UNIVERZA V LJUBLJANI
EKONOMSKA FAKULTETA

# MAGISTRSKO DELO

# RAZVOJ INFORMACIJSKEGA SISTEMA ZA VARNA ELEKTRONSKA PLAČILA

V Ljubljani, junij 2008 Darko Žajdela

**IZJAVA**

Študent **Darko Žajdela** izjavljam, da sem avtor tega magistrskega dela, ki sem ga napisal pod mentorstvom **prof. dr. Mira Gradišarja** in skladno s 1. odstavkom 21. člena Zakona o avtorskih in sorodnih pravicah dovolim objavo magistrskega dela na fakultetnih spletnih straneh.

V Ljubljani, dne _____ Podpis:_____

# KAZALO

# KAZALO TABEL

# KAZALO SLIK

# SLOVAR SLOVENSKIH PREVODOV TUJIH IZRAZOV

| **Angleški izraz** | **Slovenski prevod** |
|---|---|
| Acquirer | Pridobitelj |
| Authentication | Overjanje |
| Authentication attempt | Poizkus overjanja |
| Certificate Authority (CA) | Agencija za overjanje |
| Certificate chain | Veriga certifikatov |
| Certification Practice Statement (CPS) | Dokument o ravnanju s certifikati |
| Certificate Revocation List (CRL) | Črna lista certifikatov |
| Conditional field | Pogojno polje |
| Confidentiality | Zaupnost |
| Cipher Suite | Kriptografski paketi |
| Client | Odjemalec |
| Decrypt | Dešifriranje |
| Deflate | Stiskanje |
| Encrypt | Šifriranje |
| Enrollment during shopping | Vključitev med nakupom |
| Handshake | Rokovanje |
| Hardware Security Module (HSM) | Strojni šifrirni modul |
| Hash algorithm | Zgoščevalna funkcija |
| Integrity | Neokrnjenost |
| Interoperability | Večuporabnost |
| Issuer | Izdajatelj |
| Non-repudiation | Preprečitev tajenja komunikacije |
| Optional field | Opcijsko polje |
| Payment gateway | Plačilna vrata |
| Public Key Cryptography | Kriptografija javnih ključev |
| Public Key Infrastructure | Infrastruktura javnih ključev |
| Registration Authority (RA) | Agencija za registracijo |
| Required field | Zahtevano polje |
| Secret Key Cryptography | Kriptografija skritih ključev |
| Server | Strežnik |
| Server wallet | Strežniška digitalna denarnica |
| State Full application | Aplikacija, ki vzdržuje spomin |
| Token | Žeton |
| Web Server | Spletni strežnik |

# 1 UVOD

V zadnjih nekaj letih smo bili priča silovitemu razvoju na vseh področjih našega življenja. Finančno poslovanje in potrošniške navade so se spremenile in postajajo bolj kompleksne, kot so bile še pred nekaj leti. Tudi v bančnem sektorju smo priča uvajanju novih poslovnih rešitev in tržnih kanalov, ki omogočajo višjo storilnost in lažjo mobilnost uporabnikov.

## 1.1 Opredelitev problematike

Konec 70ih in začetek 80ih, so bili množici uporabnikom predstavljeni različni sistemi za plačevanje preko računalniških mrež. Ker so bili ti sistemi premalo uporabni za tedanje uporabnike računalniških mrež, je malo od teh sistemov prešlo začetno fazo izdelave. S pojavom interneta se je ovira za napredek na tem področju bistveno zmanjšala. Že zelo zgodaj je bilo izdelanih veliko različnih plačilnih sistemov za internet. Večina od teh rešitev ni pridobila kritične mase, ki bi dovoljevala obstanek sistema. Prva podjetja na tem področju kot so First Virtual, CyberCash in Digicash so predstavila elektronske plačilne sisteme, ki so privabili veliko uporabnikov ampak niso prinesli pričakovanega donosa (O'Mahony, Peirce, Tewari, 2001). Nekatera znana podjetja kot npr. Cisco, Amazon, Dell, so sama vzpostavila sistem elektronskega poslovanja in pri tem porabila nekaj milijonov dolarjev (Skrt, 2002). Vse do sedaj omenjene tehnologije za plačila preko računalniških mrež imajo svoje dobre in slabe lastnosti. Vsaka od teh rešitev je primerna za določeno področje poslovanja, nobena pa ni primerna za vsa področja (Puhrerfellner, 2000).

Po raziskavah sodeč imajo elektronske transakcije s karticami 6% delež med vsemi transakcijami s karticami, ki v znesku izraženo predstavljajo 5% evropskega BDP-ja (bruto domači proizvod). Število elektronskih transakcij se povečuje 50% letno (ZBS, 2007). Povečanje donosnosti iz naslova elektronskega poslovanje je možno z uporabo varnih rešitev, ki overjajo uporabnika in tako zmanjšujejo stroške, povezane z zlorabami in zavračanjem. Trenutno najbolj razširjeno okolje, ki zagotavlja izvedbo elektronskih transakcij s karticami je podobno klasičnim MOTO (Mail Order/Telephone Order - naročila preko pošte ali telefona) transakcijam. Zaradi narave transakcij na daljavo predstavljajo take transakcije tveganje, ter s tem zavračanje kupcev. Našteti dejavniki povečujejo stroške elektronskih transakcij. V povprečju je 70% vseh zavračanj povezanih z razlogom 4837 – ni odobritve imetnika kartice in razlogom 4863 – neznan imetnik kartice (MasterCard Int., 2004).

Zaradi številnih zlorab in posledično nezaupanja ljudi so številna podjetja, ki se ukvarjajo s prodajo na internetu, posvetila ogromno časa in energije, da bi ustvarila večjo varnost in kar najbolj učinkovite mehanizme za preprečevanje zlorab. Po ugotovitvah številnih raziskav, je pomanjkanje varnosti v elektronskih plačilnih sistemih, ki jih uporabljajo kupci (plačniki) in

prodajalci (prejemniki plačil), ena od glavnih ovir za nadaljnji razvoj elektronskega poslovanja (Skrt, 2002).

Eden izmed ključnih dejavnikov, ki prispeva k nizki stopnji zaznane varnosti, je pomanjkanje zaupanja. Splošno zaupanje v plačevanje prek interneta je tisti dejavnik, ki pomembno vpliva na pripravljenost kupca plačati in prodajalca sprejeti plačilo prek interneta. Tu gre za obljubo kupca prodajalcu, da bo plačal izdelek oziroma storitev in obljubo prodajalca kupcu, da bo za plačilo dobavil izdelek oziroma izvedel storitev. Tako velja, da je problem zaupanja pri plačevanju prek interneta dvojen: kupec, ki nastopa v vlogi plačnika, mora verjeti, da bo prodajalec izpolnil dano obljubo. Prodajalec, ki nastopa v vlogi prejemnika plačila, pa mora verjeti, da bo kupec plačal. Oba pa morata verjeti, da je plačevanje prek interneta varno (Bračun, 2003).

Zaradi človeške občutljivosti in nezaupanja je prihodnost elektronskega poslovanja odvisna predvsem od možnosti zaščite in čim večjega varstva zasebnosti. Narediti zanesljiv in zaupanja vreden plačilni sistem, kot je na primer dvigovanje gotovine na bančnih avtomatih in klasično plačevanje blaga s karticami, je naloga, ki se jo zavedajo vsi pomembnejši akterji svetovne trgovine (Skrt, 2002), ter tudi podjetje v katerem sem zaposlen.

## 1.2 Namen, cilj in metoda dela

Namen dela je spoznati se z elektronskimi plačilnimi sistemi, ugotoviti njihov pomen, značilnosti in nenazadnje omejitve. Za varne elektronske plačilne sisteme so značilne visoke tehnološke metode, zato bom te metode raziskal. Podrobno bom analiziral delovanje 3-D Secure plačilnega sistema, njegove lastnosti in zahteve za implementacijo. Po vseh spoznanjih o elektronskih plačilnih sistemih bom lahko ocenil prednosti in pomanjkljivosti 3-D Secure plačilnega sistema z vidika potreb podjetja v katerem sem zaposlen. Pomembno je spoznati dejavnike, ki vplivajo na nastanek novih elektronskih plačilnih sistemov.

Primarni cilj dela je kot izdajatelj kartic razviti učinkovit in varen elektronski plačilni sistem 3-D Secure. Iz tega sledijo naslednji cilji:

- povečati število trgovcev v našem procesnem centru. Skrb trgovcev je zagotovitev, da bodo za blago ali storitev prejeli proti plačilo. 3D-Secure to skrb odpravlja, saj pravila MasterCard-a in Vise jasno narekujejo odgovornosti v primeru zlorabe;
- povečati obseg elektronskih transakcij. Zaradi večjega zaupanja v plačilni sistem se bo več imetnikov kartic odločilo za plačilo prek interneta;
- večanje števila kartic v našem procesnem centru. Zaradi privlačne, varne metode nakupovanja na internetu se bo povečalo število imetnikov naših kartic;
- znižanje stroškov, ki nastanejo v primeru zlorab. Z uporabo zanesljivejše metode plačevanja se zniža število zlorab.

V magistrskem delu bom uporabil znanja, pridobljena na podiplomskem študiju na Ekonomski fakulteti v Ljubljani in izkušnje, pridobljene z delom na področju informatike in razvoja v podjetju, kjer sem zaposlen. Pri izbiri tehnologij in načrtovanju informacijskega sistema se bom opiral na domačo in tujo literaturo, na smernice največjih svetovnih proizvajalcev programske opreme in na splošne svetovne trende. S pomočjo znanja o informacijski arhitekturi in z branjem priporočil glede varnosti elektronskih plačilnih sistemov bom izbral najustreznejšo arhitekturo informacijskega sistema za naše podjetje.

# 2 ELEKTRONSKI PLAČILNI SISTEMI

Do cilja naloge je moč priti le z dobrim razumevanjem kaj so elektronski plačilni sistemi, kakšne vrste poznamo ter katere tehnološke metode taki sistemi uporabljajo za delovanje.

## 2.1 Elektronsko poslovanje

V začetku 90ih se je v poslovnem svetu pojavil nov način opravljanja poslov pod imenom elektronsko poslovanje (e-poslovanje, angl. *e-commerce*). Skozi leta se je elektronsko poslovanje spremenilo v popularno in uveljavljeno pot za sklepanje poslov. Medtem ko strokovnjaki še vedno ocenjujejo njegovo pomembnost, se elektronsko poslovanje spreminja in raste neverjetno hitro. Elektronsko poslovanje proizvaja neverjetne rezultate za podjetja in stranke, zato je ‘fenomen' elektronskega poslovanja zanimiv za vse tiste, ki so kdaj poskusil poslovati na klasični nepovezan (angl. *off-line*) ali povezan (angl. *on-line*) način. Kmalu je postalo jasno, da se bo elektronsko poslovanje uveljavilo, saj ga je mnogo podjetij in kupcev sprejelo z veliko žlico. Elektronsko poslovanje je postalo posebej pomembno za dva poslovna modela in sicer B2C (angl. *business-to-consumer*) poslovanje med podjetji in kupci ter B2B (angl. *business-to-business*) poslovanje med podjetji (Abrazhevich, 2004). Vse bolj se uveljavlja tudi poslovni model C2C (angl. *customer-to-customer*) v katerem poslujeta posameznika brez posrednikov.

Elektronsko poslovanje B2C ponuja kupcem napredne nakupovalne metode za produkte, informacije, storitve, elektronsko bančništvo, osebne finance… Kupci lahko primerjajo produkte in hkrati vplivajo na njihove lastnosti, ceno in kakovost.

Model elektronskega poslovanja B2B omogoča podjetjem lažjo organizacijo poslovanja. Podjetja se lahko s pomočjo elektronskega poslovanja hitreje prilagajajo potrebam trga ter s tem dosežejo boljše rezultate poslovanja. Neposredno sodelovanje med podjetji omogoča večjo kontrolo poslovanja ter znižanje stroškov z izključitvijo posrednikov v proizvodni verigi. Dober primer podjetij, ki slonita na tem modelu, sta Dell in Cisco (Laudon, Traver, 2002).

Učinki, ki jih prinaša elektronsko poslovanje za podjetja so:

- zmanjšanje stroškov inventarja, operative in distribucije;
- povečanje fleksibilnosti proizvodnje z nepretrgano dobavo surovin;
- višanje kvalitete produktov s povečanim sodelovanjem med kupcem in prodajalcem;
- izboljšano sodelovanje med distributerji in proizvajalci;
- večjo transparentnost cen na trgu (Laudon, Traver, 2002).

## 2.2 Uvrstitev elektronskih plačilnih sistemov v elektronsko poslovanje

Najbolj popularna definicija elektronskega poslovanja temelji na 'on-line' načinu poslovanja. Elektronsko poslovanje zagotavlja možnost izvajanja nakupov in prodaje produktov, informacij in storitev na internetu in na ostalih povezanih okoljih. Tako kot za vsako nakupovanje, je tudi v elektronskem poslovanju glavni problem varna izmenjava denarja med sodelujočima partnerjema. V elektronskem poslovanju so plačila izvedena v denarju, ki je izražen v elektronski obliki. Taka plačila poimenujemo elektronska plačila. Elektronska plačila so del elektronskega poslovanja in so eden najbolj kritičnih delov le-tega. Drugače povedano: elektronska plačila so oblika finančne izmenjave, ki se odvija med kupcem in prodajalcem in je omogočena z elektronskimi povezavami (Kalakota, Whinston, 1997).

Elektronski plačilni sistemi (v nadaljevanju EPS) omogočajo izvedbo postopka po tem, ko se kupec odloči plačati za produkt ali storitev. Izvajajo plačila od kupca do prodajalca na varen način. Vloga, ki jo zasedajo elektronski plačilni sistemi v elektronskem poslovanju, je pomemben dejavnik za prihodnost elektronskega poslovanja. Nadaljnja rast elektronskega poslovanja je zato odvisna v veliki meri od razvoja boljših elektronskih plačilnih sistemov.

Elektronska plačila so se prvič pojavila zaradi potrebe po takojšnjih plačilnih metodah v nepovezanem svetu (potreba po ‘on-line' avtorizacijah transakcij kreditnih kartic). Trenutno najbolj razširjena oblika plačila v elektronskem poslovanju je kreditna kartica. Slabosti uporabe kreditne kartice na internetu so se hitro pokazale, temu primerno so se pojavili novi EPS-ji. Tudi razvoj novih poslovnih modelov je ustvaril potrebo po novih načinih izmenjave denarja in novih EPS-jih. Pri elektronskih dražbah je prišlo do potrebe po plačilu C2C. Nekateri tipi informacijskih produktov in storitev zahtevajo mala in mikro plačila in omogočajo podjetjem zaslužek z učinkom prodaje masi ljudi. Potreba po plačilih z mobilnimi napravami je prisilila razvoj plačilnih sistemov za mobilno elektronsko poslovanje. Pomanjkanje prilagojenih plačilnih sistemov in infrastrukture je eden glavnih razlogov, ki omejuje povečanje in napredek elektronskega poslovanja (Laudon, Traver, 2002).

## 2.3 Splošno o elektronskih plačilnih sistemih

Za boljše razumevanje sedanjih trendov na področju elektronskega plačevanja se je potrebno ozreti v preteklost (Pipan, 2002). Uspeh elektronskega plačilnega sistema je odvisen od njegovega sprejetja med uporabniki.

### 2.3.1 Zgodovinski razvoj

Zgodovinski razvoj elektronskih plačilnih sistemov lahko razdelimo na štiri temeljna obdobja:

- obdobje prazgodovine;
- obdobje pionirstva;
- iniciativa bančnega sektorja;
- internetni plačilni sistemi druge generacije (Böhle, 2001).

