura. Glavna ideja JXCS arhitekture je premakniti pregledovanje in kodiranje dokumenta z enosmerno zgoščevalno funkcijo iz ranljivega računalniškega okolja na varno okolje Java pametne kartice. Največji izziv pri tem je seveda omejiti možnost procesiranja XML dokumenta na Java pametni kartici. Omenjeni pristop nam omogoča kontroliranje formiranosti in veljavnosti XML dokumenta v varnem okolju, s tem pa precej povečamo varnost v procesu podpisovanja XML dokumenta. Na konferenci je bil predlagan pregled treh lastnosti XML dokumenta pred izvedbo podpisa; formiranost sintakse, veljavnost oz. skladnost dokumenta z zahtevano shemo ter pravilnost vsebine dokumenta. Pregled vseh treh lastnosti dokumenta omogoča kartični čitalec razreda 3 ali 4. S pregledom teh treh lastnosti pred kodiranjem in podpisom

dokumenta pa rešimo tudi prej omenjen problem ″what you see is what you sign″ (Gruschka et al., 2004, str.1–15).

2.5.2 Lastnosti XML dokumenta

XML dokument je dobro formiran takrat, ko so njegovi elementi sintaktično skladni s predpisi XML standarda. Formiranje XML sintakse se torej navezuje na sintakso vsebine, komentarjev, definicije dokumenta itd. Po XML specifikaciji mora biti vsak element dokumenta pregledan in ustrezen standardu. Najpomembnejša omejitev je logična struktura oznak elementov. Oznake morajo biti ustrezno razporejene, kar pomeni, da ima vsak začetni element tudi pripadajoči končni element, ki skupaj tvorita urejeno unikatno drevesno strukturo. Na primer `<a><b>Pozdravljeni</b></a>` je dobro sintaktično formirana vsebina, medtem ko `<a>nasvidenje</c>` in `<a><b>velik</a></b>` nista dobro formirani vsebini (W3C, 2008).

Slika 23: Možne interpretacije slabo formiranega XML dokumenta:
`<ul><li>1<li>2</ul>`



Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15

Dobra formiranost XML dokumenta zagotavlja unikatnost interpretacije XML dokumenta. Zgornji primer slabo formiranega XML dokumenta `<ul><li>1<li>2</ul>` dopušča dve interpretaciji, kot je prikazano na Sliki 22:

- A) `<ul><li>1</li><li>2</li></ul>` in
- B) `<ul><li>1<li>2</li></li></ul>`

V primeru dobre formiranosti dokumenta bi bila interpretacija unikatna.

2.5.2.1 Veljavnost sheme XML dokumenta

Bolj kompleksno v primerjavi s formiranostjo XML dokumenta pa je preverjanje veljavnosti sheme XML dokumenta. Dokument je ocenjen kot veljaven takrat, ko sta veljavni deklaracija ali shema dokumenta. Shemo dokumenta predstavlja nabor slovničnih znakov, ki se preverjajo pri ugotavljanju veljavnosti dokumenta (W3C, 2008).

Nabor znakov, ki se preverjajo, je sledeč G=(∑, D, N, P, n_s), kjer predstavlja:

- ∑ nabor vsote tipov elementov in tipov atributov,
- D nabor vrst podatkov,
- N nabor ne-terminalov,
- P nabor pravil,
- n_s izhodiščni ne-terminal.

V nadaljevanju je prikazan primer sheme FinTS plačilnega mehanizma, ki se preverja pred podpisom dokumenta.

Slika 24: Primer sheme FinTS plačilnega mehanizma

```
<xsd:element name="Amount">
 <xsd:complexType>
  <xsd:sequence>
   <xsd:element name="Value" type="xsd:decimal"/>
   <xsd:element name="Currency" type="xsd:string"/>
  </xsd:sequence>
 </xsd:complexType>
</xsd:element>
```

Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

Forma prikazovanja vrednosti v proučevanem primeru.

Slika 25: Forma prikazovanja vrednosti v primeru FinTS

```
<Amount>
 <Value>100</Value>
 <Currency>Euro</Currency>
</Amount>
```

Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

Nabor znakov v shemi preučevanega primera FinTS je sledeč:

G = (∑, D, N, P, n_s), kjer je:

∑ = {Amount, Value, Currency}
D = {xsd:decimal, xsd:string}
N = {N_1, N_2, N_3}
n_s = N_1
P pa vsebuje sledeča pravila:

- $N_1 \rightarrow$ Amount (N_1, N_2)
- $N_2 \rightarrow$ Value (xsd:decimal)
- $N_3 \rightarrow$ Currency (xsd:string)

W3C XML shema ponuja bogato paleto uporabnih primerov vrednosti, ki pa jih je možno prilagajati še z elementi `<restriction>`,`<union>` in `<list>`. Našteti elementi omogočajo omejevanje vrednosti, ki jih naknadno vnaša uporabnik, v našem primeru npr. `decimal`.

Slika 26: Forma prikazovanja parametrov omejevanja

```
<xsd:element name="Value">
 <xsd:restriction base="xsd:decimal">
  <xsd:maxInclusive value="100"/>
 </xsd:restriction>
</xsd:element>
```

Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

2.5.3 Digitalni podpis XML

Digitalni XML podpis izhaja iz W3C priporočil, bolj natančno, iz področja, ki opredeljuje digitalni podpis formata XML. Področje vsebuje specifikacije zahtevane XML sintakse in procesnih pravil za kreiranje veljavnega XML podpisa (W3C, 2008). V kontekstu JXCS arhitekture je za izvajanje procesa podpisa uporabljena sledeča sintaksa:

Slika 27: Forma digitalnega podpisa

```
<Signature>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    <Reference URI>
      <Transforms></Transforms>
      <DigestMethod/>
      <DigestValue></DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue></SignatureValue>
  <KeyInfo></KeyInfo>
</Signature>
```

Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

XML podpis predstavlja element `Signature`, ki ima formirano strukturo, kot jo prikazuje zgornji del kode. Element `Signature` sestavlja zaporedje treh elementov: `SignedInfo`, `SignatureValue` in `KeyInfo`. Element `SignedInfo` vsebuje zaporedje elementov `Canonicaliza-tionMethod`, `SignatureMethod` in `Ref-erence`. Element `Ref-erence` je kreiran za vsak podpisan objekt (XML dokument ali druge podobne vsebine). Predstavlja povezave na podatkovne objekte, ki so lahko vsebovani v zunanjih dokumentih ali na istem dokumentu kot podpis. Element `Ref-erence` vsebuje tudi kodirano vrednost objekta in zgoščevalni algoritem (`DigestMethod`), s katerim je kodirana določena vsebina XML dokumenta. Elementa `Canonicaliza-tionMethod` in `SignatureMethod` pa sta samostojna podpisna algoritma in sta na voljo za vse podpisane podatkovne objekte v danem `Reference` elementu. Podpisna vrednost, zajeta v elementu `SignatureValue`, uporablja podpisni algoritem in uporabnikov privatni ključ in se nanaša na celoten `SignedInfo` element. Uporabnikov privatni ključ je lahko vključen v `KeyInfo` elementu XML podpisa, ni pa to nujno (Gruschka et al., 2004, str.1–15).

XML podpis je glede na priporočila W3C izračunan v petih korakih:

1) prevajanje dokumenta, ki bo podpisan,
2) izračun izvlečka kanonikaliziranega dokumenta,
3) generiranje `SignedInfo` elementa,
4) izračun podpisne vrednosti,
5) izvedba (`Signature`) podpisa dokumenta.

2.5.4 Vmesniki za procesiranje XML dokumenta

Obstajata dva tipa vmesnikov (API-jev) za procesiranje XML dokumentov. Prvi tip predstavljajo vmesniki, ki temeljijo na drevesni strukturi (angl. *Tree-based APIs*) DOM. Drugi tip pa predstavljajo vmesniki, ki temeljijo na dogodkih (angl. *Event-based APIs*) SAX ali StAX. Prvi tip vmesnikov deluje tako, da celoten XML dokument shrani v glavni pomnilnik, kjer je dostopen kot XML osnova za obdelavo. Te vrste vmesnikov so zelo potratne z vidika sistemskih virov, še posebno takrat, ko je dokument velik. Drugi tip vmesnikov pa deluje tako, da dogodke preko klicev (angl. *callbacks*) razčlenjuje in pripravlja podatke za obdelavo aplikacije. Po navadi te vrste vmesnikov ne gradijo notranje drevesne strukture kot v prvem primeru. Aplikacije razpolagajo z izvajalci, ki skrbijo za izvajane različnih dogodkov, tako kot je to izvedeno pri grafičnih uporabniških vmesnikih. Glede na omejene sistemske vire Java kartice je edina uporabna rešitev Event-based APIs – vmesniki, ki temeljijo na dogodkih. Priporočeni so SAX vmesniki, ki producirajo naslednje elemente (Gruschka et al., 2004, str.1–15):

- begin-element (a),
- end-element (a),
- begin-attribute (a),
- end-attribute (a),
- char-content (c).

Zgornji primer XML dokumenta je sestavljen z naslednjimi dogodki:

- begin-element(Amount),
- begin-element(Value),
- char-content(“100”),
- end-element(Value),
- begin-element(Currency),
- char-content(“EUR”),
- end-element(Currency),
- end-element(Amount).

2.5.5 Prednosti arhitekture JXCS in podpisa XML

Idejo o arhitekturi JXCS, ki so jo inženirji predstavili na konferenci v Toulouseu je možno povzeti v dveh točkah.

1) Če dokument, ki ga nameravamo podpisati, ni dobro formiran v smislu XML sintakse, niti ni skladen z ustrezno shemo ali oboje, potem je to jasen znak, da je bil dokument s strani nepooblaščene osebe prirejen. Tak dokument mora biti zavrnjen, uporabnik pa mora biti o tem na nek način obveščen.

2) Aplikacija na pametni kartici zmore razčlenitve XML dokumenta na posamezne dele tako, da so lahko le-ti v zaporedju prikazani na zaslonu bralca. Razčlenitev in prikaz XML dokumenta sta izvedena na kartici - varnem okolju, v istem okolju pa je izveden tudi digitalni podpis dokumenta.

Temeljna lastnost vsakega XML dokumenta je dobra formiranost sintakse. Edino dobra formiranost predstavlja unikatno interpretacijo XML dokumenta. Glede na zahteve priporočil W3C mora vsaka entiteta, ki tak dokument procesira, predhodno preveriti in zagotoviti dobro formiranost dokumenta. Veliko bolj kritična, v primerjavi s formiranostjo, pa je veljavnost sheme XML dokumenta. Pametna kartica, ki omogoča primerjavo dokumenta z ustrezno shemo, zagotavlja, da bo podpisan le preverjen dokument. Iz varnostnih razlogov pa je dodatno možno omejiti podpis z digitalnim potrdilom na pametni kartici. Privatni ključ digitalnega potrdila je lahko definiran le za podpisovanje dokumenta, ki vključuje shemo za plačevanje računov do določene višine zneska, npr. 150 €. Pri vseh večjih zneskih elektronski podpis XML dokumenta ne bo mogoč. Pri uporabi bralcev razreda 3 ali 4 (bralci, ki vsebujejo zaslon in tipkovnico) lahko aplikacija na pametni kartici izbrani znesek prikaže na zaslonu bralca in od uporabnika zahteva potrditev. Ta proces pa končno reši problem ″what you see is what you sign″ (Gruschka et al., 2004, str.1–15).

Več kot očitno je, da je procesiranje XML dokumenta na pametni kartici z vidika sistemskih virov vse prej kot enostavno. V Tabeli 9 so zbrani izzivi in možne izboljšave XML podpisovanja.