**Obdobje prazgodovine (1976 – 1992)**

Še preden se je internet dodobra uveljavil in postal nepogrešljiv pri elektronskem poslovanju, je bilo kar nekaj poskusov razvoja različnih sistemov elektronskega plačevanja. Mednje lahko štejemo POS[1] (angl. *point of sale*) naprave, elektronski denar (programsko in strojno podprt), elektronske denarnice, predplačilne eno-namenske kartice in mikro plačila. Tabela 1 prikazuje kronološki pregled dogodkov obdobja prazgodovine.

***Tabela 1: Pregled dogodkov v obdobju prazgodovine***

| Leto | Dogodek |
|---|---|
| **1976** | Diffie in Hellmann: začetek kriptografije javnega ključa |
| **1978** | Prva predplačilna magnetna telefonska kartica v Belgiji |
| **1982** | D. Chaum : objava študije o 'slepem podpisu', ki je pomembna za anonimnost plačil |
| **1983** | Prva predplačilna telefonska pametna kartica v Franciji (Telecarte) |
| **1984** | Minitel – uvedba mikro plačil |
| **1989** | Ustanovitev podjetja DigiCash na Nizozemskem |
| **1991** | Začetek razvoja Mondex-a v Veliki Britaniji |
| **1992** | Uvedba e-denarnice Danmont na Danskem |

*Vir: Böhle, Potential of Server-based Internet Payment Systems, 2001.*

Za to obdobje je bil značilen predvsem razvoj predplačilnih eno-namenskih pametnih kartic, ki so nasledile magnetne kartice iz 70-tih let. Leta 1992 je prišlo do uvedbe prve elektronske denarnice podjetja Danmont. To obdobje je trajalo vse do konca leta 1992, ko se je število uporabnikov interneta povečalo na milijon.

**Obdobje pionirstva (1993 – 1995)**

Druga faza je s stališča varnosti zelo vplivala na nadaljnji razvoj internetnega plačevanja. Podjetje Netscape je leta 1994 predstavilo protokol SSL (angl. *Secure Socket Layer*), ki omogoča varen prenos podatkov med kupčevim brskalnikom in trgovčevim strežnikom. Vse do tega

[1] POS je naprava, ki jo uporablja trgovec na prodajnem mestu in omogoča plačilo s kartico.

trenutka so se informacije o kreditnih karticah in bančnih računih pošiljale preko interneta popolnoma brez zaščite in so bile lahka tarča nepridipravov. V tem obdobju je podjetje DigiCash preizkusilo prvo varno metodo plačevanja imenovano Cyberbucks. Cyberbucks je bil prvi poizkus tako imenovanega elektronskega denarja, katerega izdajatelj ni banka, temveč podjetje samo. Na trgu sta se pojavili še podjetji First Virtual Inc. in Cyber Cash Inc., ki sta začeli s posredovanjem podatkov o elektronskih transakcijah med kupci, prodajalci in izdajatelji kreditnih kartic. Tudi bančni sektor je začel kazati zanimanje za elektronsko plačevanje. Tabela 2 prikazuje kronološki pregled dogodkov obdobja pionirstva.

***Tabela 2: Pregled dogodkov v obdobju pionirstva***

| Leto | Dogodek |
|---|---|
| **1994** | Razvoj SSL s strani podjetja Netscape |
| **1994** | Prihod podjetij First Virtual in Cyber Cash |
| **1994** | Uvedba elektronskih kovancev Cyberbucks podjetja DigiCash |

*Vir: Böhle, Potential of Server-based Internet Payment Systems, 2001.*

**Iniciativa bančnega sektorja (1995 – 1998)**

V obdobju pionirstva je bančni sektor izgubil nadzor nad internetnimi plačilnimi sistemi, zato si je z novimi iniciativami prizadeval ponovno prevzeti vodilno vlogo na tem področju.

Pomemben korak k temu je bil razvoj protokola za varno transakcijo SET (angl. *Secure Electronic Transaction*), ki se uporablja za elektronsko plačevanje s karticami. Bančni sektor je v tem času tudi prilagodil tradicionalne plačilne inštrumente za uporabo na internetu. V letu 1998 so nekatera pionirska podjetja na področju internetnega plačevanja zašla v finančne težave. Tabela 3 prikazuje kronološki pregled dogodkov obdobja iniciative bančnega sektorja.

***Tabela 3: Pregled dogodkov v obdobju iniciative bančnega sektorja***

| Leto | Dogodek |
|---|---|
| **1995** | Banka Mark Twain ponudi plačilni sistem Ecash podjetja DigiCash |
| **1996** | Prva transakcija preko protokola SET |
| **1997** | Uvedba e-denarnice v Belgiji |
| **1998** | Izdaja e-denarja pod vplivom regulacije bančnega sistema v Nemčiji |
| **1998** | Prenehanje delovanja podjetja First Virtual |
| **1998** | Bankrot podjetja DigiCash |

*Vir: Böhle, Potential of Server-based Internet Payment Systems, 2001.*

**Elektronski plačilni sistemi druge generacije (1999 - 2008)**

Dandanes plačevanje s kreditnimi karticami zavzema med 70 in 93 odstotkov vseh internetnih plačil. V prihodnje naj bi se ta trend nekoliko obrnil v drugo smer, na pomembnosti naj bi pridobili elektronski plačilni sistemi, kot so elektronske denarnice, e-denar, P2P[2] (angl. *Peer to Peer*). Ti plačilni sistemi vidijo svojo priložnost predvsem v skupinah ljudi, ki nimajo svojega bančnega računa ali kreditnih kartic, ter med tistimi, ki želijo popolno anonimnost plačevanja.

***Tabela 4: Pregled dogodkov v obdobju elektronskih plačilnih sistemov druge generacije***

| Leto | Dogodek |
|---|---|
| **1999** | Začetek razvoja plačilnih sistemov P2P, PayPal |
| **1999** | Pojav virtualnih denarnih računov (npr. Cash+) |
| **2000** | Prenehanje plačilnega sistema CyberCash v Nemčiji |
| **2000** | Predstavitev plačilnega sistema 3D-SET |
| **2001** | Bankrot podjetja CyberCash |
| **2001** | Predstavitev plačilnega sistema 3-D Secure |
| **2004** | Prenehanje uporabe Danmont elektronske denarnice |
| **2006** | Razvoj plačilnega sistema P2P, Google CheckOut |
| **2007** | Osnutek SEPA (angl. *Single Euro Payments Area*) on-line plačil |
| **2007** | Razvoj plačilnega sistema P2P, Amazon FPS, beta različica |

*Vir: Böhle, Potential of Server-based Internet Payment Systems, 2001.*

Pomembno vlogo v internetnem plačevanju v zadnjem času pridobivajo mobilni telefoni in z njimi povezani plačilni sistemi. PayPal-u kot prvemu plačilnemu sistemu na področju C2C so začeli konkurirati novi plačilni sistemi, kot sta na primer Google CheckOut in Amazon FPS (angl. *Flexible Payments Service*). Sistemi konkurirajo predvsem v cenovni politiki. Zaradi upada števila transakcij je leta 2004 Danmont prekinil uporabo svoje elektronske denarnice. Tabela 4 prikazuje kronološki pregled dogodkov obdobja druge generacije EPS-jev.

## 2.3.2 Zahteve elektronskih plačilnih sistemov

Elektronski plačilni sistemi morajo izpolnjevati določene zahteve, ki jih postavljajo končni uporabniki sistema. Te zahteve delimo v dve skupini in sicer na varnostne in implementacijske zahteve. Izpolnjevanje zahtev iz obeh skupin je bistvenega pomena za uspešno elektronsko poslovanje in uveljavitev plačilnega sistema (Jarupunphol, Mithcell, 2003).

[2] P2P je kratica za neposredno komunikacijo/opravljanje posla med uporabniki omrežja.

**Varnostne zahteve**

Razumeti varnostne zahteve končnih uporabnikov je kompleksna naloga, saj je odnos uporabnikov do novih tehnologij lahko motiviran z več faktorji. V skupino varnostnih zahtev uvrščamo lastnosti (Hassler, 2001):

- **zaupnost plačila -** finančni podatki kupca so zaupne narave in zato morajo ostati zaupni med prenosom in pri shranjevanju. Kupec zahteva to storitev, medtem ko prodajalec nudi to storitev;
- **neokrnjenost plačila** - transakcija mora biti zaščitena tako med prenosom kot pri shranjevanju;
- **verodostojnost posameznika** - prodajalec zahtevata overjanje kupca, kupec zahteva overjanje prodajalca;
- **odgovornost posameznika -** plačilni sistem mora jasno določati odgovornost posameznikov pri izvedbi transakcije;
- **preprečitev tajenja komunikacije** - plačilni sistem mora imeti mehanizem preprečevanja preklica izvedene storitve, kot npr. pošiljanje podatkov o naročilu/plačilu, potrditev naročila/plačila, itd.

V Tabeli 5 so zapisane dileme kupca in prodajalca o varnosti elektronskega plačilnega sistema.

**Implementacijske zahteve**

Prav tako kot varnostne zahteve tudi implementacijske zahteve v veliki meri vplivajo na uspešnost in prihodnost elektronskega plačilna sistema. Med implementacijske zahteve uporabnikov elektronskega poslovanja štejemo (Jarupunphol, Mithcell, 2003):

- **uporabnost -** sistem mora biti enostaven za implementacijo in namestitev. Kupec zahteva od izdajatelja plačilnega inštrumenta (angl. *Issuer*) in prodajalca sistem, ki je varen in enostaven. Prodajalec zahteva od pridobitelja transakcije (angl. *Acquirer*) in izdelovalcev programske opreme preprosto aplikacijo, ki ustreza varnostnim zahtevam;
- **zanesljivost** – definirana je kot verjetnost, da ne pride do izpada sistema. Pod zanesljivost sodi tudi pravilen prikaz podatkov uporabniku v spletnem brskalniku;
- **cena** - cena implementacije in uporabe sistema morata biti dosegljivi za kupca in prodajalca, saj oba nista pripravljena plačati več za to, da bi bila udeležena v elektronski transakciji. Kupec ni pripravljen plačati za digitalno potrdilo, prodajalec ni pripravljen investirati večje vsote v infrastrukturo za opravljanje elektronskih plačil;
- **hitrost transakcije** - transakcija mora biti dovolj hitra za kupca in prodajalca. Kupec si zaradi počasnosti izvedbe transakcije lahko premisli in tako prodajalec ostane brez zaslužka;

- **večuporabnost** - sistem mora biti uporaben med različnimi sistemskimi platformami, spletnimi brskalniki, strežniško programsko opremo in tako omogočati uporabnost čim večji množici kupcev in prodajalcev.

***Tabela 5: Dileme končnih uporabnikov o varnosti EPS-jev***

| | Kupec | Prodajalec |
|---|---|---|
| **Zaupnost** | Moji osebni podatki in podatki o plačilu morajo biti zaščiteni pred zlorabo (med samo transakcijo in tudi po njej). | Moji poslovni podatki morajo biti zaščiteni pred možnimi zlorabami. |
| **Neokrnjenost** | Podatki o plačilu se med samo transakcijo ne smejo spreminjati brez moje vednosti. | Podatki o plačilu se med samo transakcijo ne smejo spreminjati brez moje vednosti. |
| **Verodostojnost** | Želim preveriti, ali je prodajalec res tisti, za katerega se izdaja. | Želim preveriti ali je kupec res tista oseba za katero se izdaja, je upravičen do uporabe plačilnega inštrumenta, je plačilno sposoben? |
| **Odgovornost** | V primeru kraje denarja zaradi tuje krivde ne želim nikakršne odgovornosti in le omejeno, če je krivda moja. | V primeru kraje denarja ne želim nikakršne odgovornosti. |
| **Preprečitev tajenja komunikacije** | Imam možnost odstopa od plačila v primeru, da:<br>• prodajalec ni opravil dogovorjenega;<br>• izdelek/storitev ni enaka opisu;<br>• si premislim. | Imam zagotovilo, da kupec ne bo preklical plačila po prejetju izdelka ali storitve. |

*Vir: Centeno, Securing Internet Payments – The potential of Public Key Cryptography, 2002.*

### 2.3.3 Zaupanje uporabnikov

Eden izmed ključnih dejavnikov, ki prispeva k nizki stopnji zaznane varnosti, je pomanjkanje zaupanja. Splošno zaupanje v plačevanje prek interneta je tisti dejavnik, ki pomembno vpliva na pripravljenost kupca plačati in prodajalca sprejeti plačilo prek interneta (Nyshadham, Ugbaja, 2006). Zanimivo je pogledati raziskavo, kjer je France Bračun (Bračun, 2003) skušal ugotoviti povezavo med zaupanjem in zaznanim tveganjem pri plačevanju prek interneta.

Ugotovitve kažejo, da je pomembno ločiti med zaupanjem v EPS in zaupanjem v menjavo med kupcem in prodajalcem. V EPS uporabniki zaupajo, ko vedo, da obstajajo mehanizmi proti tajenju komunikacije ter ko je ta tehnično ustrezen. To pomeni, da uporabniki vedo kaj tvegajo pri nakupu preko interneta. Velik vpliv na zaupanje ima osebnostni značaj posameznika. V raziskavi je bilo ugotovljeno, da prodajalec in kupec močno zaupata v banko, medtem ko je vpliv

zaupanja v drugo stran prisoten le v primeru kupca, v primeru prodajalca pa je ta vpliv zanemarljiv.

Kupec je v 43% primerih pripravljen plačati prek interneta, medtem ko je 23% prodajalcev pripravljeno sprejeti plačilo prek interneta. To razliko je mogoče pojasniti z viri, ki so potrebni za uvedbo sprejemanja plačil prek interneta. Medtem ko je pri kupcu za plačevanje prek interneta potrebno zagotoviti le ustrezen dostop do interneta in odpreti račun za plačilno kartico v banki, je uvajanje sprejemanja plačil prek interneta pri prodajalcu povezano z velikimi vlaganji. Poleg dostopa do interneta in zagotovitve ustrezne zaščite podatkov, so pri uvajanju sprejemanja plačil potrebne tudi organizacijske spremembe, ki poleg ostalega zahtevajo tudi zaposlovanje ustreznih strokovnjakov. Zato na odločitev prodajalca o uvedbi sprejemanja plačil prek interneta pomembno vplivajo pričakovane koristi oz. možne zamujene priložnosti.

Zgornje ugotovitve imajo v praksi pomembne posledice. Kažejo na to, da je potrebno za uspešnost EPS-ja zagotoviti ustrezna tehnična merila in socialna pravila, ki zagotavljajo varnost plačevanja prek interneta. Pomembno je kdo zagotavlja tehnične rešitve in izvaja ukrepe v primeru zlorabe zaupanja, saj je vpliv zaupanja v banko zelo velik tako v primeru kupca, kakor v primeru prodajalca.

Če povlečemo vzporednico s klasičnimi plačilnimi sistemi, za trdnost katerih je zadolžena centralna banka, lahko domnevamo, da bo potrebno v prihodnje razmišljati o podobnih institucionalnih rešitvah tudi pri plačevanju prek interneta. Da bo z vidika uporabnikov interneta plačevanje prek interneta za nakupe v spletnih trgovinah splošno sprejemljivo in sprejeto, je potrebno zagotoviti trdnost elektronskega plačilnega sistema, tega pa je mogoče zagotoviti le na način, da uporabniki interneta zaupajo ustanovi, ki odgovarja za njegovo varnost in zanesljivost.

## 2.4 Osnovne tehnike

Za razumevanje razlik v delovanju je potrebno poznavanje osnovnih tehnik elektronski plačilnih sistemov.

### 2.4.1 Kriptografija

Kriptografija se že stoletja uporablja za zaščito zaupnih podatkov, ki jih je potrebno poslati iz ene lokacije na drugo. Ko govorimo o kriptografiji, mislimo na šifriranje podatkov v takšno obliko, da nepooblaščeni uporabniki ne morejo razbrati njihove vsebine. V preteklosti je bila kriptografija v domeni vojske, z razvojem javnih računalniških omrežij in vse večjega števila uporabnikov pa je postala nepogrešljiva tudi na tem področju. S pomočjo kriptografskih sistemov lahko dosežemo verodostojnost, tajnost in nezmožnost tajenja sporočila.