Tabela 9: Izzivi in priložnosti XML podpisa

Izzivi XML podpisa	Priložnost XML podpisa
Preverjanje forme XML sintakse na kartici	Zaupanje, da je bil podpisan le XML dokument
Preverjanje veljavnosti sheme XML na kartici	Zaupanje, da je bil podpisan le dokument tega tipa
Preverjanje vnesenih vrednosti	Zaupanje, da so bile vrednosti podpisanega dokumenta pod določeno mejo (višina transakcije)
Prikaz izbranih vrednosti na prikazovalniku bralca	Zaupanje, da tudi nepooblaščeno prirejen dokument ne bo naredil škode

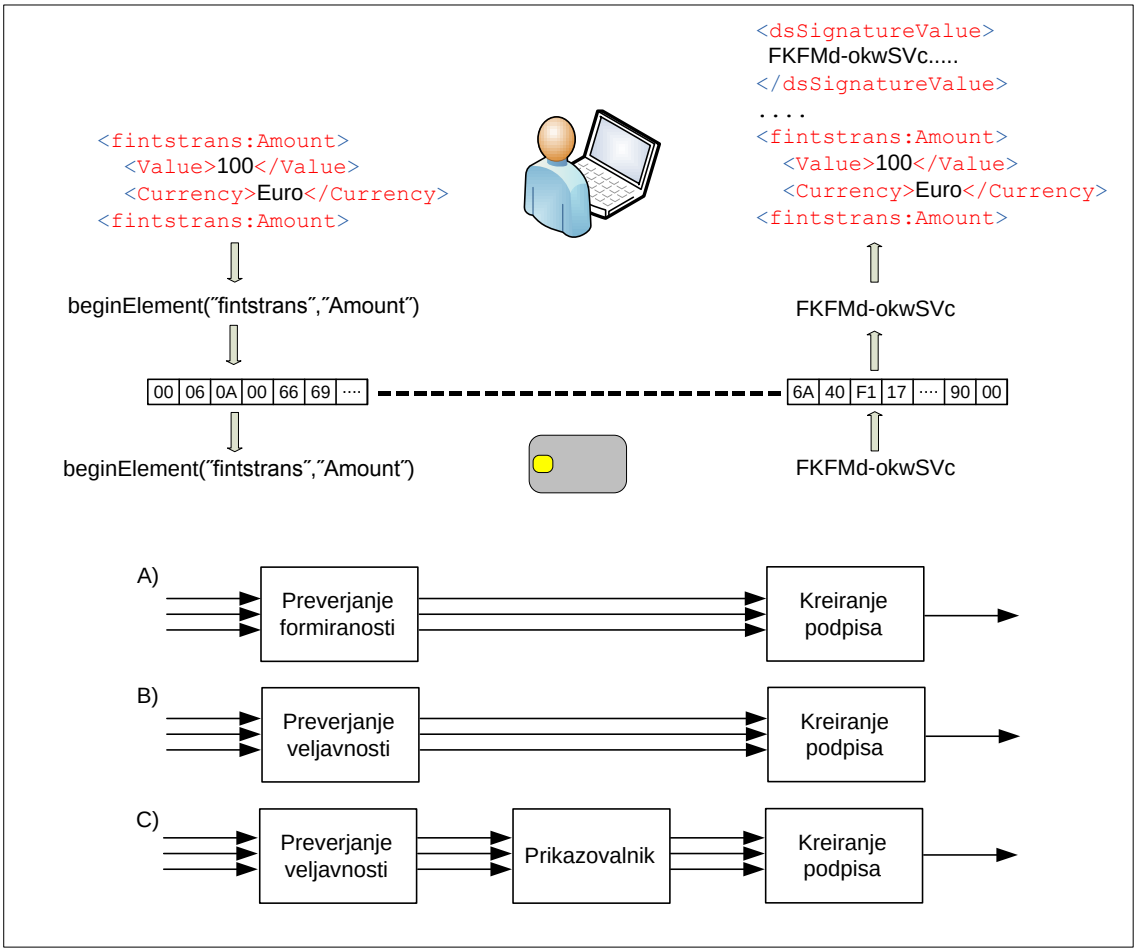
Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

2.5.6 Arhitektura JXCS

Značilnost JXCS arhitekture je, da se vsi kritični postopki z vidika varnosti izvedejo v varnem okolju − pametni kartici − vključno s:

- preverjanjem formiranosti in veljavnosti dokumenta,
- kanonikalizacijo in zgoščevanjem dokumenta ter
- izračunom podpisne vrednosti.

Slika 28: JXCS arhitektura



Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

Slika 24 prikazuje primer JXCS arhitekture. Kartični čitalec poganja XML prevajalnik, ki služi za analizo XML dokumenta, ki bo kasneje digitalno podpisan. Prevedena in razčlenjena koda v PDU formatu je nato poslana na čip pametne kartice. Koda je poslana v izvedbeno verigo izvajalcev dogodkov. Ti izvajalci procesirajo celoten XML dokument, dogodek za dogodkom. Veriga vsebuje več različnih izvajalcev glede na specifične zahteve (Slika 24; A, B, C). Po navadi so to izvajalci dogodkov, ki preverjajo formiranost in veljavnost sheme XML dokumenta, in seveda izvajalci, ki kreirajo digitalni podpis. V primeru, da se nek dogodek konča z napako, je proces prekinjen. Ko pa so vsi dogodki v verigi uspešno izvedeni, proces na koncu vrne podpisno vrednost. S to podpisno vrednostjo pa je kreiran digitalni podpis.

2.5.6.1 Izvajalec podpisa

Izvajalec podpisa je namenjen zgoščevanju kanonikaliziranega (prevedenega) dokumenta in izračunu podpisne vrednosti (angl. *SignatureValue*). S tem procesom je kreiran `SignedInfo` element. Za potrebe zgoščevanja izvajalec podpisa sestavi kanonikaliziran dokument, ki ga je prejel od predhodnega dogodka (razčlenjevanje). Prvotne oblike dokumenta pa ni potrebno vračati nazaj na pametno kartico. Omenjen pristop omogoča učinkovito kombinacijo izvedbe obeh dogodkov (preverjanje in podpisovanje XML dokumenta) na pametni kartici.

Tabela 10: Sestavljanje dokumenta iz dogodkov

Dogodki	Parameter1	Parameter2	Kanon. dokument
beginDocument			
beginElement	*name*		*<name*
beginElement	*prefix*	*name*	*<prefix:name*
addNamespace	*uri*		*xmlns=″uri″*
addNamespace	*prefix*	*uri*	*xmlns:prefix=″uri″*
beginAttribute	*name*		*name=″*
beginAttribute	*prefix*	*name*	*prefix:name=″*
endAttribute			*″*
charContente	*data*		*data*
endElement	*name*		*</name>*
endElement	*prefix*	*name*	*</prefix:name>*
endDocument			

Vir: N. Gruschka, F. Reuter & N. Luttenberger, 2004, Checking and signing XML documents on Java smart cards, str. 1-15.

Za vsak sestavljen dokument izvajalec podpisa z zgoščevalnim generatorjem in s pomočjo zgoščevalne funkcije izračuna zgoščenino za vsak kos posebej za celoten dokument. Večina zgoščevalnih algoritmov (kot MD5 ali SHA-1) ne shranjuje celotnih vhodnih podatkov, ampak procesira vhodne podatke blok za blokom, kar pomeni, da generator ne potrebuje velikega spomina za vhodno čakalno vrsto. Način zgoščevanja ″kos za kosom″ je zelo varčen način z vidika sistemskih virov. Ko je dokument v celoti zgoščen in poslan na čip pametne kartice, se sproži dogodek **endDocument**, podpisovalni element pa prične proces podpisovanja (Gruschka et al., 2004, str.1–15).

Podpisovalec je torej namenjen kreiranju `SignedInfo` elementa, ki zajema metodo kanonikalizacije, zgoščevalni algoritem ter podpisovalni algoritem. V nadaljevanju je dokumentu dodana zgoščena vsebina ter `Reference` element. Rezultat `SignedInfo` elementa je šifriranje zgoščenine s privatnim ključem uporabnika, shranjenim na čipu pametne kartice. Dobljena vrednost pa služi za kreiranje XML podpisa.

2.5.7 Čitalci pametnih kartic razreda 3 in 4

Napredni čitalci pametnih kartic z lastnim zaslonom ter numerično tipkovnico (čitalci razreda 3 ali 4) ponujajo možnosti pregledovanja dokumenta pred podpisom. Pri izmenjavi podatkov med čipom kartice in čitalcem, le-teh ni mogoče prestreči, brati in še manj spreminjati. Čitalec tako služi za varen prikaz podatkov, ki so poslani na čip pametne kartice.

Kot je bilo rečeno že v prejšnjih poglavjih, je omenjeni princip, učinkovita rešitev za reševanje problema ″what you see is what you sign″. Namreč pred pošiljanjem dokumenta v podpisovanje na pametno kartico je celoten dokument prikazan na zaslonu čitalca. Navadno so prikazovalniki čitalcev 1- do 3-vrstični in prikazujejo največ 20 znakov v eni vrstici. Zaradi tega se dokument prikazuje po delčkih, eden za drugim, dokler ni prikazan celoten dokument. Prikazovanje samo nekaterih delčkov dokumenta bi bilo nesmiselno, saj ima en sam element lahko čisto drugačen pomen kot pa v kontekstu s spremnim besedilom. Na primer, da uporabnik potrdi `<Amount>1000 EUR</Amount>`, iz samega zneska ne more vedeti, ali za ta znesek kupuje avto ali nakazuje v dobrodelne namene. Poleg prikaza celotnega dokumenta je potrebno XML dokument tudi primerjati z shemo (plačilni obrazec, nakazovanje ...) Šele, ko je shema potrjena, je lahko uporabnik prepričan, da bo znesek `<Amount>1000 EUR</Amount>` res nakazal kamor želi (Gruschka et al., 2004, str.1–15).

Ko je shema dokumenta prenesena na čip pametne kartice, se pomembni elementi (številka tekočega računa, višina transakcije ...) prikažejo na prikazovalniku čitalca, le-ta pa od uporabnika zahteva potrditev. V primeru, da uporabnik enega elementa od prikazane vsebine ne potrdi, je proces podpisovanja prekinjen.

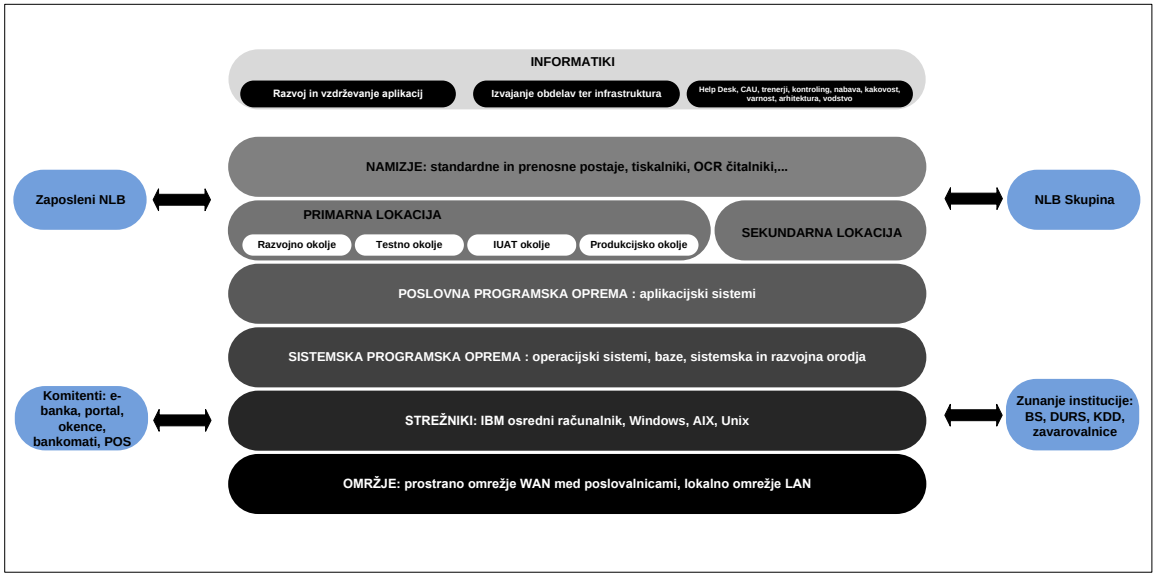
3 ARHITEKTURA INFORMACIJSKEGA SISTEMA V NLB

Arhitekturi informacijskega sistema pogosto rečemo tudi na kratko ″IT (angl. *Information technology*) arhitektura″, ki na splošno pomeni podprtost poslovnih procesov z različnimi elementi informacijske tehnologije, kot so podatki in informacije, aplikacije, strežniki, odjemalci, omrežja, sistemska okolja in orodja. V okviru IS arhitekture NLB obstaja več podsklopov − Slika 25 (NLB, 2012):

- informacijska arhitektura,
- aplikacijska arhitektura,
- tehnološka infrastruktura.

Celotni informacijski sistem upravlja UCIT (NLB, 2012).