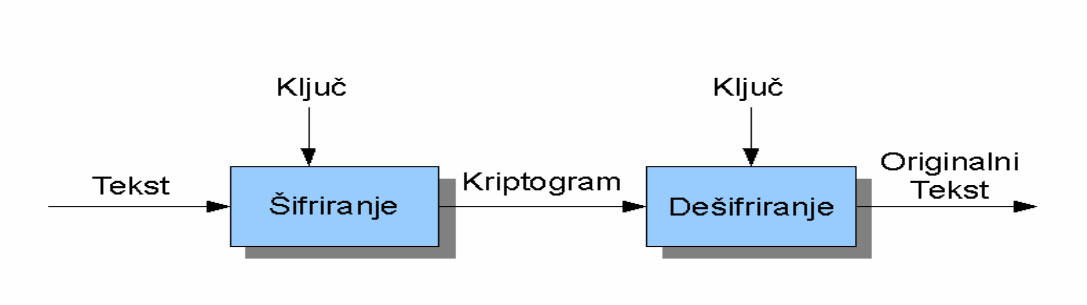
Kriptografski sistem sestavljata dva dela: kriptografski algoritem in šifrirni ključ. Kriptografski algoritem je matematična funkcija, ki podatke s pomočjo šifrirnega ključa spremeni v nepooblaščenim osebam neberljivo obliko. V preteklosti so bili algoritmi tajni, saj je že njihovo poznavanje zadostovalo za dešifriranje sporočila, dandanes pa so kriptografski algoritmi večinoma poznani in dostopni vsakomur, skriti morajo ostati le šifrirni ključi. Število možnih ključev pri algoritmu je odvisno od dolžine ključa (8-bitni ključ omogoča 256 možnih numeričnih kombinacij, kar je tudi število različnih ključev). Stopnja varnosti algoritmov za šifriranje je odvisna od dolžine ključa. Ključa dolžine 128 bitov s pomočjo metode preizkusa vseh možnih kombinacij (angl. *brute force*) in trenutno zmogljivostjo osebnih računalnikov ne najdemo v nekaj milijonih letih (Jerman Blažič, 2001).

V grobem ločimo dve vrsti kriptografskih algoritmov: simetrične in asimetrične.

**Simetrična kriptografija**

Simetrična kriptografija, znana tudi kot kriptografija skritih ključev, uporablja en sam skrivni ključ za šifriranje in dešifriranje. Problem pri simetričnem šifriranju je kako varno razdeliti šifrirne ključe pooblaščenim osebam. Pošiljatelj sporočila se mora z vsakim prejemnikom posebej dogovoriti, kateri je skrivni ključ, kar pa povečuje možnost, da kdo ta skrivni ključ prestreže in dešifrira sporočilo. Prednost simetričnega šifriranja je v njegovi hitrosti. V današnjem času se uporablja predvsem v kombinaciji z drugimi algoritmi, ki omogočajo varno izmenjavo ključev. Najbolj znan standard za simetrično šifriranje je DES (angl. *Data Encryption Standard*), ki pa ga zaradi prekratkih ključev danes ni več tako zelo varno uporabljati. Pomembnejši algoritmi so še IDEA (angl. *International Data Encryption Algorithm*), 3DES, CAST5, BlowFish, Serpent, Twofish, RC4 in v zadnjem času AES (angl. *Advanced Encryption Standard*) z 256 bitnim ključem (Oppliger, 2003). Slika 1 prikazuje potek šifriranja s simetričnim algoritmom.

***Slika 1: Potek šifriranja s simetričnim algoritmom***



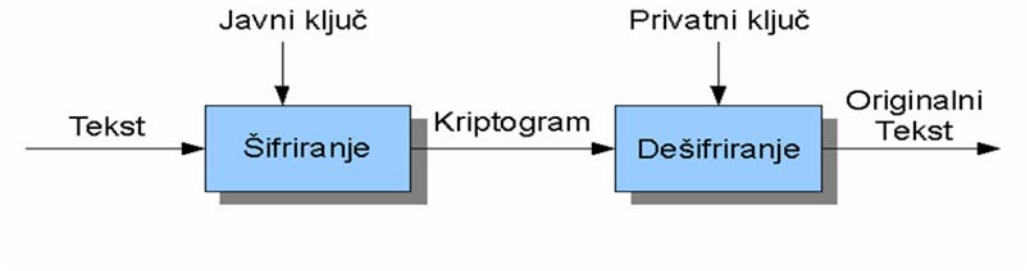

*Vir: Oppliger, Security Technologies for the World Wide Web, 2003.*

**Asimetrična kriptografija**

Asimetrična kriptografija je znana tudi kot kriptografija javnih ključev. Začetnika v asimetrični kriptografiji sta bila W. Diffie in M. Hellman, ki sta leta 1976 prvič predstavila koncept javne kriptografije. Koncept kriptografije javnega ključa temelji na paru ključev: en ključ je namenjen šifriranju, drugi pa dešifriranju sporočila. Vsak uporabnik ima tako dva ključa: zasebni ključ in javni ključ. Javni ključ se ponavadi nahaja na strežniku in je dostopen vsakomur, zasebni ključ pa je varno shranjen pri njegovem lastniku. Ključa sta matematično sorodna, a se med seboj toliko razlikujeta, da je na podlagi enega ključa nemogoče odkriti drugega. Najpogosteje uporabljen asimetrični kriptografski algoritem je RSA (poimenovan po njegovih izumiteljih Rivest-Shamir-Adelman), ki temelji na zelo velikih praštevilih. V zadnjem času na pomembnosti pridobivajo asimetrični algoritmi na podlagi eliptičnih krivulj. Njihova prednost pred RSA algoritmom je predvsem večja hitrost ob enaki stopnji varnosti (Oppliger, 2003).

Pri asimetrični kriptografiji pošiljatelj zaupno sporočilo šifrira z naslovnikovim javnim ključem. Naslovnik, ki ima edini ustrezen zasebni ključ, lahko dešifrira sporočilo. Slika 2 prikazuje postopek šifriranja z asimetričnim algoritmom. Če želimo zagotoviti še neokrnjenost sporočila in verodostojnost pošiljatelja, uporabimo postopek digitalnega podpisovanja, ki ga omogoča kriptografija javnih ključev.

***Slika 2: Potek šifriranja z asimetričnim algoritmom***




*Vir: Oppliger, Security Technologies for the World Wide Web, 2003.*

Prednost asimetrične kriptografije pred simetrično je v enostavnem razpošiljanju ključev. Javni ključ lahko brez kakršnegakoli strahu, da bo ta prestrežen, pošljemo osebi, s katero želimo varno komunicirati, ali pa ga le-ta preprosto sname iz za ta namen prirejenih strežnikov. Slabost asimetričnih algoritmov v primerjavi s simetričnimi je predvsem v hitrosti šifriranja in overjanja javnih ključev. Hitrost šifriranja je odvisna od dolžine ključa. Šifriranje in dešifriranje z 1028 bitnim ključem pri RSA algoritmu, ki zagotavlja podobno stopnjo varnosti kot 72 bitov dolg ključ pri simetričnih algoritmih, je nekajkrat počasnejše. Zaradi te pomanjkljivosti daljša sporočila običajno šifriramo s simetričnimi kriptografskimi algoritmi, ključe za te algoritme pa

zaščitimo z asimetričnimi. Kriptografske sisteme, sloneče na javnih ključih, tako uporabljamo večinoma pri šifriranju ključev.

### 2.4.2 Infrastruktura javnih ključev

Celoten sistem za uporabo varnostnih metod na podlagi asimetrične kriptografije v elektronskem poslovanju imenujemo infrastruktura javnih ključev (angl. *Public Key Infrastructure* v nadaljevanju PKI). Infrastruktura javnih ključev je kombinacija programske in strojne računalniške opreme ter politike in pravil overjanja. Osnovna naloga PKI je omogočiti varno elektronsko poslovanje uporabnikom, ki se med seboj ne poznajo in želijo varno komunicirati. PKI temelji na digitalnih certifikatih, s katerimi potrdimo uporabnikov elektronski podpis in njegov javni ključ. PKI kot celoten sistem v elektronskem poslovanju lahko združuje naslednje subjekte in dokumente:

- agencija za overjanje (angl. *Certification Authority* v nadaljevanju CA);
- agencija za registracijo (angl. *Registration Authority* v nadaljevanju RA);
- politika overjanja;
- sistem distribucije certifikatov;
- dokument o ravnanju s certifikati (angl. *Certification Practices Statement* v nadaljevanju CPS).

**Agencija za overjanje**

Osnovna naloga CA je izdajanje, varovanje in vzdrževanje certifikatov. Zaupanje v PKI temelji na CA. CA običajno skrbi za objavo črne liste certifikatov (angl. *Certificate Revocation List* v nadaljevanju CRL).

**Agencija za registracijo**

RA urad predstavlja posrednika med CA in uporabnikom. RA od naročnika, ki zaprosi za certifikat, pridobi podatke in jih preveri. Po uspešno končani registraciji naročnika pošlje do CA zahtevo za izdajo digitalnega certifikata. Zelo pomembno je zaupanje CA v verodostojnost podatkov, ki jih dobi od RA.

**Politika overjanja**

V grobem ločimo dve politiki overjanja: politiko overjanja na globalni ravni PKI, ki ureja odnose med CA, RA, lastniki in uporabniki certifikatov, ter politiko overjanja v posameznih organizacijah z lastno CA. Politika overjanja v organizaciji določa stopnjo zahtevane varnosti in vključuje dokumente, s katerimi so predpisani postopki ravnanja s ključi in drugimi pomembnimi podatki.

**Sistem distribucije certifikatov**

Certifikati so lahko distribuirani na več načinov. Izmenjajo si jih lahko uporabniki sami, le-ti se nahajajo na strežniku v organizaciji ali pa na posebnem strežniku v javnem omrežju. Način distribucije je odvisen od strukture PKI.

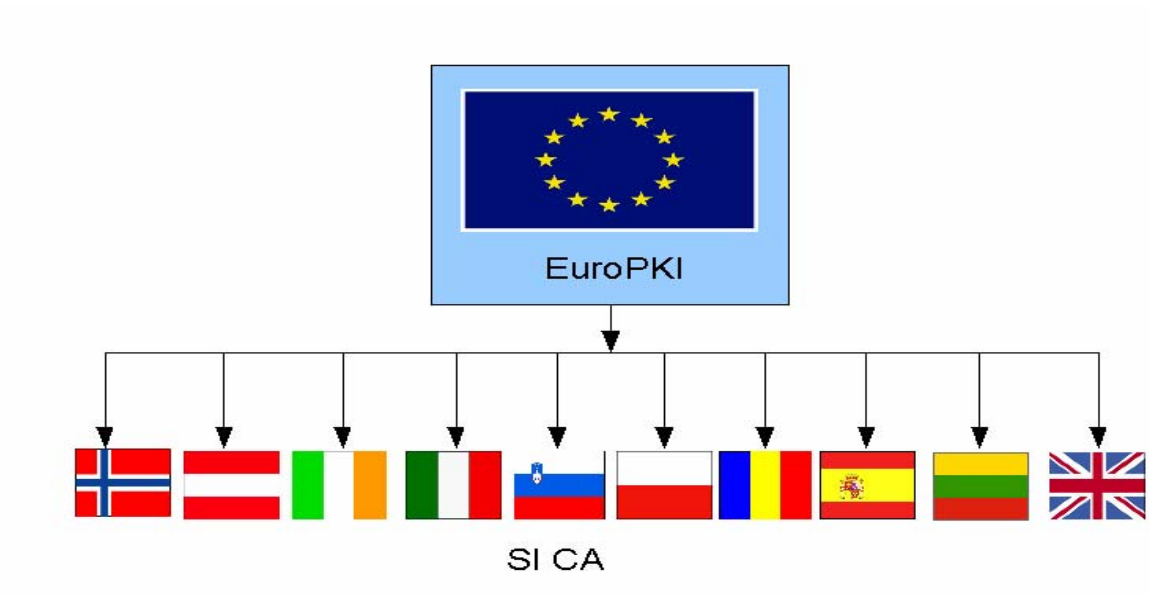
**Dokument o ravnanju s certifikati**

CPS je dokument, ki definira natančne postopke izvajanja politike overjanja v praksi in vsebuje opis strukture CA ter njenih nalog. V njem so podrobno opredeljeni postopki izdaje, sprejetja in preklica certifikata ter njegove distribucije. CPS je posebno pomemben pri komercialnih CA (angl. *Commercial Certificate Authority* v nadaljevanju CCA), saj iz njega lahko razberemo, koliko zaupanja je vredna posamezna CA.

**EuroPki**

Ključi se lahko uporabljajo za različne namene in v različnih okoljih kot so elektronsko bančništvo, državna uprava, medorganizacijsko poslovanje, vojska, itd. Vsako okolje zahteva različno stopnjo varnosti in specifično strukturo PKI, zato ni pričakovati enotne PKI. Infrastrukture med seboj niso povezane, večina jih vsebuje le eno ali nekaj CA. Ena redkih PKI, katerih namen je združevanje CA iz različnih držav, je EuroPKI.

***Slika 3: Struktura EuroPKI***




*Vir: EuroPKI.org, 2008.*

Vrhovna agencija EuroPKI deluje v Italiji in ima pod okriljem več držav, ki so razvidne iz Slike 3. Del te infrastrukture je tudi slovenska agencija za overjanje SI-CA, katera podpisuje javne ključe drugih slovenskih overiteljev. V Sloveniji imajo še svoj CA: Center vlade Republike Slovenije za informatiko SIGEN CA (izdaja kvalificirana digitalna potrdila za državljane ter za pravne in fizične osebe), SIGOV CA (izdaja kvalificirana digitalna potrdila za institucije javne uprave), Halcom, NLB (Nova Ljubljanska banka), Pošta Slovenije (Jerman Blažič, 2001).

**Digitalni certifikat**

Kriptografija na osnovi javnega ključa temelji na paru ključev. Par ključev lahko izdelamo sami, in sicer s programi kot so internetni brskalnik, programi za elektronsko pošto ter drugi. Ko sta ključa izdelana, lastnik poskrbi za ustrezno zaščito zasebnega ključa, javni ključ pa po elektronski pošti razpošlje osebam, s katerimi želi varno komunicirati. Tak način izdelave ključev ni najboljši, saj se ne zagotavlja verodostojnost pošiljatelja. Pošiljatelj lahko izdela par ključev v imenu neke druge osebe, za katero se izdaja, in naslovnik tako ne more biti povsem prepričan, ali je pošiljatelj res oseba, za katero se izdaja. Da se tem težavam izognemo, je overjanje javnih ključev temeljni pogoj za zagotavljanje verodostojnosti pri asimetrični kriptografiji. Overjanje javnih ključev opravljajo agencije CA. CA izda lastniku javnega ključa digitalno podpisano potrdilo – digitalni certifikat, s katerim zagotavlja drugim uporabnikom verodostojnost ključa. Pri uporabi javnega ključa moramo najprej preveriti veljavnost certifikata ter ostale podatke, zapisane v njem. Če certifikat od časa izdaje ni bil spremenjen ali preklican, ga lahko uporabimo. Zelo pomembno je naše zaupanje v CA, da res izdaja certifikate le pravim lastnikom javnih ključev. Certifikate lahko, glede na preverjanje podatkov lastnika ob izdaji, razvrstimo v štiri razrede, ki so opredeljeni z varnostno politiko CA na njenem strežniku. Za certifikate prvega razreda se preverja le elektronski in klasični naslov lastnika. Pri certifikatih drugega razreda se preveri osebni dokument, pri certifikatih tretjega razreda pa se preveri še lastnikova kreditna kartica. Certifikat četrtega razreda vsebuje tudi podatke o položaju znotraj organizacije oziroma o premoženjskem stanju lastnika.

Agencijo CA lahko ustanovijo tako vladne ustanove kot komercialne organizacije. CA poleg izdajanja certifikatov vzdržuje tudi bazo preklicanih in neveljavnih certifikatov, kjer lahko uporabnik preveri veljavnost certifikata. CA mora pri svojem delu izpolnjevati tudi vrsto varnostnih zahtev (Jerman Balažič, 2001), kot so:

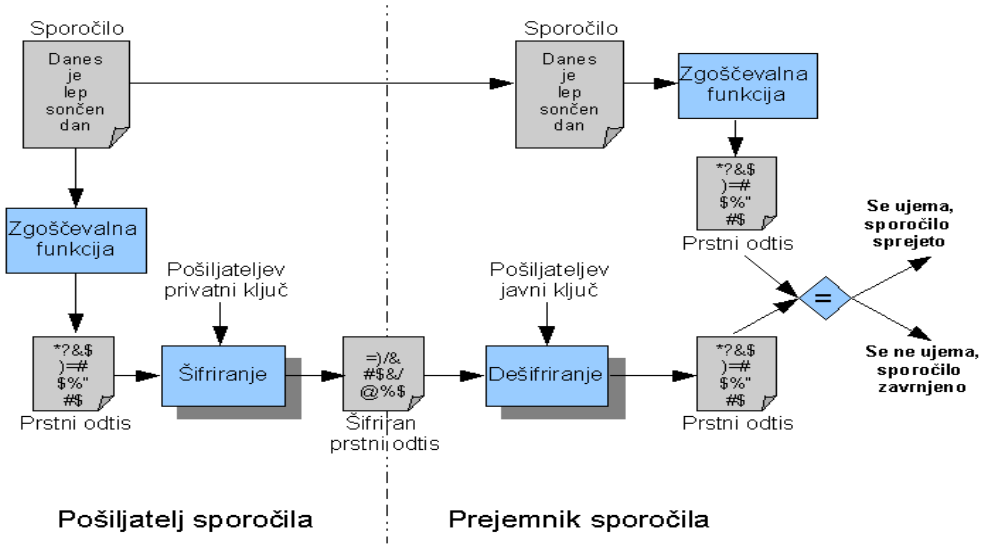
- delovna postaja CA mora biti dobro fizično varovana;
- povezava z omrežjem je omejena in strogo varovana;
- CA ne sme nuditi drugih storitev;
- upravljanje delovne postaje iz omrežja ne sme biti možno;
- zasebni ključ CA mora biti shranjen v varnem strojnem šifrirnem modulu, sicer CA ne sme biti priključena na omrežje;

- CA mora za podpisovanje uporabljati par ključev, narejenih z algoritmom RSA, dolžine vsaj 1024 bitov.

### 2.4.3 Digitalni podpis

Digitalni podpis je vrsta elektronskega podpisa, ki temelji na asimetrični kriptografiji. Enako kot pri kriptografiji javnih ključev ima uporabnik dva ključa: javni ključ in zasebni ključ. Uporabimo lahko isti par ključev kot pri asimetričnem šifriranju, vendar to ni priporočljivo, saj so varnostne zahteve v obeh primerih precej različne. Ponavadi ima uporabnik še en par ključev, ki je namenjen le za digitalno podpisovanje. Postopek digitalnega podpisovanja poteka v dveh korakih. Sporočilo najprej skrčimo z eno izmed enosmernih zgoščevalnih funkcij[3] v bloke enakih dolžin. Z zgostitvijo sporočila v konstantno velike bloke namreč uničimo pomen sporočila, ki ga je tako nemogoče rekonstruirati v prvotno obliko. Vsaka najmanjša sprememba v izvornem sporočilu povzroči spremembo vsebine bloka. Posamezni blok predstavlja 'prstni odtis' sporočila, ki ga šifriramo še z zasebnim ključem, in tako dobimo digitalni podpis. Za preverjanje digitalnega podpisa prejemnik uporabi javni ključ podpisnika, s katerim dešifrira blok. Prejemnik nato še sam izračuna vrednost enosmerne zgoščevalne funkcije podpisanega sporočila in primerja bloka. Če sta bloka popolnoma enaka, je pošiljatelj res oseba, za katero se izdaja in poslano sporočilo med prenosom ni bilo spremenjeno (Centeno, 2001). Slika 4 ilustrira celoten postopek digitalnega podpisovanja.

***Slika 4: Prikaz postopka digitalnega podpisovanja***




Vir: lasten.

[3] Zgoščevalne funkcije so matematične metode, ki vhodne podatke poljubne dolžine spremenijo v podatek fiksne dolžine (prstni odtis).

### 2.4.4 Varno komuniciranje

Internet združuje veliko množico najrazličnejših računalnikov in uporabnikov, da pa se lahko ti med seboj sporazumevajo, uporabljajo protokole. Protokoli tako predstavljajo množico pravil ali dogovorov o tem, kako komunicirati in kako razumeti preneseno sporočilo. V glavnem lahko uporabljene protokole na internetu delimo v skupine komunikacijskih, programskih in varnostnih protokolov. Pri komunikacijskih protokolih gre za vrsto pravil, po katerih si računalniki izmenjujejo informacije, medtem ko programski protokoli skrbijo za formatiranje zahtev, ki jih postavlja uporabnik ter prikaz podatkov, ki so odgovor na omenjene zahteve. Varnostni protokoli omogočajo vzpostavitev varne šifrirane povezave med dvema točkama (strežnik/odjemalec). V sistemu za e-poslovanje lahko zagotovimo varnost na različnih ravneh. Najpogosteje uporabljeni varnostni protokoli so v najbolj razširjenem protokolu TCP/IP[4] (angl. *Transmision Control Protocol / Internet Protocol*) in to na aplikacijski, transportni in omrežni ravni.

**HTTP protokol**

HTTP (angl. *HyperText Transfer Protocol*) je protokol na aplikativni plasti TCP/IP protokola. Služi prenosu informacij na internetu. Protokol je bil prvotno namenjen objavljanju in prejemanju HTML strani, kasneje pa tudi za pošiljanje drugih vsebin.

Razvoj HTTP so koordinirali WWW konzorcij in delovne skupine za medmrežni inženiring. Rezultat je bila publikacija serije RFC[5] (angl. *Request for Comments*), predvsem RFC 2616, ki definira HTTP/1.1, torej različico dandanes v pogosti rabi (Wikipedia, 2008a).

HTTP je komunikacijski protokol med odjemalci in strežniki. HTTP odjemalec, kot na primer spletni brskalnik, navadno začne zahtevo tako, da vzpostavi TCP povezavo na izbrana vrata na oddaljenem strežniku (privzeta je številka vrat 80). HTTP strežnik, ki na teh vratih pričakuje, da bo odjemalec poslal svoj zahtevek na primer "GET / HTTP/1.1" (ta zahtevek prosi za privzeto spletno stran na strežniku). Ko strežnik prejme tak zahtevek, nanj odgovori na primer z "200 OK" in lastnim sporočilom, katerega vsebina je zahtevana datoteka, sporočilo o napaki ali pa kakšna druga informacija.

[4] TCP/IP je množica protokolov, ki izvaja protokolski sklad prek katerega se izvaja internet. Največ omrežnega prometa poteka preko protokola TCP. Sporočila preko protokola TCP se zaradi vzpostavljene povezave med odjemalcem in strežnikom prenašajo zanesljivo v obe smeri, so brez napak, podvojevanja in v pravem vrstnem redu (Wikipedia, 2008e).

[5] RFC ali zahteva po razlagi je dokument, ki določa tehnične vidike Interneta. V začetku so ti dokumenti služili za zbiranje informacij tehničnih udeležencev v omrežju. Veliko RFC-jev temu namenu služi še danes, številni pa so samo zapisi dejstev (Wikipedia, 2008f).

V HTTP protokolu so definirani naslednji komunikacijski zahtevki:

- **GET** je najbolj pogosta metoda za pridobitev vsebine datoteke;
- **HEAD** je identičen zahtevek GET-u, le da strežnik nanj odgovori le z glavo datoteke. Uporablja se za pridobivanje meta-oznak;
- **POST** je podoben zahtevek GET-u, vendar telo zahtevka vsebuje tudi podatke, ki jih želimo sporočiti strežniku;
- **PUT** se uporablja za pošiljanje datotek na ciljni spletni strežnik;
- **DELETE** zbriše datoteko s strežnika (se ne uporablja pogosto);
- **TRACE** vrne nazaj zahtevek, zato da lahko odjemalec ugotovi, če so vmes dodatni strežniki, ki spreminjajo zahtevke;
- **OPTIONS** vrne seznam HTTP zahtevkov, ki jih strežnik omogoča. Zahtevek se uporabi za ugotavljanje delovanja spletnega strežnika;
- **CONNECT** se uporablja pri spletnih posrednikih za vzpostavitev SSL tunela.

**SSL/TLS**

SSL je varnostni protokol med transportnim in aplikativnim nivojem, ki ga je razvilo podjetje Netscape, da bi zagotovilo varno povezavo med odjemalcem in strežnikom, ki komunicirata prek javnega kanala. Implementiran je v večino najpogosteje uporabljenih brskalnikih in internetnih strežnikih (Robinson, 2001).

Protokol SSL pogosto uporabljajo banke v e-bančništvu. Uporabnik se najprej prepriča, ali res komunicira s pravim končnim strežnikom. Protokol SSL zagotavlja:

- šifriranje podatkov;
- overjanje strežnika in odjemalca;
- zaupnost sporočil;
- neoporečnost sporočil.

Protokol SSL je sestavljen iz dveh delov:

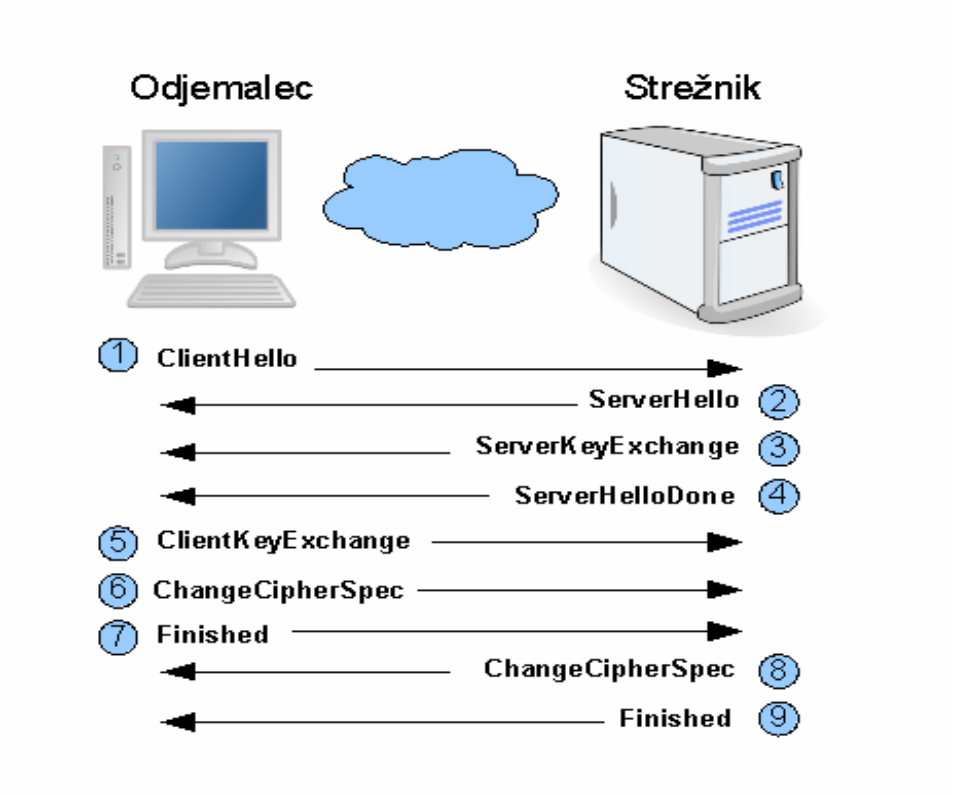
1. Zgornji sloj
    - SSL protokol rokovanja (angl. *handshake*) – so protokoli, ki poskrbijo za to, da se strežnik in odjemalec medsebojno preverita, se dogovorita za način šifriranja podatkov, si varno izmenjata simetrični ključ in dogovorita ter uskladita algoritme;
    - SSL protokol obveščanja (angl. *alert*) – skrbi za obveščanje o napakah ali prekinitvah na povezavah pri komunikaciji;
    - SSL zamenjava načina šifriranja (angl. *change cipher spec*) – namenjen zamenjavi šifriranja ter za potrjevanje o dogovorjenih parametrih med strežnikom in odjemalcem.

2. Spodnji sloj

- SSL protokol zapisa (angl. *record protocol*) – deluje kot nivo pod vsemi sporočili SSL in določa način šifriranja in zaščito celovitosti, ki se bodo uporabili. Podatke razbije na bloke določene dolžine ter vsakemu doda zaporedno številko sporočila, tip zapisa ter dolžino bloka podatka. Iz teh podatkov se izračuna MAC[6] (angl. *Message Authentication Codes*), ki služi kontroli nespremenljivosti podatkov ter overjanju sporočila.

Strežnik in odjemalec pri vzpostavitvi povezave najprej na podlagi prvega protokola preverita identiteto drug drugega, uskladita kriptografske algoritme ter si varno izmenjata ključ seje in ostale podatke, ki so potrebni za morebitno kasnejše šifriranje (Blažič Jerman, 2001). Protokol SSL nima fiksno določenih algoritmov za šifriranje, tako da jih lahko določijo proizvajalci programskih aplikacij sami. Slika 5 prikazuje potek rokovanja med odjemalcem in strežnikom pri vzpostavitvi SSL povezave (prevod imen sporočil iz Slike 15 bi bil brezpredmeten, saj bi tako iz imena izgubili pomen sporočila). Na njej je prikazano zaporedje sporočil rokovanja.

***Slika 5: Potek izmenjave sporočil SSL rokovanja***




*Vir: Stephen, SSL & TLS Essentials Securing the Web, 2000.*

[6] MAC je algoritem, ki matematično poveže ključ in zgoščevalno funkcijo v šifro. Šifra MAC služi zagotavljanju integritete podatkov, nad katerimi je bila izvedena zgoščevalna funkcija.

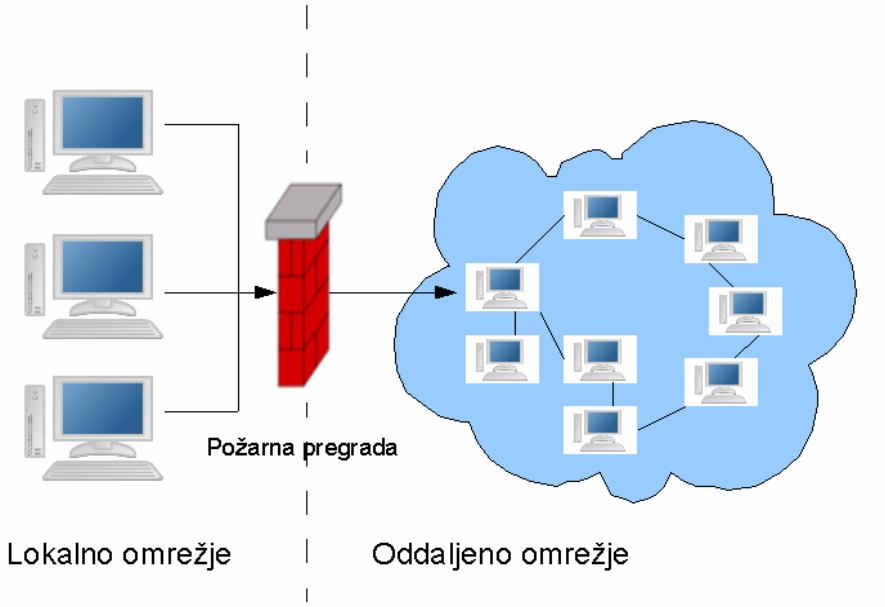
## Požarna pregrada

Požarno pregrado ali požarni zid (angl. *firewall*) si lahko predstavljamo kot varnostna vrata ali vratarja, ki nepooblaščenim osebam ne dovoli vstopa v omrežje, po drugi strani pa ne dopušča odnašanja podatkov iz omrežja. Požarna pregrada v obliki strojne ali programske opreme implementira varnostno politiko v zvezi z uporabo virov in sistemov v lokalnem omrežju. Osnovna zahteva pri postavitvi požarne pregrade je, da imajo vsi uporabniki lokalnega omrežja čim manj oviran dostop do javnega omrežja, iz omrežja internet pa v lokalno omrežje prepuščamo le povezave do javnih strežnikov.