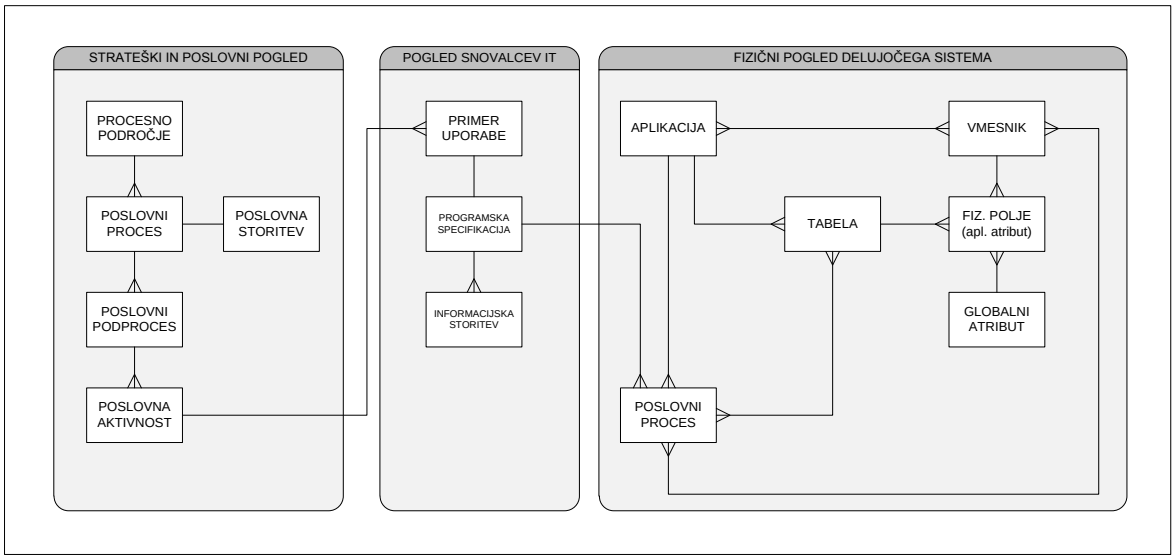
Slika 29: Prikaz plasti informacijskega sistema NLB



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

Informacijska arhitektura mora na vseh nivojih upoštevati tudi pravila informacijske varnosti, neprekinjenega poslovanja, elektronskega arhiviranja itd. Poiskati je potrebno stične točke med različnimi pogledi na arhitekturo in širše, na poslovno arhitekturo banke (pogledi poslovnega ali tehničnega stratega, procesnega tehnologa, načrtovalca, razvijalca, končnega uporabnika so namreč lahko med seboj zelo različni). Stične točke, ki jih omenja Zachmann-ov model celovite arhitekture, so navadno: podatek, proces ali lokacija, lahko pa tudi ljudje, čas ali planiranje (NLB, 2012).

Slika 30: Primer povezave poslovne in informacijske arhitekture preko različnih stičnih točk



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

3.1 Informacijska arhitektura

Informacijska arhitektura je osredotočena na potrebe uporabnikov po informacijah. Te potrebe so podprte s storitvami, ki jih zagotavljajo aplikacije, ki obdelujejo poslovne podatke, vse aplikacije pa tečejo na tehnološki infrastrukturi.
Informacijsko arhitekturo obravnavamo 2-nivojsko:

- visokonivojski modeli ter sheme,
- registri, slovarji in podatkovni modeli.

Visokonivojski modeli povezujejo nastajanje, upravljanje, hranjenje in širjenje informacij banke s tehnologijo, ki je za to potrebna. Poudarjajo pomembnost hranjenja vseh poslovnih podatkov na enem centralnem sistemu, torej v podatkovni bazi na osrednjem računalniku. Notranja varnostna politika ne odobrava hranjenja poslovnih podatkov na sekundarnih sistemih, delovnih postajah in prenosnikih – tako v prostorih banke kot pri uporabnikih doma. Drugi nivo zajema strukture ključnih poslovnih informacij, ki so:

- register tabel NLB,
- register vmesnikov NLB,
- slovar podatkov NLB,
- podatkovni modeli posameznih aplikacij,
- register job-ov NLB.

Za podatke so vzpostavljena pravila lastništva, dostopa in uporabe, ki zagotavljajo, da je sleherna informacija uporabljena v skladu z njenim namenom in upravljana v skladu s politikami, pravili in procedurami, ki veljajo v banki (NLB, 2012).

3.2 Aplikacijska arhitektura

Temelj te arhitekture je *Register aplikacij NLB*, kjer so zbrane vse aplikacije informacijskega sistema NLB. Banka ima heterogeno aplikacijsko okolje, kar je posledica mešanega izvora aplikacij: deloma lastni razvoj, deloma zunanji razvoj, deloma nakup aplikacij »na ključ«. Pri tem je uporabljenih vrsto različnih tehnologij in platform.

V zadnjih letih so pomembna prizadevanja za vzpostavitev storitveno orientirane arhitekture (angl. *Service Oriented Architecture* – SOA), temelječe na samostojnih komponentah poslovne logike, ki se jih da večkrat ponovno uporabiti. Zato se uveljavlja pristop večnivojske aplikacijske arhitekture, kjer je vsaka aplikacija sestavljena iz:

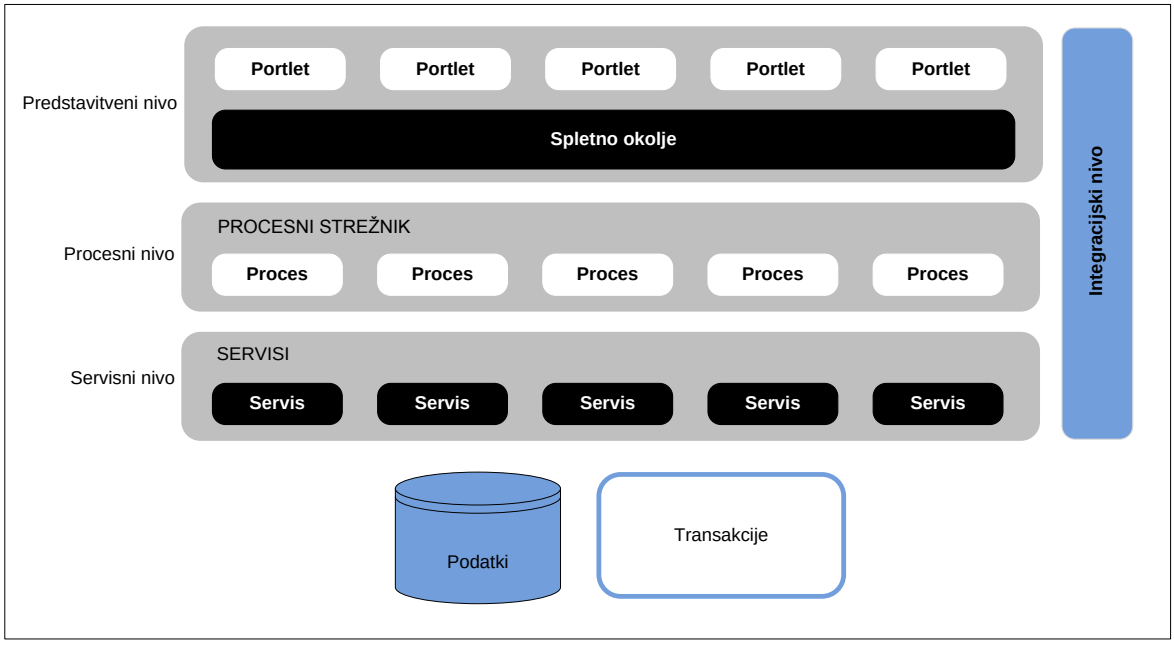
- predstavitvenega nivoja (omogoča uporabnikom dostop skozi različne vmesnike in tehnologije),

- logičnega nivoja (samostojne enote poslovne logike, ki jih uporabimo večkrat in v različnih tokih),
- podatkovnega nivoja (podatkovne baze ter standardizirani podporni viri in servisi).

3.2.1 Koncept aplikacijske arhitekture

Splošna usmeritev je razvoj novih aplikacij v skladu s storitveno usmerjeno arhitekturo SOA povsod, kjer je to smiselno in cenovno upravičeno.

Slika 31: Koncept ciljne aplikacijske arhitekture NLB



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

Vrstni red uvajanja principov SOA je od spodaj navzgor:
1. **Servisni nivo**
Izgradnja enotnih servisov za pogosto uporabljane funkcije, ki se trenutno podvajajo v različnih sistemih, spodbujanje ponovne uporabe že zgrajenih servisov.
2. Procesni nivo
Izločitev procesne logike za pomembne poslovne procese na ločen nivo.
3. **Predstavitveni nivo**

Izgradnja enotnih portletov za pogosto uporabljane sklope ekranov, ki se trenutno podvajajo v različnih sistemih, sestavljanje predstavitvenega dela aplikacije iz portletov, spodbujanje ponovne uporabe že zgrajenih portletov. Integracijski nivo zajema postavitev in uporabo vodila za integracijo (angl. *Enterpise Service Bus* – ESB).

Na področju varnosti so usmeritve naslednje (NLB, 2012):

- uporaba ustreznih mehanizmov za varno izmenjavo podatkov med različnimi sistemi glede na potrebe (šifriranje),
- uporaba elektronskega podpisa pri zajemu elektronske dokumentacije,
- uporaba časovnega žiga pri hranjenju elektronsko podpisanih dokumentov v elektronskem arhivu NLB.

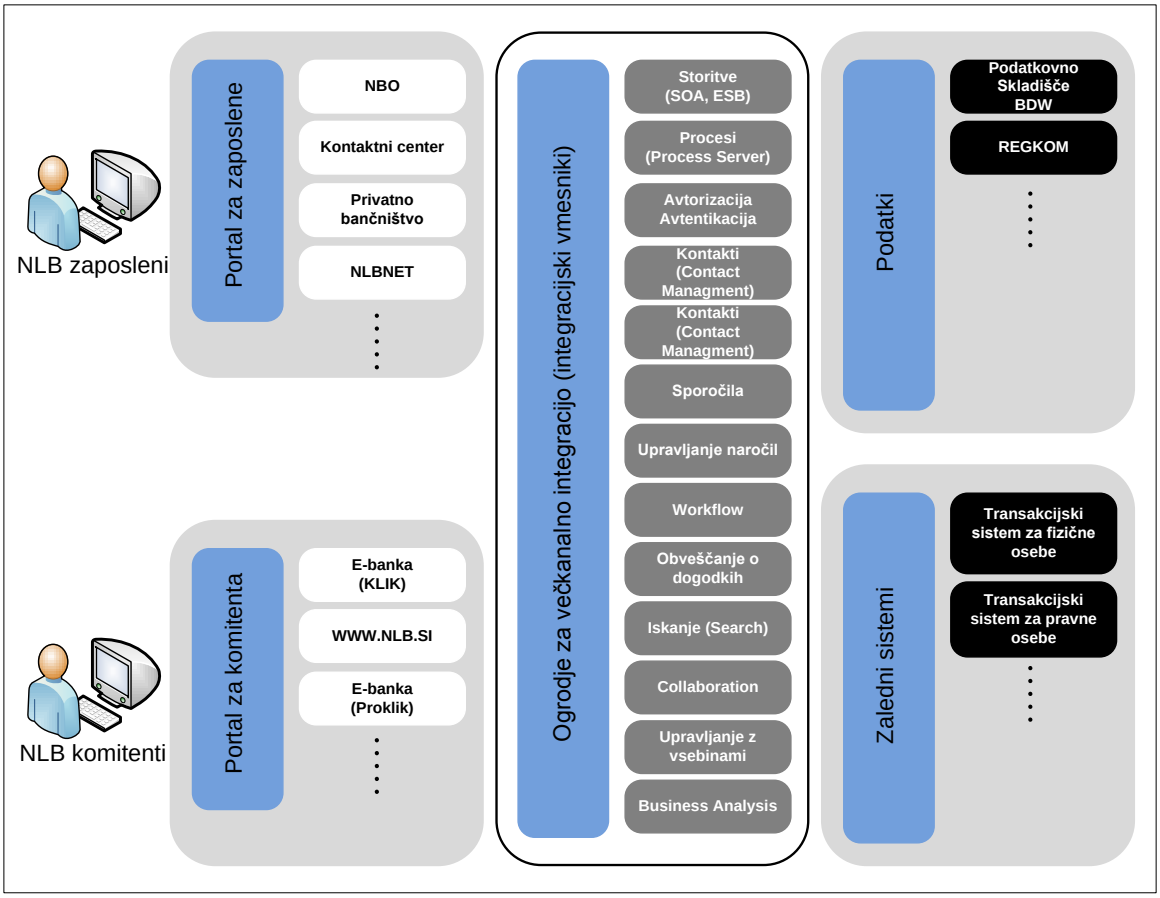
3.2.2 Podroben prikaz aplikacijske arhitekture e-bančništva za zaposlene in komitente NLB

Zaradi določene mere podvajanja istih funkcionalnosti in procesov na različnih tržnih poteh je na tem področju zelo smiselno in upravičeno uporabiti pristope storitvene arhitekture SOA, ki omogoča, da se zaledne funkcionalnosti in procesi razvijejo na enem mestu in se nato uporabljajo za vse kanale.

NBO (Novo bančno okence) je glavna aplikacija, ki jo za svoje delo uporabljajo uporabniki v poslovalnicah NLB. Vendar pa se za nekatere pogosto uporabljane funkcije v poslovalnicah še vedno uporabljajo druge aplikacije, kar za uporabnika pomeni zamudno preklapljanje med aplikacijami in pretipkavanje podatkov.

Na področju elektronskega bančništva (Klik in Proklik), zunanjega spletnega portala NLB ter notranjega intraneta (NLBNET) so v uporabi sistemi, ki so bili zasnovani in postavljeni pred več kot desetimi leti, do danes pa so doživeli mnoge nadgradnje in razširitve funkcionalnosti. Sistemi trenutno večinoma pokrivajo potrebe NLB, vendar bo potrebno začeti z načrtovanjem in prenovo obstoječega sistema. Na področju Kontaktnega centra in Teledoma je razvita povsem nova podpora, katere del je tudi centralni sistem za upravljanje s kontakti, ki je pripravljen za integracijo z vsemi ostalimi tržnimi potmi. Podpora je izvedena v okviru aplikacije NBO, kar dodatno pripomore k integralnosti IT Sistemov (NLB, 2012).

Slika 32: Aplikacijska arhitektura sistema podpore e-kanalom



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

Na Sliki 28 je prikazana arhitektura sistema podpore e-kanalom (e-banka in bančno okence). Uporabniške aplikacije preko integracijskih vmesnikov uporabljajo skupne podatke, zbrane v podatkovnih skladiščih (angl. *Base Data Warehouse* – BDW) in registru komitentov (REGKOM). Ravno tako pa so integracijski vmesniki vmesni člen med uporabniškimi aplikacijami in transakcijskimi sistemi, kot sta sistema za fizične in pravne osebe.

3.3 Tehnološka arhitektura

V NLB v zadnjih nekaj letih potekajo intenzivne akcije za medsebojno uskladitev in zbliževanje poslovnega in tehnološkega dela v kar največjem delu razvoja, vzdrževanja in obratovanja informacijskega sistema. Na osnovi poslovne strategije nastaja poslovna arhitektura kot podlaga za ustrezno informacijsko arhitekturo, katere osnovni vsebinski del je tudi tehnična arhitektura. Le-ta temelji na sprejetih strateških tehnoloških smernicah za določeno časovno obdobje, ki omogoča, da se tehnična arhitektura smiselno in stvarno vpelje v konkretno okolje.

Razvojno okolje predstavlja celoto strojne in programske opreme, podprte z ustrezno metodologijo, kjer se informacijski sistem razvija do uvedbe v produkcijo. Gre za okolje celotnega življenjskega kroga razvoja informacijskega sistema. V tem pomenu je razvojno okolje samo poseben primer in del izvajalnega okolja. Izvajalno okolje predstavlja celoto bistvenih tehnoloških delov v okviru strojne in/ali programske opreme, znotraj katere informacijski sistem vsakodnevno teče v eni od stopenj življenjskega kroga (razvojno okolje, testno okolje, sprejemno (angl. *User Acceptance Testing* – UAT) okolje, produkcija), pri čemer gre poseben poudarek produkciji. Upravljanje z dokumenti in pisarniško poslovanje sta umeščena v okvir tehnologije, ker obstajata na videz neopazno, zahtevata pa precejšnjo porabo najrazličnejših virov.

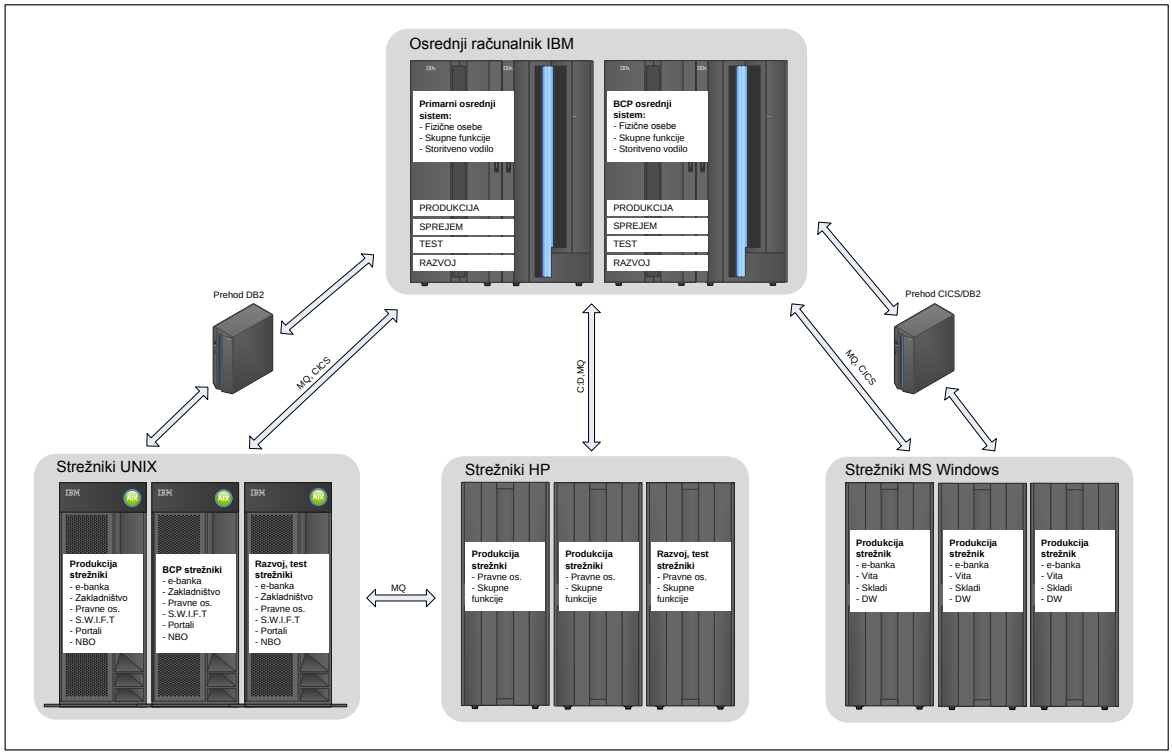
NLB se že daljši čas nahaja v fazi prenove poslovnih procesov s poglavitnima ciljema zniževanja stroškov in ohranjanja primerjalne prednosti, ki je bila pridobljena v dolgoletnem uspešnem poslovanju. Oboje dandanes vse bolj zahteva kar največjo mero prilagodljivosti v smislu kar najhitrejšega odziva na tržne potrebe, t. j. na spremenjene navade in/ali pričakovanja strank. V praksi to pomeni bistveno zahtevo zmožnosti čim krajšega življenjskega kroga razvoja informacijsko podprte rešitve, od ideje, preko zasnove in realizacije, pa vse do uvedbe v redno produkcijo. Tehnologija sama zase ni in ne more biti rešitev poslovnih zahtev. Le-te so lahko smiselno zajete in obdelane v ustrezno opredeljenih in celovito povezanih poslovnih procesih (po možnosti modeliranih), ki so osnova za kasnejšo aplikativno integracijo v okviru storitveno usmerjene arhitekture. Je pa tehnologija skupek tistih virov, brez katerih že lep čas ni več sprotnega bančnega poslovanja, torej je smotrna in usmerjena izraba le-teh lahko dodatna osnova za doseganje zastavljenih ciljev (NLB, 2012).

3.3.1 Koncept tehnološke razvojne arhitekture

Razvojno okolje zavzema celoto potrebne aplikativne in infrastrukturne opreme za zagotovitev zadovoljivo podprtega življenjskega kroga informacijskega sistema. Razvojni sistemi so lahko relativno enostavni, dokler zagotavljajo sprejemljive odzivne čase in zadosten nabor podatkov. Poleg obstoječih testnih okolij za posamezne aplikacije se vzdržuje integralno testno okolje v produkcijsko primerljivi konfiguraciji, ki se uporablja tudi za uporabniške sprejemne teste UAT. Vsi koraki življenjskega kroga razvoja so podprti z enotno rešitvijo za vodenje konfiguracije in upravljanje s spremembami. Glede na izbranega strateškega partnerja je to lahko skupina orodij IBM ki so komplementarna orodja razvojni tehnologiji. Na osrednjem bančnem računalniku se uporabljajo IBM orodja SCLM za vodenje verzij in distribucijo v različna okolja (test, IUAT in produkcija). Strateška razvojna tehnologija je Java, ki se uporablja v okviru aplikativnih strežnikov in ostalih razvojnih orodij. Le-ta se striktno uporablja za razvoj poslovno kritičnih aplikacij in aplikacij z visoko stopnjo integracije z zalednimi sistemi. Vedno več pozornosti pa se posveča enakovredni tržno prisotni tehnologiji MS .NET predvsem za razvoj spletnih aplikacij in za zaledne podporne sisteme. Poleg tega se s poznavanjem in vzgojo notranjih

razvijalcev za MS .NET zagotavlja tudi učinkovitejši nadzor nad prilagajanjem kupljenih programskih paketov standardom NLB, d. d. (varnostna politika, revizijska sled, dodeljevanje pooblastil, standardni način avtorizacije uporabnika …). Skladno z razvojem podatkovnega skladišča (angl. *Data Warehouse* – DWH) in njegovim dostopom do integriranih podatkov v enotni referenčni strukturi se kot strateška razvojna tehnologija uporablja MS .NET. Na osrednjem IBM računalniku se razvoj še naprej izvaja s programskim jezikom COBOL in CICS. Za izdelavo specifičnih programskih podpor in API-jev se lahko uporabljata tudi assembler in C++. Razvoj se izvaja v okolju podatkovne baze DB2 (NLB, 2012).

Slika 33: Tehnološka arhitektura NLB



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

Izvajalno okolje poslovnih aplikacij v NLB je sila heterogeno, kakor je poenostavljeno prikazano na Sliki 29. Stopnja integracije med fizično različnimi platformami je relativno ohlapna in se opira na datotečno izmenjavo podatkov preko programja za omrežno izmenjavo datotek (Sterling Commerce C:D) oz. za vrstičenje sporočil (MQ), spletne aplikacije ter aplikacije tipa odjemalec/strežnik pa uporabljajo za povezovanje tudi prehod CICS oz. DB2.

Osrednji računalniški platformi se uporabljata kot aplikativni, podatkovni in datotečno/tiskalniški strežnik, strežniška platforma AIX kot aplikativni in podatkovni strežnik, strežniška platforma Windows pa namensko ločeno kot aplikativni in/ali podatkovni strežnik ter ločeno kot datotečno/tiskalniški strežnik (NLB, 2012).

3.4 Varnostni mehanizmi e-bančništva v NLB

Že v uvodu naloge in poglavju o aplikacijski arhitekturi NLB je bilo omenjeno, da je pri razvoju elektronskega bančništva varnost bistvenega pomena. Varnost elektronskega bančništva v NLB temelji na uporabi mehanizmov za varno izmenjavo podatkov med posameznimi notranjimi mehanizmi informacijskega sistema ter izmenjavo podatkov med elektronsko banko in njenimi uporabniki. Med osnovne varnostne mehanizme elektronskega bančništva spadajo: šifriranje – SSL povezava, uporaba elektronskega podpisa ter avtentikacija uporabnika z digitalnim potrdilom. Za dodatno zaščito same transakcije, ko se je uporabnik na vstopu v e-banko že avtenticiral, pa skrbi tako imenovani podpis transakcije. Uporabnik mora pred izvedbo transakcije v zato namenjeno polje vnesti dva naključna znaka osemmestnega gesla, ki ga je predhodno prejel po pošti. Tveganje za nepooblaščen vstop v elektronsko banko ali zlorabo pa je NLB še dodatno zmanjšala z implementacijo RSA sistema. RSA adaptivno avtentikacijski sistem je mehanizem, ki omogoča spremljanje obnašanja komitenta v smislu njegovega poslovanja z elektronsko banko. Sistem si v svojo bazo beleži običajno vedenje komitenta (višina zneskov nakazil ali plačil, ciljne račune, mesto plačevanja (IP naslov), način dostopa do e-banke ...). V primeru, da je to običajno obnašanje komitenta prekinjeno z neprimerno večjim zneskom ali spremembo kraja plačila, bo sistem sprožil opozorilo in zahteval dodatno preverjanje komitenta. To dodatno preverjanje komitenta se lahko izvede s telefonskim klicem ali SMS sporočilom. Sistem pa lahko v takih primerih zahteva tudi dodatni faktor avtentikacije uporabnika (angl. *step out authentication*), kot na primer enkratno geslo OTP, GRID dodatno geslo, SMS potrjevanje itd. V tem primeru pa bi bila potrebna nadgradnja varnostne infrastrukture NLB (NLB, 2012).