Požarna pregrada je tako namenjena preverjanju podatkov, ki se prenašajo med lokalnim omrežjem in internetom. Filter je tista komponenta požarnega zidu, ki nad vsakim paketom izvede množico pravil iz varnostne politike, določenih s strani administratorja. Pravila temeljijo na selektivni osnovi, ki filtrira vhodne dostope v svoje omrežje in preverja pravila, ki lahko temeljijo na uporabniških imenih, internetnih IP naslovih pošiljatelja ali prejemnika, imenih domen, številkah komunikacijskih vrat, itd. (Kalakota, 1997).

Požarna pregrada ne more varovati virov podjetja pred napadi iz notranjega omrežja, saj je lahko le vmesnik med internim omrežjem podjetja in internetom ali vmesnik med posameznimi oddelki podjetja (običajno se uporablja v večjih podjetjih). V vsakem primeru lahko zaposleni v podjetju ukrade ključne informacije podjetja in poškoduje poslovne vire, ne da bi se to prikazalo na požarni pregradi (Collin, 1998). Slika 6 prikazuje tipično postavitev požarne pregrade med lokalnim in oddaljenim omrežjem.

***Slika 6: Umestitev požarne pregrade med lokalnim in oddaljenim omrežjem***




*Vir: Wikipedia, Firewall, 2008b.*

### 2.4.5 Strojno varovanje ključev

Kriptografski ključi, ki se uporabljajo v različne namene, morajo biti varno shranjeni. Z razkritjem ključa tudi najbolj varen protokol komunikacije ni več varen. Lahko se reče, da je varnost pogojena s tem, koliko je sam ključ, ki se uporablja v komunikaciji, varno shranjen. Ključi so lahko shranjeni programsko v programski opremi ali pa v posebnih napravah imenovanih strojni šifrirni moduli (angl. *Hardware Security Module* v nadaljevanju HSM). Na nekaterih področjih (na primer v agencijah za overjanje in bankah) morajo biti vsi ključi, z razkritjem katerih bi bilo ogroženo poslovanje inštitucije, varno shranjeni v HSM napravah. Pametna kartica ima podobne lastnosti kot HSM, zato jo uvrščamo med HSM-je.

**Strojni šifrirni moduli**

HSM je strojna naprava in njemu pripadajoča programska oprema. Ponavadi je HSM priključen na računalnik in ponuja vsaj minimalne kriptografske funkcije. Take funkcije so šifriranje, dešifriranje, izdelava ključev, računanje zgoščevalne funkcije, itd. Naprave ponujajo uporabniški in razvojni vmesnik ter so fizično odporne na vdore.

HSM izvaja številne varnostne funkcije ter omogoča pohitritev kriptografskih operacij. Naprava se lahko uporablja tudi za zaščito baze podatkov z zaupnimi podatki. Zaupen podatek je na primer stanje bančnega računa. Naprava se v tem primeru obnaša kot vmesnik za šifriranje podatkov pred vnosom ali pa za dešifriranje podatkov pred ogledom. Ker HSM varuje ključ, ki je bil uporabljen za izračun MAC kode stanja, ne more teoretično nihče drug reproducirati prave MAC kode stanja računa. Tako je nemogoče, da bi nepooblaščena oseba vnesla želeno stanje v bazo podatkov. Če MAC koda stanja ni pravilna, lahko aplikacija avtomatično sproži ukrepe, kot so log zapisi ali razne oblike sporočanja varnostnega incidenta.

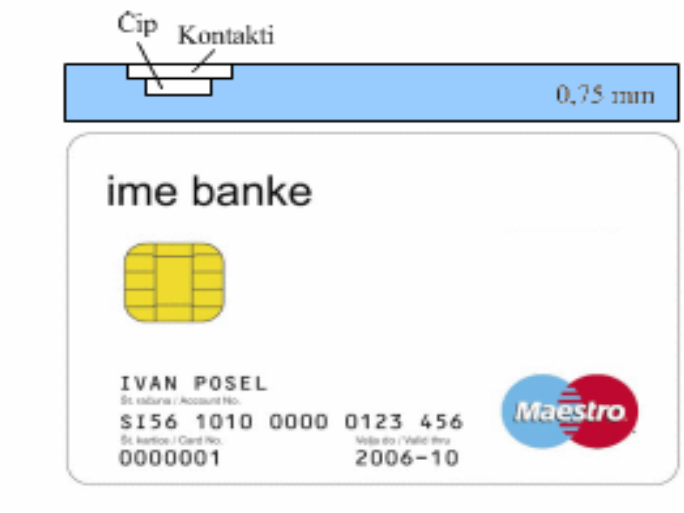
HSM-ji morajo znati upravljati s ključi, kar pomeni, da skrbijo za rezervno kopijo ključa in varno prenašanje ključa v druge naprave. Rezervna kopija ključev mora biti narejena preko varne povezave med HSM in drugo napravo, kjer se kopija shrani. Ponavadi se za shranjevanje kopije ključa uporabi več pametnih kartic, ki se jih razdeli med varnostne inženirje. Čitalnik pametnih kartic mora biti neposredno povezan s HSM, saj je na ta način onemogočeno prestrezanje ključa (Attridg, 2002).

**Pametna kartica**

Pametna kartica je plastična kartica z vgrajenim mikroprocesorjem na čipu, ki se je v svetu prvič pojavila leta 1979. Pojem pametna kartica opisuje mikroračunalnik, ki je v ohišju kartice. Tehnologija pametnih kartic nam omogoča prenos in hranjenje informacij s pomočjo integriranega vezja, ki je vgrajen v kartici in v katerem lahko hranimo šifrirni ključ oz. digitalno

potrdilo. Kartica poskrbi, da se podatki z zunanjim svetom izmenjujejo na varen in zanesljiv način. S pomočjo čitalnika je mogoče s pametnimi karticami poslovati kjerkoli (Hendry, 1997). Danes so v bančnem poslovanju pametne kartice nadomestile uporabo kartic z magnetnim zapisom, ki so na trgu prisotne že dlje časa in so cenejše, vendar slabše zaščitene pred zlorabami. S pomočjo posebnih naprav je namreč možno zapis z magnetne kartice enostavno prekopirati na drugo. Magnetno kartico je tudi moč uporabiti brez poznavanja PIN[7] (angl. *Personal Identification Number*) številke, saj za uporabo zadošča že podpis, ki ga lahko oseba brez težav ponaredi. V primerjavi z magnetno kartico dovoli pametna kartica uporabo le z vnosom PIN številke, ki jo pozna samo imetnik kartice. Poleg tega tehnologija pametne kartice preveri ali je terminal, preko katerega poteka plačilo originalen ter preveri pravilnost izvedbe transakcije. Takšen postopek je veliko varnejši, saj je pametna kartica brez poznavanja PIN številke praktično neuporabna in se ob več hkratnih napačnih vnosih blokira. Pametne kartice se lahko uporabijo za varno hranjenje raznih podatkov (Activa, 2007). Slika 7 prikazuje pametno kartico iz prednje in bočne strani.

***Slika 7: Zgled pametne kartice***




*Vir: Activa, Pametna kartica, 2007.*

## 2.5 Razvrstitev elektronskih plačilnih sistemov

Plačilna sredstva, ki se uporabljajo na internetu, so zasnovana tako, da opravljajo enake ali podobne naloge kot klasične oblike plačevanja. V literaturi lahko zasledimo več razvrstitev elektronskih plačilnih sistemov. Nekatere razvrščajo EPS-je po tipu informacije, ki si jo udeleženci izmenjujejo. Tako loči sisteme na tiste, ki uporabljajo račune ali žetone (angl. *token*). Drugi razvrščajo na podlagi denarnega toka med plačnikom in prejemnikom plačila

[7] PIN je osebna identifikacijska številka, ki služi za overjanje posameznika.

(Abrazhevich, 2004). Na svetu obstaja že več kot 150 različnih EPS-jev, nekaj od teh je opisano ali omenjeno v tem poglavju. V magistrskem delu sem EPS-je razvrstil v tri skupine:

- elektronski denar;
- sistemi na podlagi računa;
- kartični plačilni sistemi.

### 2.5.1 Elektronski denar

Elektronski denar je pravzaprav le elektronska različica klasičnega denarja, ki povzema njegove lastnosti (likvidnost, nizki stroški transakcije, anonimnost). Avtor ideje o elektronskem denarju je David Chaum. Elektronski denar je lahko predstavljen kot elektronski kovanec, certifikat, paket podatkov ali elektronski žeton. Za uporabo elektronskega denarja stranke kupijo elektronske žetone od izdajatelja (podjetje, ki je vključeno v plačilni sistem) s kreditno kartico, elektronskim čekom, fizičnim denarjem preko posebnih bankomatov, itd. Nekateri od sistemov omogočajo zamenjavo elektronskega denarja nazaj v klasični denar, kar je zelo pomembna lastnost sistema (Wayner, 1997).

Za elektronski denar je pomembna standardizacija, saj uporabljeni protokoli pri teh sistemih niso medseboj združljivi (Fischer, 2002). Pomembno na tem področju je razvoj standarda za elektronski denar CEPS (angl. *Common Electronic Purse Specifications*). Cilj standarda je definirati zahteve za razvoj globalnega elektronskega denarja. CEPS je bil razvit marca leta 1999, med podporniki je kar 30 držav. Visa Cash je primer sistema, ki izhaja iz CEPS (Abrazhevich, 2004).

Danes najbolj znana sistema z elektronskim denarjem sta Ecash podjetja DigiCash in CAFE, ki so ga razvili s projektom ESPRIT pod okriljem evropske unije. Oba sistema temeljita na elektronski denarnici, ki jo ima uporabnik na svojem računalniku. Med predstavniki te skupine plačilnih sistemov so tudi Egold, Milicent, PayWord, MicroMint in NetCash. Večina od teh sistemov je samo teoretičnih in se jih v produkciji ne uporablja (O'Mahony, Peirce, Tewari, 2001).

**Ecash**

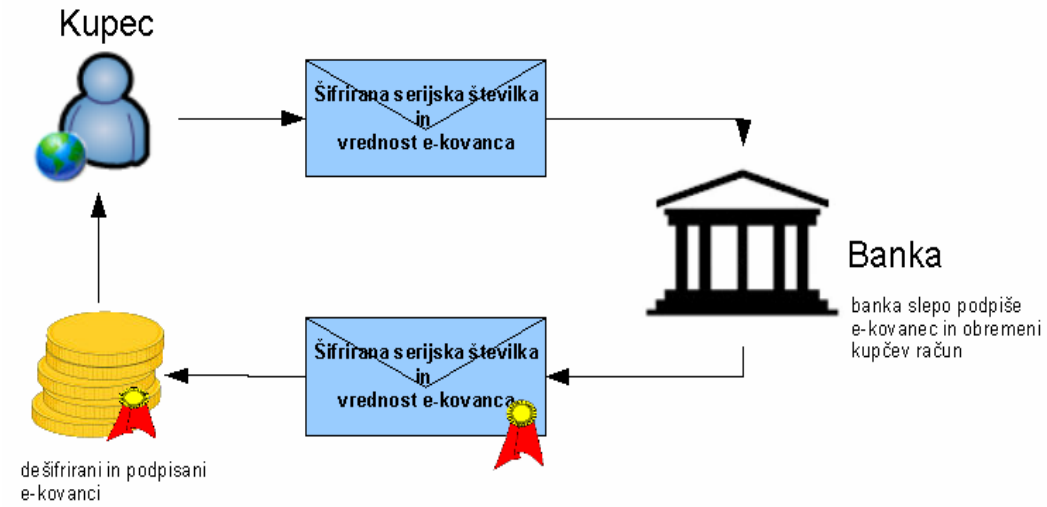
Ecash je varen in anonimen sistem za plačevanje na internetu, ki ga je razvilo podjetje DigiCash. V uporabi je od leta 1995, ko je banka Mark Twain iz ZDA začela kot prva poslovati z elektronskim denarjem.

V sistemu elektronskega denarja Ecash so predvideni trije udeleženci: kupec, prodajalec in banka, ki podpira sistem Ecash. Pri isti banki morata imeti odprt svoj račun tako kupec kot tudi

prodajalec. Kupec dviguje elektronski denar pri banki ter ga shranjuje v elektronsko denarnico, ki jo ima na svojem računalniku. Elektronska denarnica je programska različica klasične denarnice v kateri ima kupec shranjene e-kovance, podatke o transakcijah ter varnostne protokole. Banka ob izdaji e-kovancev bremeni kupčev račun za izdano vrednost. Kupec ima tudi možnost pologa e-kovancev nazaj v banko.

E-kovance v sistemu Ecash soustvarja tudi kupec. Za zagotavljanje anonimnosti plačnika je DigiCash vpeljal posebnost, ki se ji reče slepi podpis. Ta omogoča kupcu dvig denarja in pretvorbo le-tega v e-kovance, ne da bi banka lahko pri tem povezala določene kovance z določenim kupcem, kar je lastnost gotovine. Vsak kovanec ima serijsko številko, ki jo izdela kupčeva elektronska denarnica. Serijska številka je naključno izbrana številka dolžine 100 cifer, zato je tudi majhna verjetnost njene podvojitve. To serijsko število elektronska denarnica pomnoži s slepilnim faktorjem, ki ga pozna le kupec. Tako šifrirano serijsko številko in vrednost e-kovanca v digitalni kuverti pošlje banki. Banka odšteje vrednost kovanca s kupčevega računa in digitalno podpiše kuverto ter jo vrne v kupčevo digitalno denarnico. Banka z digitalnim podpisom jamči vrednost e-kovanca. Kupčeva elektronska denarnica odstrani digitalno kuverto, šifrirano serijsko številko deli s slepilnim faktorjem in tako dobi digitalno podpisan e-kovanec s pravo serijsko številko. Slika 8 prikazuje izdelavo e-kovanca v sistemu Ecash.