3.4.1 PKI infrastruktura AC NLB

Za distribucijo digitalnih potrdil uporabnikom e-banke NLB skrbi PKI infrastruktura, katere lastnik je agencija AC NLB. AC NLB je overitelj, ki izdaja in upravlja s kvalificiranimi digitalnimi potrdili za overjanje varnega elektronskega podpisa. AC NLB izdaja potrdila v skladu z Zakonom o elektronskem poslovanju in elektronskem podpisu (ZEPEP, Uradni list RS, št. 57/2000, 30/2001, 25/2004, 73/2004-ZN-C, 98/2004-UPB1, 61/2006-ZEPT) in njegovimi podzakonskimi predpisi, katerih pravna pravila so v celoti povzeta z direktivo Evropskega parlamenta in Sveta Evropske unije z dne 13. decembra 1999 o skupnem okviru Skupnosti za elektronske podpise (AC NLB, 2012).

Kvalificirana digitalna potrdila, ki jih izdaja overitelj AC NLB, so namenjena za:

- upravljanje s podatki NLB,
- dostop in izmenjavo podatkov, s katerimi upravlja NLB,
- varno elektronsko komuniciranje med imetniki kvalificiranih digitalnih potrdil overitelja AC NLB in

- storitve oz. aplikacije, za katere se zahteva uporaba digitalnih potrdil overitelja AC NLB,
- šifriranje podatkov in sporočil v elektronski obliki po protokolih SSL (angl. *Secure Sockets Layer*) in TLS (angl. *Transport Layer Security*),
- varno pošiljanje elektronske pošte po protokolu S/MIME (angl. *Secure Multipurpose Internet Mail Extensions*),
- digitalno podpisovanje podatkov in sporočil v elektronski obliki ter overjanje identitete podpisnika,
- varno brisanje podatkov v elektronski obliki.

Identiteta overitelja:

c=si,o=ACNLB
CP_{NAME} - AC NLB-1
CP_{OID} - 1.3.6.1.4.1.7.5.9.7.1.4.1

Agencijo AC NLB sestavljajo notranji in zunanji prostori AC NLB, strojna in programska oprema, osebje ter metode in postopki pri upravljanju s potrdili in drugih storitev v zvezi z elektronskim podpisovanjem. Šifrirni algoritmi, formati podatkov in protokoli, ki jih uporablja AC NLB, pa so (AC NLB, 2012):

- za podpisovanje potrdil algoritem SHA-1 z RSA s parom ključev dolžine 2048 bitov,
- za šifriranje podatkov algoritme Triple DES, CAST-128 in RC2 (standardi FIPS PUB 186-2, ANSI X9.30 (1), IEEE P1363 in ISO/IEC 14888-3),
- zgostitvene algoritme SHA-1 (FIPS PUB 180-1 in ANSI X9.30(2)) in MD5 (RFC 1321),
- način uporabe algoritma RSA za upravljanje s ključi RSA (RFC 1421 in RFC 1423(PEM) in PKCS#1),
- format potrdil ustreza priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997 ter X.509 ver. 3 (v3),
- registri preklicanih potrdil ustrezajo priporočilu ITU-T za X.509 (1997) in ISO/IEC 9594-8:1997, vključno z verzijo 2 (v2),
- oblika RSA enoličnih razločevalnih imen ter format javnega ključa ustrezajo priporočilu RFC 1422 in 1423 (PEM) in PKCS#1,
- protokol LDAP ustreza priporočilu RFC 1777 in RFC 2559,
- hranjenje zasebnega ključa ustreza priporočiloma PKCS#5 in PKCS#8,

- komunikacija med programsko opremo na strani imetnika in infrastrukturo NLB CA poteka po protokolu SEP (angl. *Secure Exchange Protocol*), ki temelji na standardu GULS (angl. *Generic Upper Layers Security*), ki ustreza priporočilom ITU-T za X.830,

- X.831, X.832 in ISO/IEC 11586-1, 11586-2 in 11586-3 ali protokolu PKIX-CMP, ki temelji na priporočilu RFC 2510.

Vsa potrdila temeljijo na standardu X.509v3 in so shranjena na LDAP strežniku, ki ni javno dostopen. Potrdila se nahajajo v podstrukturi:

ou=Fizicne osebe, o=NLB, o=ACNLB, c=SI

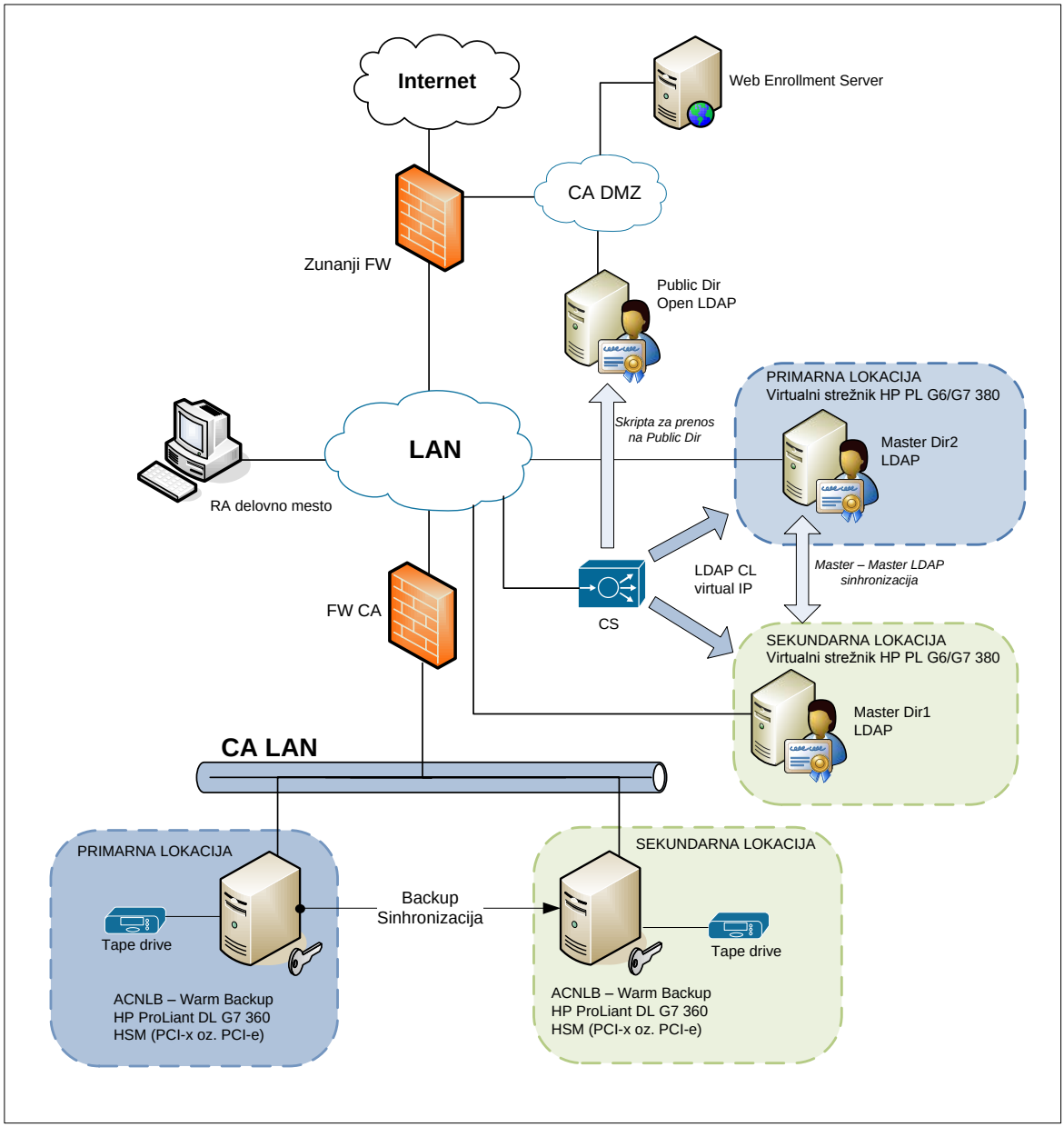
Vsa preklicana digitalna potrdila AC NLB se nahajajo v centralnem registru preklicanih potrdil (angl. *Certificate revocation list* – CRL). V vsakem izdanem certifikatu pa sta navedeni distribucijski točki za prevzem list preklicanih potrdil. Primer izpisa distribucijskih točk je naslednji:

[1]CRL Distribution Point
Distribution Point Name:
Full Name:
Directory Address:
CN=CRL483
O=ACNLB
C=SI
[2]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=ldap://acldap.nlb.si/o=ACNLB,c=SI?certificateRevocationList
URL=http://acldap.nlb.si/crl/acnlbcrl.crl

3.4.1.1 Strojna oprema PKI infrastrukture AC NLB

Strojno infrastrukturo ACNLB sestavljajo: CA strežnik, notranji in zunanji LDAP strežnik, strežnik za prevzem certifikatov (angl. *Enrollment server*), postaja za administracijo RA ter dvonivojska požarna pregrada. Omenjena arhitektura je prikazana na Sliki 30.

Slika 34: Strojna oprema PKI infrastrukture AC NLB



Vir: NLB, Informacijski sistem NLB (Interno gradivo), 2012.

Zaradi zagotavljanja delovanja infrastrukture v visoki razpoložljivosti so vse entitete v omrežju podvojene. Glavna CA strežnika delujeta v ″Warm backup″ načinu, kar pomeni, da med njima poteka sinhronizacija varnostnih kopij. V primeru okvare primarnega CA strežnika se za aktivacijo sekundarne lokacije uporabi zadnjo varnostno kopijo. Iz slike je razvidno, da LDAP imenika delujeta v ″online″ načinu, kar pomeni, da med njima poteka sinhronizacija stanja, kar povzroča, da se vsaka sprememba stanja na prvem strežniku odrazi tudi na drugem strežniku. Imenika se v omrežju predstavljata z enotnim virtualnim IP naslovom na delilniku prometa (angl. *Content switch – CS*). Na LDAP strežniku, ki je dostopen iz interneta, je zaradi notranje varnostne politike objavljena le lista preklicanih certifikatov CRL in ne celotna drevesna struktura LDAP imenika. Iz zunanjega

internetnega sveta pa mora biti zaradi prevzema certifikatov dostopen tudi prevzemni strežnik (angl. *Enrollment server*). V omrežju opazimo tudi delovno postajo RA, ki je namenjena izključno administraciji. Fizično sta RA postaji nameščeni v posebnem prostoru, vstop v ta prostor pa je dovoljen samo pooblaščenim osebam. Celotna infrastruktura je varovana z zunanjo požarno pregrado, glavna CA strežnika pa sta varovana tudi z namensko požarno pregrado (AC NLB, 2012).

3.5 ANALIZA USTREZNOSTI VARNOSTNIH MEHANIZMOV E-BANČNIŠTVA V NLB

V banki NLB se zavedamo pomena varnosti, zato v e-bančništvu uporabljamo najsodobnejše oblike varnega poslovanja preko spleta. Po raziskavah slovenskih medijskih hiš ima NLB eno iz med najbolj varnih spletnih bank v Sloveniji. Celotna infrastruktura omrežja NLB je pred internetnim omrežjem varovana z zmogljivimi požarnimi pregradami ter s posodobljenim sistemom za detektiranje vdorov (angl. *Intrusion detection system* – IDS) in sistemom za preventivno zaščito pred udori (angl. *Intrusion prevention system* – IPS). Strežniki elektronskega bančništva NLB so nameščeni v segment požarne pregrade (angl. *Demilitarized Zone* – DMZ), ki je ločen od lokalnega omrežja NLB ter ščiten pred zunanjim internetom z dodatno namensko požarno pregrado.

Za varnost poslovanja komitentov in e-banke NLB skrbijo varnostni mehanizmi, ki zagotavljajo visoko stopnjo varnosti:

- Šifriranje za zaščito zaupnosti podatkov, ki se prenašajo preko interneta med uporabnikom in strežnikom e-banke NLB. S šifriranjem je zagotovljeno, da je elektronsko poslovanje skrito očem nepooblaščenih oseb (podatke lahko bereta le elektronska poslovalnica in njen uporabnik).
- Overjanje z digitalnim potrdilom, pri katerem se elektronska banka prepriča o identiteti tistega, ki hoče poslovati z njo, uporabnik pa se prepriča, da si zares izmenjuje podatke z e-banko NLB.
- Statično vstopno geslo v spletno aplikacijo e-banke NLB. Uporabnik mora pred vstopom v e-banko vnesti vstopno geslo, ki ga prejme pri registraciji uporabe spletne banke NLB.
- Avtorizacija transakcije, uporabnik mora pri vsakem nakazilu na nove račune pred izvedbo transakcije z miško vnesti dva znaka gesla, ki ga je prejel po pošti po registraciji uporabe spletne banke NLB.
- RSA adaptivna avtentikacija. Na podlagi zgodovine obnašanja komitenta sistem presodi, ali gre za običajno vedenje komitenta ali gre za posebne razmere in predlaga dodatno preverjanje komitenta, na primer s telefonskim klicem ali SMS sporočilom.

3.5.1 Analiza SWOT varnostnih mehanizmov e-banke NLB

Spodnja analiza SWOT predstavlja prednosti, slabosti, priložnosti in nevarnosti obstoječih varnostnih mehanizmov za e-bančništvo v NLB.

Tabela 11: Analiza SWOT varnostnih mehanizmov e-banke NLB

PREDNOSTI	**SLABOSTI**
➢ Enostavnost uporabe e-storitev ➢ Časovni prihranek pri običajnem vedenju komitenta ➢ Nižje cene storitev ➢ Uporaba najsodobnejših tehnologij za zaščito ➢ Uporabnost digitalnega potrdila v druge namene ➢ Uporaba varnostnih mehanizmov pri mobilnih uporabnikih	➢ Izguba (kraja) digitalnega potrdila, vstopnega gesla ➢ Psihološke ovire (strah pred tovrstnim poslovanjem)
PRILOŽNOSTI	**NEVARNOSTI**
➢ Intenzivnejši marketing e-poslovanja ➢ Varnostni mehanizmi in njihova predstavitev potencialnim uporabnikom ➢ Spletna anketa o zadovoljstvu obstoječih uporabnikov ➢ Intervju z znano osebo, ki je uporabnik e-storitve	➢ Izguba (kraja) digitalnega potrdila, vstopnega gesla ➢ Odsotnost protivirusnih programov na domačem računalniku ➢ Shranjevanje gesel v brskalnikih ➢ Shranjevanje gesel na mobilnih telefonih

Integracija obstoječih varnostnih mehanizemov e-bančništva NLB ima kar nekaj prednosti. Zelo pomembni prednosti sta enostavnost in hitrost uporabe. V primeru, da komitent posluje z znanimi računi in brez povečanih transakcijskih zneskov, ter ob predpostavki, da ima komitent digitalno potrdilo že prevzeto, je potrebna samo izbira pravega digitalnega potrdila za avtentikacijo komitenta v elektronsko banko. Uporaba spletne banke je v tem primeru zelo hitra in enostavna. Vsi sistemi varnostnega mehanizma so del informacijskega sistema NLB, tako da je strošek samo vzdrževanje infrastrukture in pa licence programske opreme. Uporabnikov strošek pa je digitalno potrdilo, kar je v primerjavi z ostalimi sistemi (EMV CAP, OTP ...) precej cenejša različica. Uporabnikovo digitalno potrdilo pa je uporabno tudi za druge namene. Velika prednost je tudi ta, da so mehanizmi uporabni tudi za mobilno bančništvo na prenosnih telefonih ali tabličnih računalnikih. Slabost obstoječih varnostnih mehanizmov pa je možnost izgube ali kraje uporabnikovega digitalnega potrdila, neuspešno varovanje e-bančništva pred napadi MiTM in MiTB ter slabost, katere so deležni vsi sistemi, nezaupanje komitentov v sodobno tehnologijo. Obstoječa integracija pa prinaša še mnoge priložnosti, predstavitev delovanja sistemov potencialnim uporabnikom ter intenzivnejši marketing ...

Varnostni mehanizmi e-banke NLB so bili tudi varnostno pregledani s strani zunanjih za to usposobljenih podjetij in dosegli visoke ocene. Poudariti je treba, da je overjanje uporabnikov z digitalnimi potrdili cenovno zelo ugodna rešitev, tako za uporabnika kot tudi za banko. Namreč banka ima za izdajanje digitalnih potrdil v lasti svojo PKI infrastrukturo, kar pomeni, da so strošek samo licence programske opreme, strojna oprema in pa vzdrževanje infrastrukture. Na strani uporabnika pa obstojita dve možnosti. Cenejša možnost je, da uporabnik shrani digitalno potrdilo na računalnik in tvega vdor v računalnik ter krajo digitalnega potrdila. Druga možnost pa je, da uporabnik digitalno potrdilo shrani na varni nosilec – pametno kartico, kar pomeni, da si mora uporabnik priskrbeti tako pametno kartico kot čitalec pametnih kartic. Slednja možnost je z vidika varnosti precej boljša od prve in v končni fazi tudi nekoliko dražja, vendar je odločitev seveda na strani uporabnika. Digitalno potrdilo za dostop do e-banke NLB pa lahko uporabniki uporabijo tudi za druge namene, na primer za dostop do različnih aplikacij javne uprave, zdravstva, digitalni podpis in šifriranje elektronske pošte in drugih dokumentov.

3.5.2 Analiza ostalih varnostnih mehanizmov

Poleg varnostnih mehanizmov, ki so podrobneje opisani v nalogi (PKI infrastruktura, EMV CAP in JXCS arhitektura), pa obstaja še veliko tehnologij, ki bolj ali manj uspešno ščitijo pred napadi na e-bančništvo. V spodnji Tabeli 12 so razvrščeni varnostni mehanizmi, ki najpogosteje ščitijo bančne ali druge transakcijske sisteme. Iz tabele je razvidno, kako posamezni mehanizmi uspešno ščitijo različne napade. Natančno učinkovitost sistemov je težko določiti, saj je njihova uspešnost odvisna tudi od samega okolja, kjer so mehanizmi implementirani, in seveda od kombinacije mehanizmov, saj se redko zgodi, da elektronsko banko ali neki transakcijski sistem ščiti samo en sistem.

Tabela 12: Prikaz učinkovitosti ostalih varnostnih mehanizmov

VARNOSTNI MEHANIZMI	Ribarjenje	MITM	MITB		Vsi napadi
PKI Pametna kartica + XML podpis (JXCS)	DA	DA	DA		DA
PKI Pametna kartica + biometrični zapis	DA	DA	NE		NE
PKI Pametna kartica + čitalec (EMV CAP)	DA	DA	NE		NE
Strojna oprema OTP	DA	DA	NE		NE
PKI Digitalna potrdila	DA	NE	NE		NE
GRID geslo, M-OTP, SMS-OTP	DA	NE	NE		NE
Izziv/odgovor (Challenge/response)	DA	NE	NE		NE
PIN geslo	NE	NE	NE		NE

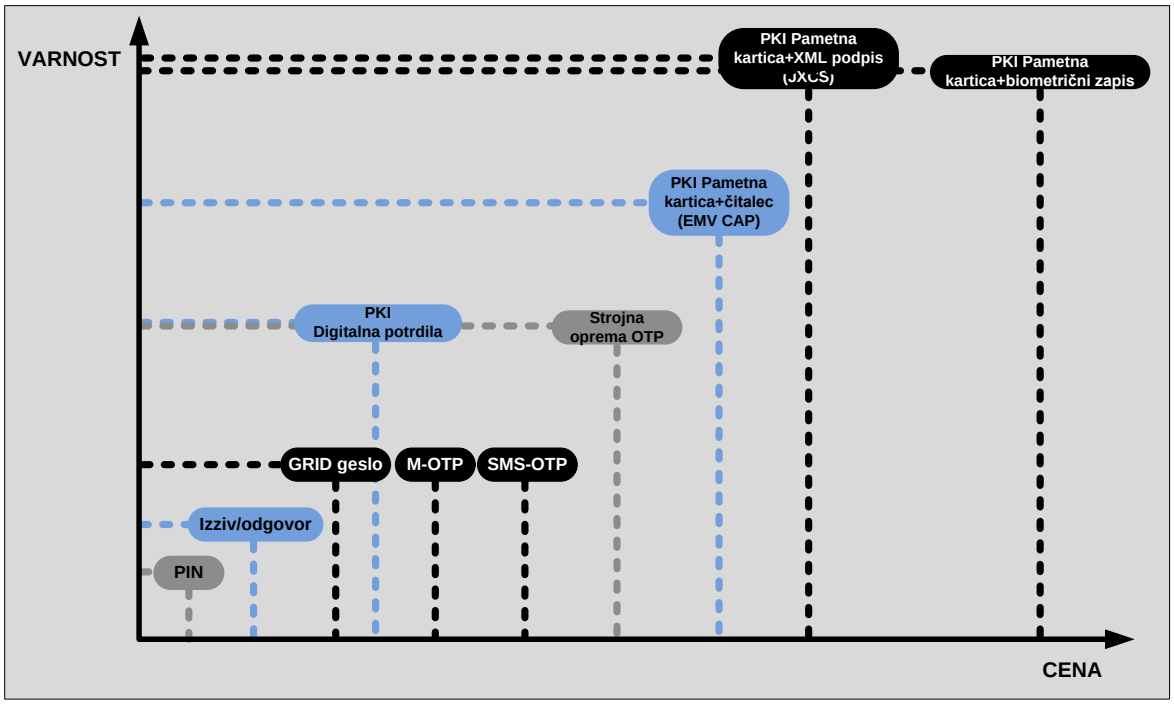
DA	Ubrani napad
NE	Ne ubrani napada

VIr: Mobile Banking, 2012.

Še vedno je daleč najučinkovitejši sistem pri zagotavljanju varnosti e-bančništva, JXCS arhitektura, ki je podrobneje opisana v poglavju 2.5. Omenjeni mehanizem ščiti

elektronsko poslovanje pred vsemi do sedaj detektiranimi naprednimi napadi. Malo manj zanesljiv je sistem, kjer se uporabnik v e-banko avtenticira z lastnimi biometričnimi podatki (prstni odtis, DNK ...), ki so shranjeni na pametni kartici. Sistem je za implementacijo za enkrat še nekoliko neprimeren, saj je oprema za nameščanje in pretvarjanje biometričnih podatkov še zelo draga. Seveda pa avtentikacija uporabnikov s pomočjo biometrije postaja trend in se uveljavlja vedno hitreje. Cenejši in podobno učinkovit kot predhodni mehanizem je EMV CAP sistem, opisan v poglavju 2.4. Sistem EMV CAP je zaradi vplivnosti organizacije EMV zelo pogost v evropskih državah. Še vedno pa ne ščiti najnaprednejših napadov, npr. MiTB. Infrastruktura sistema je kompleksna, kar povzroča dražje in zahtevnejše vzdrževanje, prisotnost pametnih kartic, bralcev in OTP generatorjev pa sistem uvršča med bolj zahtevne za uporabo tudi na uporabniški strani. Omeniti je potrebno tudi avtentikacijo z GRID geslom, ki ga v nalogi posebej nisem opisoval. Način avtentikacije je zanimiv, enostaven, banki in uporabniku pa ne povzroča visokih stroškov. Banka uporabniku pošlje polje naključnih znakov (GRID), e-bančna aplikacija pa za avtentikacijo uporabnika zahteva vnos niza naključnih znakov iz omenjenega polja. Kljub enostavnosti uporabe in nizki ceni pa je sistem za implementacijo v velike transakcijske sisteme neprimeren, saj ne ščiti niti pred MiTM niti pred MiTB. Seveda je situacija povsem drugačna v primeru, ko je mehanizem implementiran v kombinaciji z nekim drugim mehanizmom in služi samo kot dodatna avtentikacija uporabnika.