***Slika 8: Izdelava e-kovanca v sistemu Ecash***



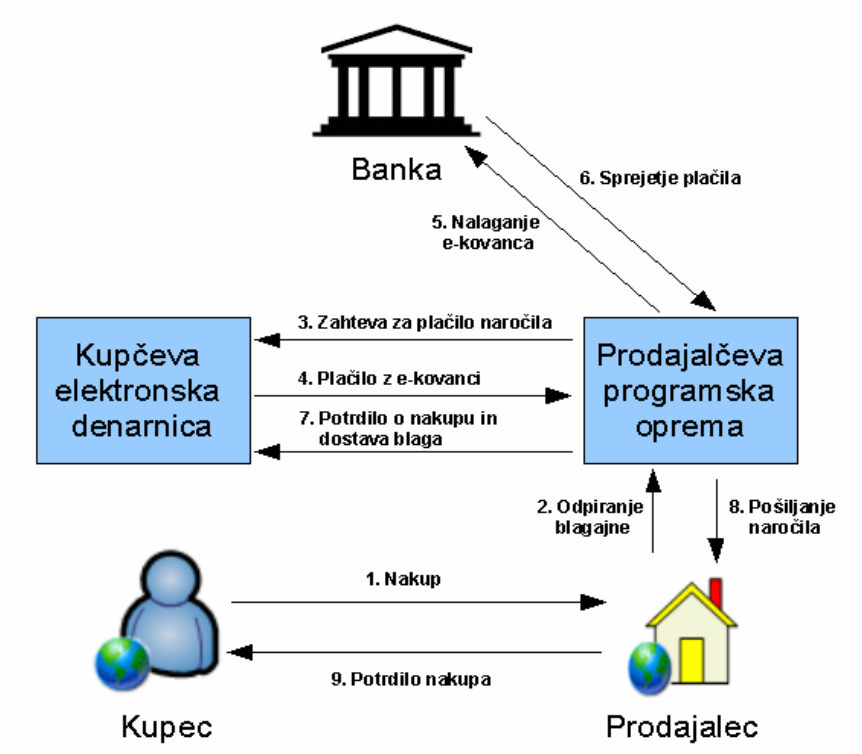

*Vir: O'Mahony, Peirce, Tewari, Electronice Payment Systems for E-Commerce, 2001.*

Ko je kovanec porabljen, banka ne ve, kdo je oseba, ki ga je porabila, vendar mora izplačati na e-kovancu zapisano vrednost, ker se je s svojim digitalnim podpisom zavezala, da bo to storila. Pri prenosu podatkov Ecash uporablja kombinacijo asimetrične RSA kriptografije in simetrične kriptografije. Posebnost elektronskega denarja je tudi v tem, da se lahko izdaja v poljubnih vrednostih in ni nujna preslikava denominacije realnega denarja. Tako ni nujno, da so e-kovanci

v vrednosti 1 EUR, 2 EUR, 5 EUR, 100 EUR, temveč so lahko tudi v vrednosti 164 EUR, 12.26 EUR, itd.

Plačilo poteka tako, da kupec z brskalnikom na trgovčevem strežniku izbere blago in trgovcu pošlje naročilo. Trgovec nato pošlje zahtevo za plačilo kupčevi elektronski denarnici. Zahteva za plačilo vsebuje naslednje podatke: valuto, znesek, datum, podatke o banki in bančnem računu trgovca ter opis naročila. Elektronska denarnica kupca vpraša za potrditev plačila. Ob potrditvi plačila elektronska denarnica pošlje e-kovance na trgovčev račun. V primeru, da v denarnici nima drobiža, se elektronska denarnica poveže z banko in opravi zamenjavo. Trgovec te e-kovance posreduje naprej banki, ki preveri njihovo veljavnost. Banka najprej preveri digitalni podpis, s čimer ugotovi, ali je res ona izdajateljica teh e-kovancev. V drugem delu kontrole pa preveri, če ti e-kovanci morda že niso bili kdaj porabljeni. To naredi tako, da serijsko številko e-kovanca primerja z obstoječo bazo že porabljenih e-kovancev. E-kovanci imajo omejeno časovno veljavnost, s katero nekoliko omejimo količino podatkov v bazi že porabljenih e-kovancev. Če serijska številka e-kovanca že obstaja, je bil ta že porabljen. V tem primeru banka ustavi transakcijo in to sporoči trgovcu. V primeru, da serijskih številk ni v bazi že porabljenih e-kovancev, transakcija poteka naprej. Na trgovčevem Ecash računu se poveča vsota za vrednost prejetih e-kovancev, v bazo že porabljenih e-kovancev pa se vpišejo serijske številke le-teh. Trgovec nato pošlje kupčevi elektronski denarnici še potrdilo o nakupu ter dostavi blago (O'Mahony, Peirce, Tewari, 2001). Slika 9 prikazuje potek nakupa v sistem Ecash.

***Slika 9: Potek nakupa z elektronskim denarjem v sistemu Ecash***




*Vir: O'Mahony, Peirce, Tewari, Electronice Payment Systems for E-Commerce, 2001.*

**Mondex**

Koncept Mondex je leta 1990 razvila angleška bančna organizacija NatWest v sodelovanju z mnogimi zunanjimi sodelavci. Prva poskusna uporaba Mondex-a je bila leta 1992, v katero je bilo vključenih 6000 zaposlenih v NatWestu, ki so lahko v trgovinah in restavracijah znotraj podjetja plačevali z Mondex-ovo kartico. Leta 1995 je prišlo do prve komercialne uporabe, dve leti kasneje pa je večinski lastnik Mondexa postal MasterCard. Sistem Mondex temelji na tehnologiji pametnih kartic. Njegova pomembna značilnost je omogočanje pretoka e-kovancev iz ene v drugo elektronsko denarnico in obratno, brez vmesnega prenosa e-kovancev v banko, katera podpira sistem Mondex. Sistem Mondex je definiran kot protokol med čipi. Za poslovanje z Mondex-ovo kartico (polnjenje, plačevanje in ogled stanja sredstev na kartici) so potrebni čitalniki. Čitalniki so različnih oblik in velikosti, od obeska za ključe, ki omogoča le pregled stanja na kartici, oblike žepnega računalnika, ki omogoča prenos e-kovancev z ene kartice na drugo ter čitalniki, prilagojeni za delo na osebnem računalniku ali mobilnem telefonu. Medij za prenos e-kovancev je lahko internet, telefonska povezava, brezžična povezava ali lokalni čitalnik kartic.

Če se želi postati lastnik Mondex-ove kartice, je potrebno odpreti račun pri banki, ki podpira sistem Mondex. Banka izda kartico in jo napolni z dogovorjeno vsoto e-kovancev, za ta znesek pa bremeni imetnikov račun. Tako kot mnoge druge elektronske denarnice, ki uporabljajo kartico, tudi Mondex-ova zagotavlja informacije za administracijo poslovanja in podatke o opravljenih informacijah. Tako lahko banka spremlja ves pretok denarja na kupčevem in prodajalčevem računu. To omejuje anonimnost sistema, kar mnogi smatrajo kot slabost. Plačilno sredstvo s podobno funkcionalnostjo, ki omogoča tudi anonimnost plačevanja je finska kartica Avant, ki se polni na bančnih avtomatih in je prenosljiva (O'Mahony, Peirce, Tewari, 2001).

### 2.5.2 Sistemi na podlagi računa

Značilno za sisteme na podlagi računa je, da izmenjavo denarja med računi opravlja ponudnik plačilne storitve. Uporabniki lahko avtorizirajo plačila iz svojega elektronskega računa, tako kot bi to počeli s klasičnimi bančnimi računi. Sistemi se med seboj razlikujejo po načinu kako plačnik avtorizira transakcijo. Predstavniki te skupine elektronskih plačilnih sistemov so Yahoo PayDirect, PayPal, Google Checkout ter teoretična plačilna sistema NetBill in NetCheque (Abrazhevich, 2004). V to skupino sistemov prihajajo v letu 2008 nova dva sistema Amazon FPS in SEPA (angl. *Single Euro Payments Area*) on-line kreditna plačila, pri katerem se kot elektronski račun uporablja kar klasični bančni račun.

**PayPall**

Podjetje Paypal je leta 2000 nastalo z združitvijo podjetij Confinity in X.com in se je v začetku usmerilo predvsem v plačevanje storitev prek elektronske pošte, vendar so njegove storitve že do aprila 2000 uporabili v več kot milijon dražbah na dražbeni strani eBay, čeprav je eBay takrat ponujal konkurenčni sistem Billpoint - tega je uporabilo 50-krat manj trgovcev. Čez dve leti je eBay obupal nad tem, da bi presegel konkurenta, in je Paypal preprosto kupil (za podjetje je odštel 1,5 milijarde dolarjev). V naslednjih petih letih so številne finančne ustanove, tudi tako ugledne, kot sta Citibank in Western Union, poskušale s svojimi rešitvami, vendar Paypal-ovega položaja na prestolu med spletnimi finančnimi ponudniki nobena izmed njih ni niti najmanj ogrozila. Edina prednost, ki so jo imeli konkurenti, je bila možnosti uporabe v državah, kjer Paypal še ni bil na voljo. Ker je ta svojo mrežo čedalje bolj širil, je tudi s teh trgov hitro izrinil konkurenco, takoj ko je omogočil plačevanje in sprejemanje plačil v novih državah. V Paypal-u se je leta 2006 pretočilo skoraj 40 milijard dolarjev sredstev. Paypal je bil sicer pravi inkubator podjetnikov in raznih finančnikov, ki so se nato preizkusili pri svojih projektih. Tako so ljudje iz Paypal-a posredno ali neposredno med drugim povezani z ustanovitvijo podjetij LinkedIn, Facebook, SpaceX, Tesla Motors in Youtube. Med državami, ki so dolgo čakale na to, da je Paypal omogočil svoje storitve njihovim državljanom, je bila tudi Slovenija. Paypal omogoča poleg plačevanja tudi prejemanje plačil preko kreditne kartice z dobropisom.

Paypal-ova konkurenčna prednost, a včasih tudi slabost, je varovanje kupcev in prodajalcev pred zlorabami. Tako podjetje v sporu med kupcem in prodajalcem omogoča povrnitev denarja ogoljufanemu kupcu oziroma prodajalca zavaruje pred neutemeljenimi obtožbami kupcev. Težava pri reševanju sporov je, da se pravice kupcev in prodajalcev nekoliko prekrivajo, tako da so postopki reševanja navadno dokaj dolgi. Če gre torej za izdelek, ki ga kupec nujno potrebuje, oziroma imamo na drugi strani prodajalca v finančni stiski, ki potrebuje denar od prodaje, je postopek reševanja pri prodaji nastalega nesporazuma prav nerodno dolg.

Za uporabo Paypal-ovih storitev uporabnik potrebuje le veljaven elektronski naslov in kreditno kartico. Po prijavi svojo identiteto potrdi s tem, da na račun Paypal s kartico naloži majhen znesek (1,5 evra) in vpiše CVC[8] (angl. *Card Verification Code*) kreditne kartice. S tem potrjuje, da je dejanski lastnik te kartice in da so podatki, ki jih je navedel, pravilni, kar mu omogoča uporabo osnovnih storitev kot sta plačevanje izdelkov in storitev z računa ter prejemanje denarja na račun. Pri transakcijah na primer na dražbeni spletni strani ali v trgovini s podporo Paypal tako ni več potrebno vpisovati številke kreditne kartice, ampak le podatke svojega Paypal-ovega računa. Tako se, če Paypal-u seveda zaupamo, izognemo neprijetni situaciji, ko številko kartice vpisujemo na strani, ki jim sicer ne zaupamo. S tem pa drugim tudi omogočamo, da nam nakazujejo denar, ne da bi se bali za svoje osebne podatke ali številke kartic, saj vidimo le

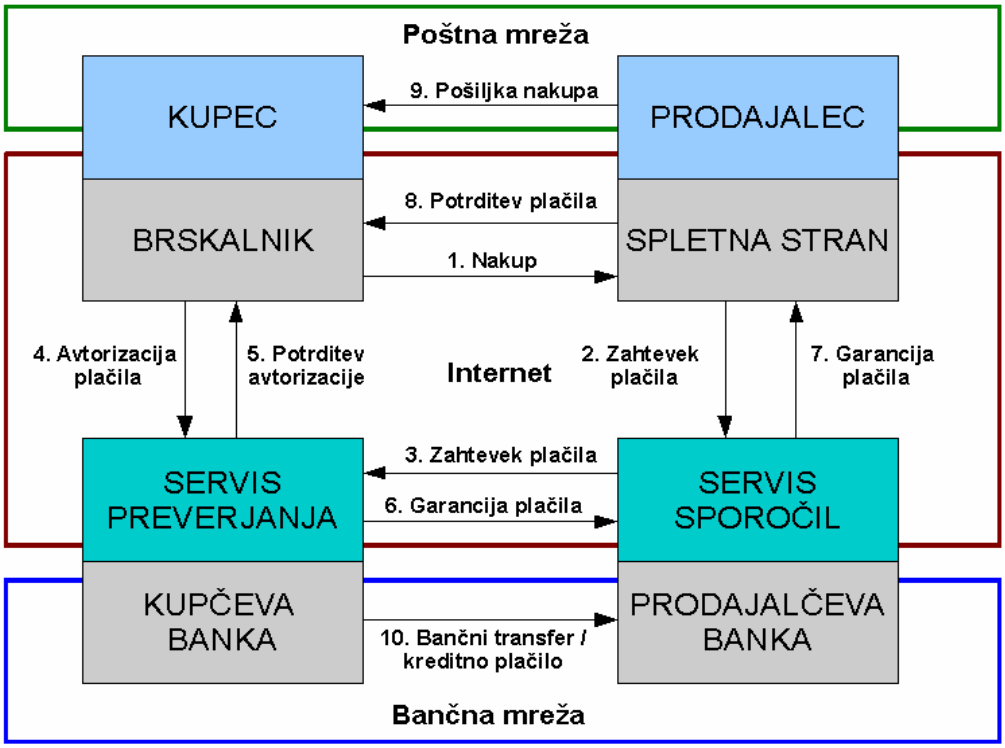
[8] CVC je številka natisnjena na zadnji strani kartice. Koda je nekakšen dodatek številki kartice.

podatke njihovega računa Paypal (Šepetavc, 2007). Iz elektronskega računa PayPal si lahko imetnik kadarkoli z dobropisom prenese sredstva na kreditno kartico.

**SEPA on-line**

Evropsko plačilno združenje je pripravilo predlog, s katerim bi lahko poenotili elektronska plačila v Evro območju in s tem prihranili sredstva. Shema SEPA[9] za 'on-line plačila' deluje na klasičnem štirikotnem modelu kreditnih plačil, kjer obe, banka kupca in banka prodajalca, ponujata svojim komitentom to storitev. Po naročilu blaga s strani kupca preko spletne strani pri prodajalcu sledi zahteva prodajalca po 'on-line plačilu' pri svoji banki, ta pa posreduje zahtevo po 'on-line' plačilu naprej banki kupca. Sledijo nujne avtorizacije, potrditve in garancije plačila. Prodajalec dostavi blago in prejme plačilo, ki ga banka prodajalca kot nepreklicno kreditno plačilo nakaže njegovi banki. Na tak način je zagotovljena varnost in zanesljivost 'on-line' plačil SEPA. Slika 10 prikazuje podrobnejši potek nakupa v sistemu SEPA on-line.

***Slika 10: Potek nakupa v SEPA online sistemu***




*Vir: EPC, SEPA online payment, 2007.*

Prednost te sheme za kupca je širša uporaba 'on-line' plačil preko enotne poznane sheme, prodajalcu pa je zagotovljeno plačilo v realnem času povsod po Evropi. Prednosti na strani bank

[9] SEPA je enotno območje plačil v evrih – evroobmočja (www.sepa.si, 2008).

so razširitev možnosti uporabe obstoječe SEPA infrastrukture za izdelavo novih storitev na svetovnem spletu in boljša izraba obstoječih naložb zaradi povečanega števila transakcij.

Za dokončno delovanje sistema obstajajo še številna odprta vprašanja, kot na primer: jasna opredelitev kriterijev za vključevanje strank, pravna veljavnost sporazumov po različnih državah, vzpostavitev primernih modelov za vse vključene stranke, razlike na področju sodelovanja in konkurence (npr. standardizacija nabora podatkov in sporočil), ipd. (EPC, 2007).

### 2.5.3 Kartični sistemi

Trenutno se velik del elektronskih plačil opravlja s plačilnimi sistemi, ki temeljijo na kreditnih in debetnih karticah. Pri debetnih karticah gre za takojšen odvzem sredstev iz računa, medtem ko se pri kreditnih karticah odvzem sredstev odloži. Velika prednost kartičnih plačilnih sistemov je v tem, da imetniki kartico uporabljajo že na POS terminalih in bankomatih in jim za udeležbo v elektronskem plačilu ni potrebno storiti ničesar dodatnega. Največji problem kartičnih sistemov je v varnosti izvedbe transakcije. Kartični plačilni sistemi niso primerni za mala in mikro plačila, saj je lahko pri takih plačilih strošek izvedbe transakcije krepko višji od zneska plačila. Pri plačilih s kartico na medmrežju gre za tako imenovano CNP (angl. *Card Not Present*) transakcijo. CNP transakcije so tiste, kjer kartica in imetnik kartice nista fizično prisotna v trgovini. Pri CNP transakcijah je zelo težavno preveriti ali je kupec pooblaščen uporabnik kartice, kar omogoča možnost zlorabe kartice. Kartične ustanove so za zmanjšanje števila nepooblaščenih CNP transakcij  začele uvajati varne kartične plačilne sisteme kot so SET, 3D-SET in 3-D Secure (Abrazhevich, 2004).

Ker je predmet magistrske naloge analiza in implementacija varnega kartičnega elektronskega plačilnega sistema 3-D Secure, je sistem podrobno predstavljen v četrtem  poglavju.

**Klasični SSL/TLS način**

Še vedno najbolj pogost način uporabe kartic v elektronskem plačilu poteka na klasičen tako imenovan SSL/TLS način. Pri SSL/TLS načinu mora imetnik kartice za izvedbo transakcije vpisati številko kartice, veljavnost kartice ter CVC kartice. Podatki o kartici se pošiljajo preko varne SSL/TLS povezave do trgovca. Za vzpostavitev SSL/TLS povezave predloži trgovec njegov strežniški certifikat, kar dokazuje, da je trgovec tisti, za katerega se izdaja. Trgovec si podatke kartice shrani in od svoje banke (pridobitelja transakcije) zahteva avtorizacijo transakcije. Pridobitelj pošlje avtorizacijo transakcije preko kartičnih mrež do izdajatelja kartice. Ta v procesu avtorizacije preveri obstoj kartice, datum veljavnosti, CVC ter razpoložljiva sredstva kartice. Sledi proces poravnave sredstev, kjer prodajalčeva banka dobi denar od kupčeve banke in nakaže sredstva na prodajalčev račun. Kupčeva banka zmanjša razpoložljivost sredstev iz kupčevega računa (Jarupunphol, Mitchell, 2003).

**Prednost SSL/TLS načina so:**

- enostavna uporaba. Imetniki kartic lahko uporabljajo SSL/TLS transparentno, saj to omogočajo že vsi spletni brskalniki. Trgovec lahko implementira SSL/TLS brez dodatnih stroškov;
- sistem ni kompleksen, kar omogoča zelo hitro izvedbo transakcije.

**Slabosti SSL/TLS načina so:**

- trgovec ne more identificirati ali je kupec pooblaščen za uporabo kartice. V primeru zlorabe nosi trgovec breme zavrnitve CNP transakcije;
- SSL/TLS varuje samo prenos podatkov, zato mora trgovec vpeljati dodatne varnostne mehanizme za shranjevanje občutljivih podatkov;
- trgovcu omogoča vpogled v podatke kartice.

**SET**

Najbolj znan sistem za varno elektronsko plačevanje s kartico na internetu je protokol za varno transakcijo SET. SET sta leta 1997 razvili podjetji MasterCard in Visa v njunem skupnem podjetju SETco. Pri izgradnji sistema SET je sodelovalo tudi nekaj najbolj znanih podjetij s področja informacijske tehnologije kot so IBM, Microsoft, Baltimore Technologies, Globeset in Verisign. Osnovni namen SET-a je zagotovitev varnega prenosa informacij o plačilu preko zasebnega in javnega omrežja, kot je internet. SET danes predstavlja pomemben mejnik v varnem internetnem plačevanju s kartico, saj vzbuja zaupanje in občutek varnosti vseh udeležencev v procesu plačevanja.

Pri plačevanju s kartico v sistemu SET so udeleženi:

- kupec – lastnik kartice;
- izdajatelj kartice;
- prodajalec / trgovec;
- pridobitelj transakcije.

Za uporabo sistema SET mora lastnik kartice predhodno od izdajatelja kartice pridobiti digitalno denarnico, digitalni certifikat, pametno kartico ali kakšno drugo orodje, ki omogoča overjanje. Digitalna denarnica opravlja podobne naloge kot običajna denarnica. V njej so shranjeni identifikacijski podatki o lastniku kartice, digitalni certifikat, številke kreditnih kartic, računi ter druge informacije, ki so dosegljive, kadar lastnik kartice nakupuje v spletnih trgovinah. Digitalno denarnico, ki jo ima lastnik kartice shranjeno na svojem računalniku, imenujemo klientova denarnica. Digitalna denarnica je lahko shranjena tudi na strežniku izdajatelja kartice in jo

imenujemo strežniška denarnica. Digitalni certifikat omogoča overjanje identitete lastnika kartice. Izda ga izdajatelj kartice in je shranjen v digitalni denarnici lastnika kartice.

Za uporabo sistema SET mora prodajalec pridobiti POS programsko opremo in digitalni certifikat. POS programska oprema omogoča prodajalcu sprejemanje transakcij s strani kupcev ter njihovo kasnejšo avtorizacijo in poravnavo preko pridobitelja transakcije. SET protokol omogoča uporabo kreditne in debetne kartice. Uporablja se ga lahko preko mobilnih naprav kot sta mobilni telefon in dlančnik. Prodajalčev digitalni certifikat omogoča overjanje prodajalca ter hkrati izkazuje odnos med prodajalcem in pridobiteljem transakcije. Digitalni certifikat pridobi prodajalec od svojega pridobitelja.

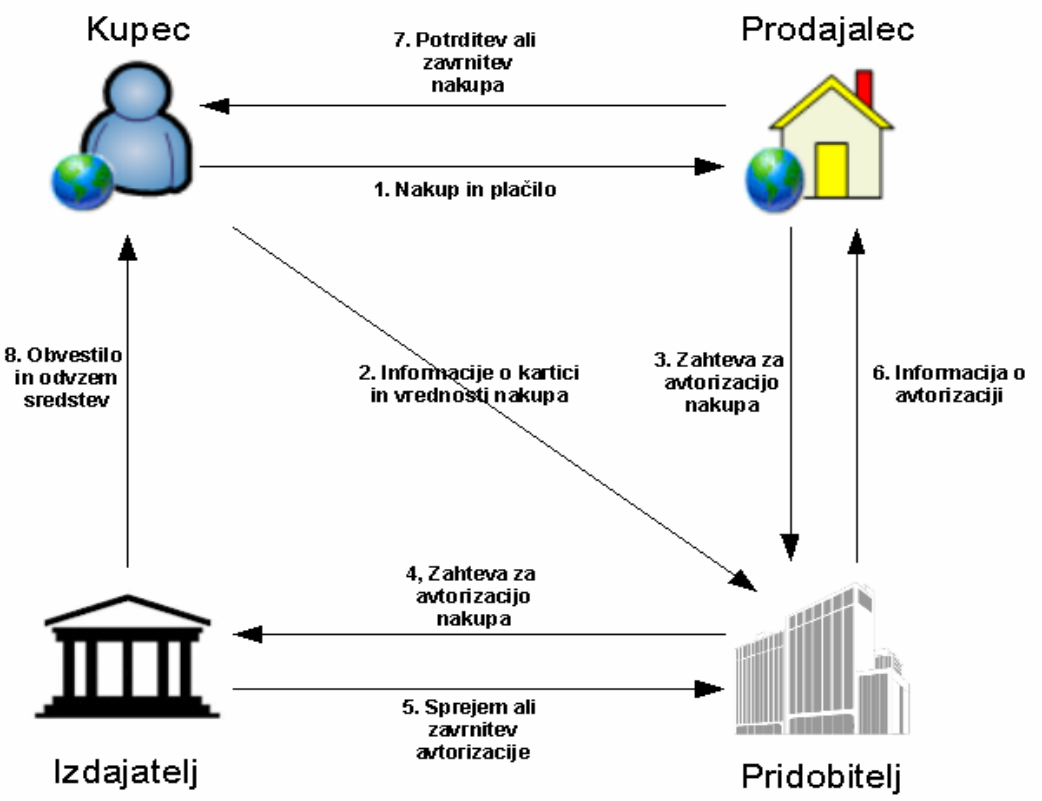
Pridobitelj transakcije mora imeti plačilna vrata, skozi katera se prenašajo SET sporočila, kot so podatki o plačilu, podatki overjanja udeležencev in informacije o naročilu. Glavna naloga plačilnih vrat je sprejemanje sporočil s strani prodajalca in izdajatelja kartice ter njihovo pravilno razvrščanje in usmerjanje (O'Mahony, Peirce, Tewari, 2001).

**Potek nakupa v sistemu SET**

1. Proces transakcije v SET-u se prične, ko kupec v elektronski trgovini izbere želene izdelke in jih položi v virtualno košarico ter potrdi svoje naročilo. Digitalna denarnica dokonča naročilo in ga pošlje naprej;
2. SET programska oprema šifrira vse kupčeve podatke o naročilu ter informacije o kartici in vrednosti naročila s 1024 bitnim ključem. Podatki se preko prodajalčeve programske opreme preusmerijo k plačilnim vratom pridobitelja transakcije. V informacijskem toku prejme prodajalec le kupčevo naročilo in specifikacijo načina plačevanja, vse ostale informacije o plačilu pa so poslane pridobitelju transakcije;
3. Pridobitelj dešifrira podatke o nakupu in prodajalčevo zahtevo za avtorizacijo nakupa. Prodajalec se pri preusmeritvi podatkov do pridobitelja predstavi s svojim certifikatom;
4. Pridobitelj pošlje zahtevo za avtorizacijo naročila izdajatelju kartice;
5. Izdajatelj kartice preveri veljavnost kartice in razpoložljiva sredstva kupca ter pošlje odgovor pridobitelju;
6. Po opravljeni avtorizaciji pošlje pridobitelj transakcije prodajalcu informacijo o avtorizaciji;
7. Prodajalec sporoči kupcu rezultat nakupa.

Tako kot pri klasičnem SSL/TLS načinu pride tudi v SET sistemu do poravnave, kjer izdajatelj kartice zmanjša sredstva na imetnikovem računu in poravna dolg pridobitelju transakcije. Ta nato nakaže sredstva na prodajalčev račun. Slika 11 prikazuje potek nakupa v sistemu SET.

*Slika 11: Potek nakupa s plačilnem sistemu SET*




*Vir: Pipan, Elektronski plačilni sistemi na internetu,2002.*

**Prednosti sistema SET:**

- s pomočjo digitalnih certifikatov omogoča SET overjanje vseh udeležencev;
- SET za varen prenos podatkov uporablja 1024 bitni asimetrični ključ in SSL, ki omogoča vzpostavitev varnega kanala med strežniki in brskalnikom. Uporabljena kriptografija omogoča avtorizacijo, preverjanje identitete, preprečitev zanikanja transakcije in zagotovitev tajnosti;
- identiteta kupca je delno skrita, saj lahko prodajalec razbere le naročilo in način plačila, ne pa tudi identitete kupca. Pridobitelj pa dobi le informacijo o identiteti kupca, številko kartice in vrednost nakupa, ne dobi pa informacijo o vsebini naročila.

**Slabosti sistema SET:**

- implementacija SET je dražja od SSL/TLS načina za kupca in trgovca;
- bolj kompleksen način uporabe kot SSL/TLS;
- SET ne omogoča več uporabnost, saj se digitalna denarnica nahaja na enem računalniku in ni prenosljiva;
- SET uporablja kompleksne kriptografske algoritme kar lahko povzroči počasno izvedbo transakcije (Jarupunphol, Mitchell, 2003).

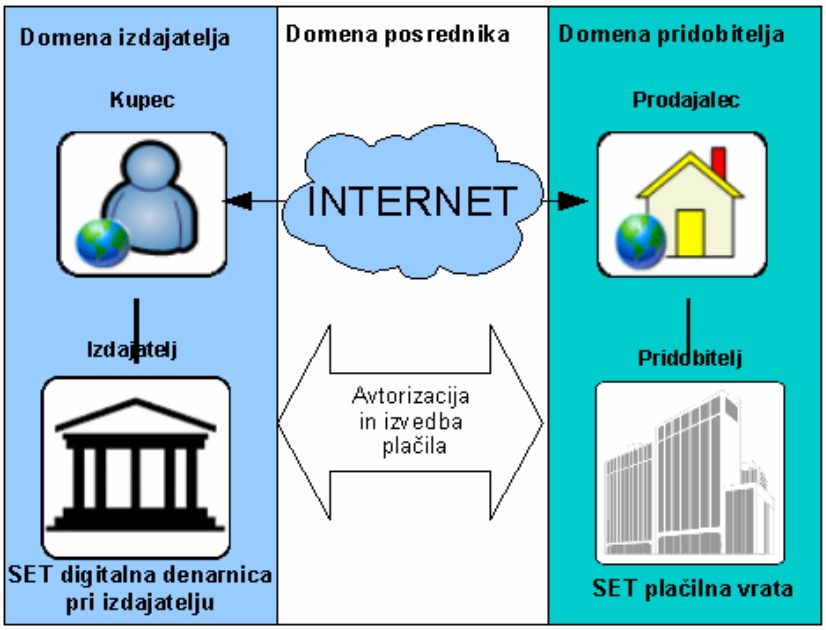
### 3D-SET

3D-SET je novejša in fleksibilnejša različica SET-a, ki ga je razvila Visa. Sistem SET temelji na infrastrukturi javnih ključev. Za delovanje uporablja ločene digitalne certifikate za vsakega udeleženca posebej (pri prenosu sporočila se uporabljajo štirje pari ključev), kar se odraža na njegovi kompleksnosti. V sistemu 3D-SET ima kupec za razliko od SET-a vse podatke o svojih karticah, digitalni certifikat in informacije o preteklih transakcijah varno shranjene v digitalni denarnici na izdajateljevem strežniku. 3D-SET temelji na treh domenah, kar je razvidno iz Slike 12:

- izdajateljeva domena – sestavljata jo imetnik in izdajatelj kartice;
- pridobiteljeva domena – sestavljata jo prodajalec in pridobitelj transakcije;
- posrednikova domena – vmesnik med kupčevo in prodajalčevo banko (Visa, MasterCard).

Transakcija se prične, ko kupec na strežniku elektronske trgovine izbere možnost 3D-SET. Prodajalčev strežnik pošlje sporočilo izdajatelju kartice, ta pa kupcu prikaže okno za overjanje, kjer se kupec identificira. V primeru uspešnega overjanja se kupčev digitalni certifikat, ki je shranjen v digitalni denarnici na strežniku, aktivira. Nadaljevanje transakcije poteka enako kot v sistemu SET. Prednost 3D-SET-a pred SET je v boljšem izpolnjevanju implementacijskih zahtev za kupca pri enako učinkovitem izpolnjevanju varnostnih zahtev. Kupec ni omejen na nakup samo iz domačega računalnika in ni omejen na določen operacijski sistem ali strojno opremo (GPayments, 2001).

***Slika 12: Prikaz domen 3D-SET plačilnega sistema***




*Vir: Pipan, Elektronski plačilni sistemi na internetu,2002.*

# 3 KARTIČNI PLAČILNI SISTEM 3-D SECURE

Premalo varni in preslabo uporabljeni EPS-ji so vzpodbudili Viso v razvoj novega EPS-ja pod imenom 3-D Secure. Namen 3-D Secura je združiti varnost sistema SET ter uporabnost SSL/TLS sistema in tako povečati zaupanje v elektronske nakupe (Visa Int., 2006a).

V 3-D Secure sistemu se pri vsakem nakupu kupca overi. Sistem omogoča različne načine overjanja. Kupec se lahko identificira na klasični način z uporabo statičnega gesla ali z uporabo pametne kartice in izdelavo enkratnih gesel. Preverjanje identitete s pametno kartico ponuja plačniku podobno izkušnjo kot pri klasičnih plačilih s pametno kartico in uporabo PIN številke. Z uporabo enkratnih gesel kupec dokazuje, da ima kartico v rokah, z uporabo PIN številke pri vsaki izdelavi enkratnega gesla pa tudi, da je pooblaščen uporabnik kartice. Kombinacija 3-D Secure z uporabo pametne kartice omogoča elektronska plačila s kartico, pri katerih ne gre za CNP transakcije, kar zmanjšuje zlorabe (Visa Int.,2001a).