Slika 35: Razmerje med ceno in varnostjo ostalih varnostnih mehanizmov



VIr: Mobile Banking, 2012.

Na Sliki 31 je prikazano razmerje med ceno in varnostjo mehanizmov. Za najnižjo ceno nam najšibkejšo varnost nudi statično geslo ali PIN, ki ga mora uporabnik vnesti pred

vstopom v e-banko. Iz grafa je očitno, da višjo varnost, ko zahtevamo, globlje bo potrebno seči v žep.

3.5.3 Potreba po nadgradnji varnostnih mehanizmov e-banke NLB

Kot vsaka druga banka tudi NLB poskuša najti ustrezno ravnovesje med ceno in višino zagotovljene varnosti e-banke. Analiza varnostnih mehanizmov e-banke NLB je pokazala, da je obstoječi sistem dober, ni pa brezhiben, saj še vedno ne ščiti pred naprednimi napadi MiTM in MiTB. Glede na to, da NLB že upravlja s PKI infrastrukturo, bi bilo smiselno to infrastrukturo nadgraditi z XML podpisovanjem transakcij v varnem okolju. Za nadgradnjo bi bilo potrebno prirediti e-bančno aplikacijo ter razviti ustrezno kartično aplikacijo, ki bi omogočala procesiranje in podpis XML dokumenta z uporabnikovim privatnim ključem. Nadgrajen sistem bi e-bančništvo NLB varoval tudi pred najnaprednejšimi napadi, kot sta na primer MiTM in MiTB. Seveda bi bil to dodaten strošek tako za banko kot za komitenta. Komitent bi tako imel na izbiro cenejše manj varno ali dražje bolj varno e-poslovanje. Banka pa se v tem primeru investiciji v nadgradnjo sistema ne bi mogla izogniti. V primeru, da bi se komitent odločil za povečanje varnosti njegovega poslovanja z banko, bi moral poleg obstoječega certifikata dokupiti tudi pametno kartico in ustrezen čitalec, ki bi omogočal XML podpis v varnem okolju. JXCS infrastruktura pa ne pokriva mobilnih uporabnikov, kar pomeni, da bi bilo potrebno dograditi arhitekturo tudi za mobilne uporabnike. Mobilni telefoni in tablični računalniki ne omogočajo priključevanja USB bralcev, tako da XML podpis v varnem okolju v tem primeru ne pride v poštev. V obstoječi sistem bi bilo smiselno vpeljati enkratna gesla za mobilne naprave (angl. *Mobile OTP*), katera bi služila za podpis transakcij. Obstoječa infrastruktura omogoča postavitev dodatnega strežnika za prevzem digitalnih potrdil (angl. *Enrollment server*) na mobilne naprave. Obstoječa programska oprema pa omogoča razširitev in uvedbo mobilnih enkratnih gesel M-OTP. V tem primeru je na mobilne naprave potrebno naložiti OTP generator (angl. *Soft token*), ki služi izključno za generiranje enkratnih gesel. Tako bi digitalno potrdilo na mobilni napravi služilo za avtentikacijo uporabnika, enkratno geslo pa za podpis oz. avtorizacijo transakcije.

Najbolj ustrezna ter optimalna rešitev za izboljšavo varnostnih mehanizmov v NLB je torej vzpostavitev arhitekture JXCS. Prvi korak nadgradnje obstoječega mehanizma je prilagoditev spletne aplikacije Klik. Razviti bi bilo potrebno modul za preverjanje XML podpisa, generiranega na strani odjemalca. Naslednji korak je izbira ustreznega kartičnega operacijskega sistema ter razvoj ustrezne aplikacije za izvajanje podpisa v varnem okolju. Zadnji korak nadgradnje obstoječega mehanizma pa se izvede na uporabniški strani. Uvedba ustreznih čitalcev pametnih kartic, ki bi bili sposobni procesirati digitalni podpis v varnem okolju. Za nadgradnjo mehanizma bi bil potreben finančni vložek tako na strani banke kot na strani uporabnika. Glede na finančni vložek implementacij ostalih varnostnih mehanizmov ta ni najvišji. Koristi ter pridobitve v smislu povečanja varnosti pa so pri implementaciji arhitekture JXCS največje. Največja prednost pred ostalimi mehanizmi je

ubranitev napadov MiTM, MiTB ter vseh ostalih naprednih napadov na elektronsko bančništvo. Bistvenega pomena je tudi, da ostaja strojna infrastruktura varnostnega mehanizma na strani banke nespremenjena, kar pomeni, da vzdrževalci sistema po nadgradnji nimajo dodatnega dela. Razlika se odrazi le na strani uporabnika, saj potrebuje dva nova kosa strojne opreme, pametno kartico ter čitalec pametnih kartic. Nekateri uporabniki so zaradi večje varnosti digitalna potrdila že sedaj shranjevali na pametne kartice, kar pomeni, da se zanje tudi po nadgradnji mehanizma proces poslovanja bistveno ne spremeni. Velika prednost implementacije arhitekture JXCS je tudi ta, da kljub uporabi napredne tehnologije od uporabnika ne zahteva dodatnega učenja ali napora pri koriščenju e-bančnih storitev.

Z izvedbo omenjene nadgradnje obstoječe infrastrukture bi e-bančništvo NLB močno izboljšalo raven varnosti ter povečalo dodano vrednost. S tem bi si NLB pridobila konkurenčno prednost pred ostalimi bankami, povečalo pa bi se tudi zaupanje obstoječih in novih komitentov.

3.5.4 Zunanje izvajanje avtentikacije in avtorizacije komitentov

Zunanje izvajanje (angl. *Outsourcing*) je v nekaterih primerih elegantna rešitev za podjetja, ki želijo zmanjšati stroške ali se osredotočiti na svoje temeljne aktivnosti. Podjetje se odloči za zunanje izvajanje takrat, ko ugotovi, da za izvajanje določenega procesa nima dovolj znanja, dovolj virov in meni, da bi proces za njih bolje izvajalo podjetje, ki ima na tem področju veliko več izkušenj. Tudi NLB bi se namesto nadgradnje obstoječega sistema lahko odločila za zunanje izvajanje avtentikacije uporabnikov e-banke. Vendar je pred tako odločitvijo potrebna temeljita analiza. Zavedati se je potrebno, da lahko nepremišljena oddaja ključnega procesa v zunanje izvajanje povzroči veliko škode in veliko izgubo za podjetje. Zunanje izvajanje ključnega procesa varovanja bi lahko pripeljalo do nezaupanja komitentov v e-banko, kar pa lahko banki predstavlja resen problem. Zunanje izvajanje bi lahko pripeljalo do popolne izgube nadzora nad procesom in izgube dragocenih varnostnih podatkov. Zunanji izvajalec bi lahko nepričakovano in proti dogovorom spremenil poslovanje in tehnologijo, kar bi bil močan negativni vpliv na uporabnike e-banke NLB. Banka je za razvoj in nadgradnje varnostnega mehanizma do sedaj skrbela sama, v primeru, da bi se odločila za ta korak, pa bi počasi začela izgubljati dragoceno znanje, kar bi pripeljalo do popolne odvisnosti od zunanjega izvajalca. Zunanje izvajanje tako ključnega procesa za banko je torej nedopustno.

SKLEP

Ker je z vidika razvoja elektronskega bančništva varnost ključna, se temu vprašanju upravičeno posveča velika pozornost, hkrati pa se morebitni varnostni spodrsljaji navadno zamolčijo v želji, da se ohrani zaupanje strank. Dobra zaščita v e-bančništvu je ključnega pomena, saj ji morajo zaupati tako komitenti (uporabniki) kot banke. Velikokrat se pokaže, da je vzpostavitev zaupanja strank celo pomembnejše od same tehnološke rešitve. V sodobnih bankah se zato navadno uporablja tehnologija pametne kartice kot podlaga za identifikacijo uporabnikov in digitalno podpisovanje transakcij na osnovi podpisanih zasebnih in javnih ključev.

Varnostni ukrepi so široka paleta s številnimi načini in področji uporabe, ki ponujajo različne rešitve. Predvsem morajo biti rešitve cenovno optimalne in enostavno razširljive, za končnega uporabnika morajo biti neznane, biti pa morajo tudi take, da nadaljnje odpiranje omrežij in njihovo medsebojno povezovanje ne ogroža varnosti zasebnega dela omrežja. Pri izbiri rešitev je vedno treba tehtati med udobnostjo in varnostjo uporabe storitve. Večja kot je varnost, manjša je udobnost opravljanja storitev in obratno. Za zagotovitev varnosti prenosa informacij pa se je treba držati ustreznih varnostnih zahtev, ki so povezane z uporabo interneta.

Za zagotavljanje visoke varnosti poslovanja banke in komitentov je potrebna integracija več sistemov, ki se medsebojno dopolnjujejo. Sem sodijo SSL/TLS šifriranje prometa, statična gesla, večfaktorska avtentikacija uporabnika, avtorizacija transakcije in učeči se sistemi, ki opozarjajo in zahtevajo dodatno preverjanje uporabnika ob neobičajnem vedenju komitenta. Temeljni varnostni elementi e-banke NLB so vzajemna avtentikacija bančnega strežnika in uporabnikovega odjemalca ter avtentikacija komitenta s kvalificiranim digitalnim potrdilom. PKI infrastruktura in digitalna potrdila so že dokaj stara tehnologija, vendar predstavlja še enega najbolj razširjenih varnostnih mehanizmov v elektronskem bančništvu in elektronskem poslovanju nasploh. Rešitev se še posebej dobro obnese ob upoštevanju navodil izdajatelja o varni hrambi in varni uporabi digitalnih potrdil. Kot smo že ugotovili v prejšnjih poglavjih, integracija varnostnih mehanizmov v NLB dosega visoko varnost, še vedno pa ne zaustavi naprednejših napadov, kjer napadalec prestreže SSL komunikacijo MiTM ali se infiltrira v uporabnikov brskalnik MiTB.

Analiza je pokazala, da bi bilo potrebno za ubranitev tovrstnih napadov obstoječi sistem nadgraditi z digitalnim XML podpisovanjem transakcij. JXCS arhitektura trenutno ščiti pred vsemi znanimi napadi in velja za enega boljših varnostnih mehanizmov. Arhitektura izkorišča visoko tehnologijo čip pametnih kartic, ki omogočajo procesiranje XML dokumenta in na koncu podpis s privatnim ključem uporabnika, shranjenim ravno tako na čipu pametne kartice.

Prva stopnja zaščite e-bančništva NLB še vedno ostaja vzajemna avtentikacija strežnika in odjemalca ter SSL/TLS šifriranje prometa. Ko je medsebojno zaupanje strežnika in odjemalca vzpostavljeno, se med njima vzpostavi SSL/TLS tunel za varen prenos podatkov. Uporabnik se nato s svojim digitalnim potrdilom, shranjenim na pametni kartici, avtenticira v e-bančni spletni aplikaciji. Pred potrditvijo transakcije uporabnik na zaslonu bralca preveri vse potrebne parametre XML dokumenta in s tipkovnico vnese podatke o transakciji. S podpisno tipko izvrši ukaz za digitalno podpisovanje transakcije, nato pa jo vrne strežniku e-banke. Transakcija je bila tako preverjena in digitalno podpisana na kartici in bralcu, to okolje pa je napadalcu nedostopno, kar pomeni, da je ubranjen napad MiTB. V primeru zlorabe SSL/TLS povezave MiTM in poskusa spremembe podatkov o transakciji bo prejemnik oz. e-bančna aplikacija zaradi elektronskega podpisa zaznala nepooblaščeno spremembo podatkov. Za tak način plačevanja uporabnik potrebuje pametno kartico ter čitalec razreda 3 ali 4, kar pomeni, da se poslovanje malenkostno podraži, vendar je odločitev o uporabi zanesljivejšega poslovanja seveda na uporabnikovi strani. Smiselna bi bila tudi nadgradnja varnostnega sistema za mobilno bančništvo. Z nadgradnjo strežnika za prevzem digitalnih potrdil na mobilne naprave in uvedbo enkratnih gesel za podpis transakcij bi tudi mobilno bančništvo NLB doseglo najvišjo možno raven varnosti poslovanja.

Skozi nalogo smo ugotovili, da so digitalna potrdila, čeprav je to precej stara tehnologija, še vedno učinkovita ali celo edina učinkovita zaščita pred t. i. napadi MiTM, kjer se napadalec postavi v omrežju med uporabnika in banko. Da pa bi se e-bančništvo NLB uspešno ubranilo tudi napadov MiTB, pa bi bilo potrebno obstoječi mehanizem nadgraditi še z XML podpisovanjem transakcij v varnem okolju. Mobilno bančništvo pa bi z uvedbo podpisovanj transakcij z enkratnimi gesli dvignilo varnost na povsem zadovoljivo raven.
Ugotovili smo tudi, da za zagotavljanje zadostne varnosti e-bančništva sama tehnologija ni dovolj. Nujno potrebna je tudi ozaveščenost nas uporabnikov. Zaradi hitro razvijajoče se tehnologije in vsak dan novih možnosti, ki jih le-ta prinaša, je potrebno osnovno znanje, ki ga imamo domala vsi uporabniki modernih tehnologij, ves čas izpopolnjevati in prilagajati. Kar je včasih veljalo za neproblematično (varno) uporabo tehnologije ali pa ta sploh še ni bila v uporabi, je morda danes lahko vir tveganj, ki ga bodo napadalci zlahka uporabili proti nam.

LITERATURA IN VIRI

1. *A guide to EMV*. Najdeno 16. marca 2012 na spletnem naslovu http://www.emvco.com/best_practices.aspx?id=217
2. AC NLB. (2011). Politika AC NLB Javni del notranjih pravil. Najdeno 10. februarja 2011 na spletnem naslovu http://www.nlb.si/images/content/_doc/ Politika_ ACNLB - 41.pdf
3. *Bankomati*. Najdeno 14. marca 2011 na spletnem naslovu http://www.bankart.si/si/ ponudba/upravljanje_mreze_ bankomatov/
4. Bric, R. (2010,). O varnosti in nevarnosti elektronskega bančništva. *Moj mikro*. Najdeno 20. junija 2011 na spletnem naslovu http://www.mojmikro.si/taxonomy /term/859
5. ComTrade. (2011). Tehnološki preboj Nove Ljubljanske banke. Najdeno 10. aprila 2012 na spletnem naslovu http://local.comtrade.com/si/SiteAssets/Download/NLB _Klik_Studija_primera.pdf
6. *Cryptographic Key Lenght Recommendation*. Najdeno 20.januarja 2012 na spletnem naslovu http://www.keylength.com/en/4/
7. *Cryptographic Services*. Najdeno 20. junija 2012 na spletnem naslovu http://publib.boulder.ibm.com/infocenter/zos/v1r11/index.jsp?topic=/com.ibm.zos.r11. csfb500/csfb5za061.htm
8. *Cryptography Research*. Najdeno 20. junija 2012 na spletnem naslovu http://researcher. watson. ibm.com/researcher/view_project_subpage.php?id=2700
9. Gabrijelčič, P. (2006). Elektronsko bančništvo v Sloveniji. Najdeno 20. marca 2011 na spletnem naslovu http://www.monitor.si/clanek/elektronsko-bancnistvo-v-sloveniji
10. Gradišar, M. (2003). Elektronsko poslovanje. Ljubljana: Ekonomska fakulteta.
11. Groznik, A., Trkman, P., & Lindič J. (2009). *Elektronsko poslovanje*, str. 60. Ljubljana: Ekonomska fakulteta.
12. Gruschka, N., Reuter, F., & Luttenberger, N. (2004). Checking and signing XML documents on Java smart cards, *IFIP World Computer congress*, str. 1–15.
13. Gullberg, P. (2011). *Remote Authentication for Everyone Everywhere*. Goteborg: Todos.
14. *HalcomCA*. Najdeno 5. oktobra 2011 na spletnem naslovu http://www.halcom-ca.si/index.php?section=1

15. Hernaus, M. (1997). Elektronsko bančništvo v Hipotekarni banki Brežice. Banke in tveganje. *Zbornik 3. Strokovnega posvetovanja o bančništvu.* Ljubljana: Zveza ekonomistov Slovenije
16. *Internet Security and Encryption*. Najdeno 3. marca 2012 na spletnem naslovu http://www.entrust.com/resources/whitepapers.cfm
17. *Internet X.509 Public Key Infrastructure.* Najdeno 24. novembra 2011 na spletnem naslovu http://www.ietf.org/rfc/rfc4211.txt
18. ISO 7816-4. (2011). *CardWerk*. Najdeno 20. novembra 2011 na spletnem naslovu http://www.cardwerk.com/smartcards/smartcard_standard_ ISO7816-4.aspx
19. *JavaCard Technology*. Najdeno 20. novembra 2011 na spletnem naslovu http://www.scribd.com/doc/38629586/Java-Card-Technology
20. Jerman-Blažič, B. (2001). *Elektronsko poslovanje na internetu*. Ljubljana: GV Založba.
21. Kovačič, A. (1998). *Informatizacija poslovanja*. Ljubljana: Ekonomska fakulteta.
22. *Kriptografija*. Najdeno 5. maja 2011 na spletnem naslovu http://www.si-ca.si/
23. *Mobile Banking*. Najdeno 26. februarja 2012 na spletnem naslovu http://asseco.com/see/offer/mobile-banking/
24. *Multi-Factor Authentication*. Najdeno 25. februarja 2012 na spletnem naslovu http://www.actividentity.com/products/authenticationdevices/
25. MULTOS. (2012). Guide to Generating Application Load Units. Najdeno 7. februarja 2012 na spletnem naslovu http://www.multos.com/uploads/GALU.pdf
26. NLB. (2012). *Informacijski sistem NLB* (Interno gradivo). Ljubljana: NLB.
27. Nordfjell, H. (2011). Gemalto Ezio devices protecting nordeas customers online. Najdeno 15. februarja 2011 na spletnem naslovu http://www.gemalto.com/ brochures/download/eba_cs_nordea.pdf
28. Online banking. (2012). *V Wikipediji*. Najdeno 20. marca 2012 na spletnem naslovu http://en.wikipedia. org/wiki/Online_banking
29. *OTP One Time Password.* Najdeno 22. februarja 2012 na spletnem naslovu http://www.gemalto.com/technology/otp.html
30. *Public key infrastructure*. Najdeno 5. aprila 2011 na spletnem naslovu http://www.entrust.com/public-key-infrastructure.htm
31. RIS. (2011). Raba interneta v Sloveniji. Najdeno 12. marca 2011 na spletnem naslovu http://www.ris.org/c/1357/ebancnistvo/?preid=0

32. *Secure Sockets Layer (SSL).* Najdeno 8. novembra 2011 na spletnem naslovu http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL
33. *Securing Digital Identities & Information*. Najdeno 6. decembra 2011 na spletnem naslovu http://www.entrust.com/financial-institutions/index.htm
34. SEPA. (2011). SEPA enotno območje plačil v evrih. Najdeno 5. oktobra 2011 na spletnem naslovu http://www.sepa.si/SloPrenova/Gradiva_Publikacije/EPC /GradivaEPC.htm#Splošno
35. *Smart Card Alliance Financial Resources*. Najdeno 16. marca 2012 na spletnem naslovu http://www.smartcardalliance.org/pages/smart-cards-applications-financial#emv-credit-and-debit-payment
36. *Smart Cards.* Najdeno 2. novembra 2011 na spletnem naslovu http://en.wikipedia. org/wiki/Smart_card#Terminology
37. Smith, J. (2002). Introduction to Public-Key Cryptography. Najdeno 5. maja 2011 na spletnem naslovu http://www.see.ed.ac.uk/~memos/pkey.html
38. Svojšak, M. (1999). *Elektronsko bančništvo* (Interno gradivo). Ljubljana: SKB d.d.
39. SWIFT. (2011). *V Wikipediji.* Najdeno 19. junija 2011 na spletnem naslovu http://en.wikipedia.org/wiki/Society_for_Worldwide_Interbank_Financial_Telecomin
40. *Typs of Smart Cards*. Najdeno 2. novembra 2011 na spletnem naslovu http://www.smartcardbasics.com/smart-card-types.html
41. Vodopivec, T. (2010). Kdo se boji črnega moža. *Poročilo o dogodku Varnost in nevarnost elektronskega bančništva.* Ljubljana: ComTrade d.d.
42. W3C (2008). XML Signature Syntax and Processing (Second Edition). Najdeno 25. marca 2012 na spletnem naslovu http://www.w3.org/TR/xmldsig-core/
43. Združenje bank Slovenije. (2007). Najdeno 5. oktobra 2011 na spletnem naslovu http://www.zbs-giz.si/news.asp?StructureId=470&ContentId=776

PRILOGA

Tabela: Seznam kratic

PKI	*Public Key Infrastructure*	*Infrastruktura javnih ključev*
TLS	*Transport Layer Security*	
SSL	*Secure Socket Layer*	
USB	*Universal Serial Bus*	*Univerzalno serijsko vodilo*
MiTM	*Man in the Middle*	*Mož v sredini*
MiTB	*Man in the Browser*	*Mož v brskalniku*
SMS	*Short message service*	*Kratko sporočilo*
EMV	*Europay MasterCard and VISA*	
CAP	*Chip Authentication Program*	
W3C	*World Wide Web Consortium*	
XML	*Extensible Markup Language*	
PIN	*Personal identification number*	*Osebna identifikacijska številka*
WWW	*World Wide Web*	*Svetovni splet*
RIS		*Raba interneta v Sloveniji*
DES	*Data Encryption Standard*	*Podatkovni šifrirni standard*
NIST	*National Institute of Standards and Technology*	
IDEA	*International Data Encryption Algorithm*	
AES	*Advanced Encryption Standard*	*Napredni šifrirni standard*
ECC	*Elliptic curve cryptosystems*	
OSI	*The Open Systems Interconnection*	
IETF	*Internet Engineering Task Force*	
TCP	*Transmission Control Protocol*	
UDP	*User Datagram Protocol*	
HTTP	*Hypertext Transfer Protocol*	
SMTP	*Simple Mail Transfer Protocol*	
POP3	*Post Office Protocol version 3*	
LDAP	*Lightweight Directory Access Protocol*	
MAC	*Message Authentication Code*	
CA	*Certification authority*	*Certifikatska agencija*
RA	*Registration authority*	*Agencija za registracijo*
CRL	*Certificate Revocation List*	*Lista preklicanih certifikatov*
SEP	*Secure Exchange Protocol*	
GULS	*Generic Upper Layers Security*	
SI-CA	*Slovenian Certification Authority*	*Slovenska certifikatska agencija*
CSCA-SI	*Country Signing Certificate Authority Slovenia*	
CP	*Certification Policy*	*Certifikatska politika*
CPS	*Certification Practice Statement*	*Izjava certifikatske politike*

Se nadaljuje

Nadaljevanje

CPOID	*Certification Policy Object IDentifier*	
OTP	*One Time Password*	*Enkratno geslo*
ICC	*Intergrated Circuit Cards*	
CAD	*Card Acceptance Device*	
SEPA	*Single Euro Payments Area*	*Europski enotni plačilni sistem*
EEPROM	*Electrically Erasable Programmable Read-Only Memory*	
ROM	*Read-only memory*	
RAM	*Random-access memory*	
GSM	*Global System for Mobile*	*Globalni mobilni sistem*
SIM	*Subscriber identity module*	
KMA	*Key Management Authority*	
IIPT	*Intel Identity protection technology*	
HSM	*Hardware Security Modul*	*Strojni varnostni modul*
API	*Application programming interface*	*Programski vmesnik*
IT	*Information technology*	*Informacijska tehnologija*
SOA	*Service Oriented Architecture*	*Storitveno orientirana arhitektura*
ESB	*Enterprise Service Bus*	
BDW	*Base Data Warehouse*	*Glavno podatkovno skladišče*
UAT	*User Acceptance Testing*	*Sprejemno testno okolje*
SCLM	*Software Configuration and Library Manager*	
DWH	*Data Warehouse*	*Podatkovno skladišče*
S/MIME	*Secure Multipurpose Internet Mail Extensions*	
CS	*Content switch*	
DMZ	*Demilitarized Zone*	
RC2	*Ron's Code 2*	*Šifrirni algoritem*
RC4	*Ron's Code 4*	*Šifrirni algoritem*
DES	*Data Encryption standard*	*Podatkovni šifrirni standard*
CAST	*CERN Axion Solar Telescope*	