Kmalu po predstavitvi plačilnega sistema 3-D Secure je prišlo do dogovora med MasterCard-om in Viso, da bosta plačilni sistem tržila vsak pod svojo blagovno znamko in sicer MasterCard pod blagovno znamko MasterCard SecureCode (v nadaljevanju MSC) ter Visa pod blagovno znamko Verified by Visa (v nadaljevanju VBV).

3-D Secure je odprt sistem in omogoča plačila iz različnih naprav, povezanih v internet, kot so osebni računalnik, mobilni telefon, dlančnik, itd.

## 3.1 Udeleženci sistema

Udeleženci 3-D Secure sistema so imetnik kartice, izdajatelj kartice, prodajalec ter pridobitelj transakcije.

**Imetnik kartice**

Imetnik kartice je pooblaščen lastnik kartice, ki je izdana s strani izdajatelja kartice. Če želi imetnik kartice sodelovati v 3-D Secure programu, se mora vanj prijaviti. V okolju elektronskega poslovanja kupec komunicira s prodajalcem prek interneta z uporabo osebnega računalnika in spletnega brskalnika. (Visa Int., 2006b).

Prednosti sodelovanja v 3-D Secure programu za imetnika kartice so:

- zaupanje pri nakupih na internetu;
- ni potrebna dodatna programska ali strojna oprema (razen čitalnika ob uporabi metode identifikacije s pametno kartico);

- enostavna uporaba kartice za opravljanje elektronskih plačil;
- kontrola nad uporabo kartice pri internetnih nakupih.

**Izdajatelj kartice**

Izdajatelj kartice (finančna inštitucija / banka) izdaja kartice, ki so lahko udeležene v 3-D Secure sistemu. Izdajatelj kartice zagotavlja pridobitelju transakcije plačilo za avtorizirano transakcijo če je ta upošteval vsa pravila uporabljene kartice (Visa Int., 2006b).

Prednosti sodelovanja v 3-D Secure programu za izdajatelje kartic so:

- dodana vrednost karticam;
- povečana prepoznavnost blagovne znamke, ker je izdajatelj kartice prisoten pri vsakem internetnem nakupu. To ojača razmerje med izdajateljem in imetnikom kartice;
- omogoča izdajateljem uporabo enake tehnologije overjanja uporabnika kot pri elektronskem bančništvu;
- ni potrebna nabava dodatne programske ali strojne opreme za imetnika kartice (razen ob uporabi pametne kartice).

**Prodajalec**

Prodajalec je fizična ali pravna oseba, ki pogodbeno sprejema plačilne kartice kot plačilno sredstvo za nakup. Z vključitvijo v 3-D Secure sistem prodajalec ponuja kupcu možnost varnega plačila preko interneta. Prodajalec, ki sprejema plačilne kartice, mora imeti sklenjeno pogodbeno razmerje s pridobiteljem transakcije (Visa Int., 2006b).

Prednosti sodelovanja v 3-D Secure programu za prodajalca so:

- enostavna vključitev v sistem, saj mora prodajalec na spletnem prodajnem mestu nastaviti le aplikacijo v obliki vtičnika (angl. *plug-in*);
- minimalno dopolnjen proces nakupa;
- povečana prodaja, saj kupec zaupa vpisati svoje podatke pri nakupu;
- zmanjšana možnost zlorab;
- zagotovljeno plačilo izvedene prodaje;
- sprejemanje Maestro debetne kartice.

**Pridobitelj transakcije**

Pridobitelj transakcije je v razmerju s prodajalcem in pridobiva podatke o izvedenih transakcijah ter sproža avtorizacijo in poravnavo transakcije (Visa Int., 2006b).

Prednosti sodelovanja v 3-D Secure programu za prodajalca so:

- zmanjšano število zavrnjenih transakcij;
- povečano število transakcij;
- dodana vrednost za prodajalca.

**Splošne prednosti za udeležence**

Bistvena prednost udeležencev v 3-D Secure programu je zmanjšanje zlorab in dvomljivih transakcij. Študije so pokazale, da tretjina imetnikov kartice ne zaupa internetnim nakupom zaradi dvomljive varnosti transakcij. MasterCard-ove raziskave pravijo, da lahko dosežemo 80% manj zavračanj z overjanjem imetnika kartice (MasterCard Int., 2004). 3-D Secure program lahko prepriča kupce v varno nakupovanje na internetu.

Kombinacija enostavnosti, fleksibilnosti implementacije in varnosti nudi naslednje koristi vsem udeležencem:

- povečanje zaupanja kupcev, kar povečuje prodajo;
- povečano zaupanje prodajalcev pri sprejemanju različnih mednarodnih kartic;
- zmanjšano število pritožb, zavračanj in stroškov povezanih z njimi;
- globalno podprt servis;
- uporaba SSL/TLS varne komunikacije;
- možnost uporabe pametne kartice;
- uporaba debetnih Maestro kartic.

## 3.2 Pravila zavračanja transakcij

MasterCard in Visa določata pogoje, pod katerimi je mogoče zavračati transakcije. Zaradi novega 3-D Secure sistema so se pravila zavračanja dopolnila. Z novimi pravili je 3-D Secure sistem postal bolj zanimiv za izdajatelje kartic in pridobitelje transakcij. Izdajatelji kartic imajo večjo moč zavračanja transakcij, v kolikor je imetnik kartice prijavljen v 3-D Secure program, medtem ko imajo pridobitelji transakcij večjo možnost zavračanja, če je prodajalec udeležen v 3-D Secure programu.

Nova pravila uvajajo nove šifre razlogov za zavrnitev transakcij. V primeru, da je prodajalec udeležen v 3-D Secure sistem ne more izdajatelj kartice zavračati transakcijo s šifro razloga 4837 (ni odobritve imetnika kartice), 4863 (neznan imetnik kartice) ali 4849 (vprašljiva vloga prodajalca[10]). Odgovornost za transakcijo v 3-D Secure sistemu prevzema izdajatelj kartice, ko:

[10] Izdajatelj je upravičen uporabiti šifro 4849 če sumi, da je bil prodajalec namenoma vključen v zlorabo kartice

- je prodajalec udeležen v 3-D Secure;
- pri overjanju imetnika kartice izdajatelj kartice pripravi 3-D Secure podatke za prodajalca;
- pridobitelj transakcije upošteva vse zahteve, ki veljajo za prometne podatke;
- odgovor na avtorizacijo transakcije označuje, da je izdajatelj kartice odobril transakcijo in preveril 3-D Secure podatke avtorizacije.

Če izdajatelj kartice ugotovi, da 3-D Secure prometni podatki niso enaki podatkom overjanja, ima ta še vedno možnost zavrniti transakcijo pod zgoraj navedenimi šiframi (MasterCard Int., 2004).

## 3.3 Tri-domenski model

Sistem 3-D Secure delimo na tri domene:

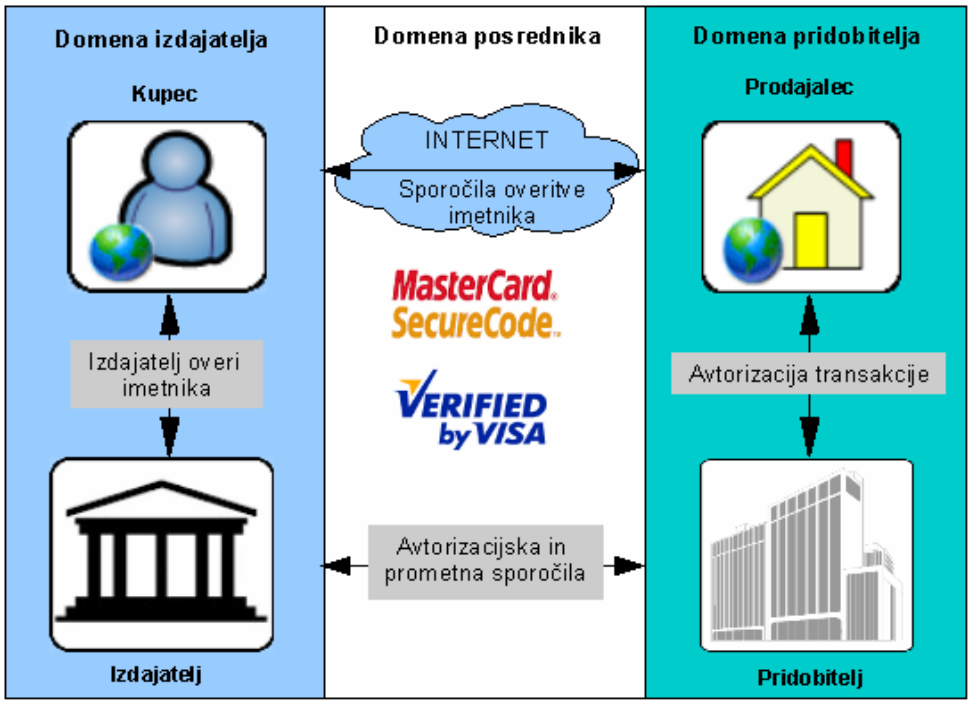
- domena izdajatelja (v domeni sta izdajatelj in imetnik kartice);
- domena pridobitelja (v domeni sta pridobitelj transakcije in prodajalec);
- domena posrednika (v domeni sta MasterCard ali Visa).

**Komunikacija domen**

Domene medseboj komunicirajo s 3-D Secure sporočili. Domena posrednika opravlja storitev posredovanja sporočil med pridobiteljevo in izdajateljevo domeno. Najpogosteje se v sistemu 3-D Secure uporabljajo naslednja sporočila. Potek komunikacije je razviden iz Slike 13:

- sporočila overjanja imetnika kartice med izdajateljevo in pridobiteljevo domeno;
- sporočila overjanja imetnika kartice med izdajateljem in imetnikom kartice v izdajateljevi domeni;
- avtorizacijska sporočila v pridobiteljevi domeni (prodajalec zahteva avtorizacijo transakcije od pridobitelja);
- avtorizacijska sporočila in sporočila poravnave prometa med pridobiteljevo in izdajateljevo domeno.

*Slika 13: Prikaz 3-D Secure domen in komunikacije domen*




*Vir: Visa Int., 3-D Secure Implementation Guide, 2001c.*

### Komponente sistema

Storitev komunikacije domen opravljajo komponente 3-D Secure sistema. Tabela 6 razvršča komponente 3-D Secure sistema znotraj domen.

***Tabela 6: Komponente 3-D Secure sistema***

| Izdajateljeva domena | Posrednikova domena | Pridobiteljeva domena |
|---|---|---|
| Imetnikov spletni **brskalnik**;<br><br>Strežnik vključitev (Enrollment Server – **ES**);<br><br>Strežnik upravljanja z dostopi (Access Control Server – **ACS**);<br><br>Strežnik overjanja podatkov 3-D Secure (Authentication Data Validation Server - **ADVS**); | Strežnik preusmerjanja (Directory Server – **DS**);<br><br>Agencija za overjanje (Certificate Authority - **CA**);<br><br>Strežnik zgodovinskih podatkov (History Server – **HS**); | Prodajalčev vtičnik (Merchant Plug-In – **MPI**);<br><br>Plačilna vrata (Payment Gateway – **PG**);<br><br>Strežnik preverjanja digitalnega podpisa (Digital Signature Validation Server – **DSVS**); |

*Vir: MasterCard Int., 3-D Secure Member Enrollment and Implementation guide, 2004.*

### 3.3.1 Domena izdajatelja

V izdajateljevi domeni so naslednje komponente 3-D Secure sistema:

**Imetnikov spletni brskalnik**

Spletni brskalnik je računalniški program - aplikacija, ki omogoča brskanje po spletu ter zna prikazovati HTML dokumente in razne večpredstavne vsebine (Wikipedia, 2008c). Aplikacija omogoča varno komunikacijo preko SSL/TLS protokola. Imetnik kartice uporablja spletni brskalnik za opravljanje elektronskega nakupa ter prijavo v 3-D Secure program preko strežnika za vključitev. Imetnikov spletni brskalnik preusmerja nekatera sporočila overjanja (PaReq, PaRes) med prodajalčevo in izdajateljevo domeno.

**Strežnik vključitve**

Strežnik za vključitev nudi spletno stran za vključitev kartice v 3-D Secure program. Spletna stran omogoča imetniku kartice začetno prijavo, administracijo in pregled 3-D Secure transakcij. Strežnik za vključitev in strežnik upravljanj z dostopi sta ponavadi ena (skupna) komponenta izdajatelja kartice.

**Strežnik upravljanja z dostopi**

Strežnik upravljanja z dostopi služi za izvajanje dveh ključnih procesov 3-D Secure sistema. Preveri, ali je številka kartice vključena v program. V primeru, da je kartica vključena opravi overjanje imetnika kartice. Strežnik pripravi podatke overjanja za pridobitelja transakcije.

**Strežnik overjanja podatkov 3-D Secure**

Strežnik upravljanja z dostopi pripravi podatke overjanja za pridobitelja transakcije. Pridobitelj uporabi podatke overjanja za pravilno izvedbo avtorizacije transakcije. Izdajatelj kartice preveri prejete 3-D Secure podatke iz avtorizacijskega sporočila s pomočjo strežnika overjanja 3-D Secure podatkov.

### 3.3.2 Domena pridobitelja

V domeni pridobitelja so naslednje komponente 3-D Secure sistema.

**Prodajalčev vtičnik**

Prodajalčev vtičnik (razširitvena aplikacija) skrbi za izvedbo elektronskega plačila. Aplikacija prikazuje spletno okno za vpis podatkov kartice, izdeluje in obdeluje sporočila overjanja imetnika kartice ter prikazuje izdajateljevo okno za overjanje. Aplikacija izvede avtorizacijo transakcije preko plačilnih vrat pridobitelja transakcije.

**Plačilna vrata**

Plačilna vrata omogočajo prodajalčevi razširitveni aplikaciji izvedbo avtorizacije transakcije. Preko plačilnih vrat lahko prodajalec pregleduje in potrjuje avtorizacije transakcij. V nekaterih primerih plačilna vrata izdelujejo in obdelujejo overitvena sporočila ter tako prevzamejo vlogo prodajalčeve razširitvene aplikacije.

**Strežnik overjanja digitalnega podpisa**

Kot že samo ime pove strežnik za overjanje digitalnega podpisa overja izdajateljev digitalni podpis sporočila PARes (glej poglavje 3.7.6). Preverjanje digitalnega podpisa se lahko opravi tudi v prodajalčevem vtičniku.

### 3.3.3 Domena posrednika

Posrednikova domena je jedro 3-D Secure sistema. Posrednikova naloga je posredovanje overitvenih, avtorizacijskih in prometnih sporočil med pridobiteljevo in izdajateljevo domeno. V domeni posrednika so naslednje komponente 3-D Secure sistema:

**Strežnik preusmerjanja**

Strežnik preusmerja overitvena (VEReq, VERes) sporočila med pridobiteljevo in izdajateljevo domeno. Strežnik se odloča ali bin kartice[11] sodeluje v 3-D Secure programu.

**Agencija za overjanje**

Agencija za overjanje upravlja, izdeluje in razpečuje certifikate za 3-D Secure komponente. Ti certifikati so:

- korenski certifikati (MasterCard-a ali Vise);
- strežniški in odjemalčevi SSL certifikati;

[11] Bin je prvih 6 številk kartice. Izdajatelj pridobi pravico za izdelavo kartice z določenim binom od kartičnih inštitucij.

- certifikati za digitalno podpisovanje.

Komponente sistema uporabljajo tudi SSL certifikate, ki so javne narave in jih izdajajo komercialne agencije za overjanje, kot je VeriSign.

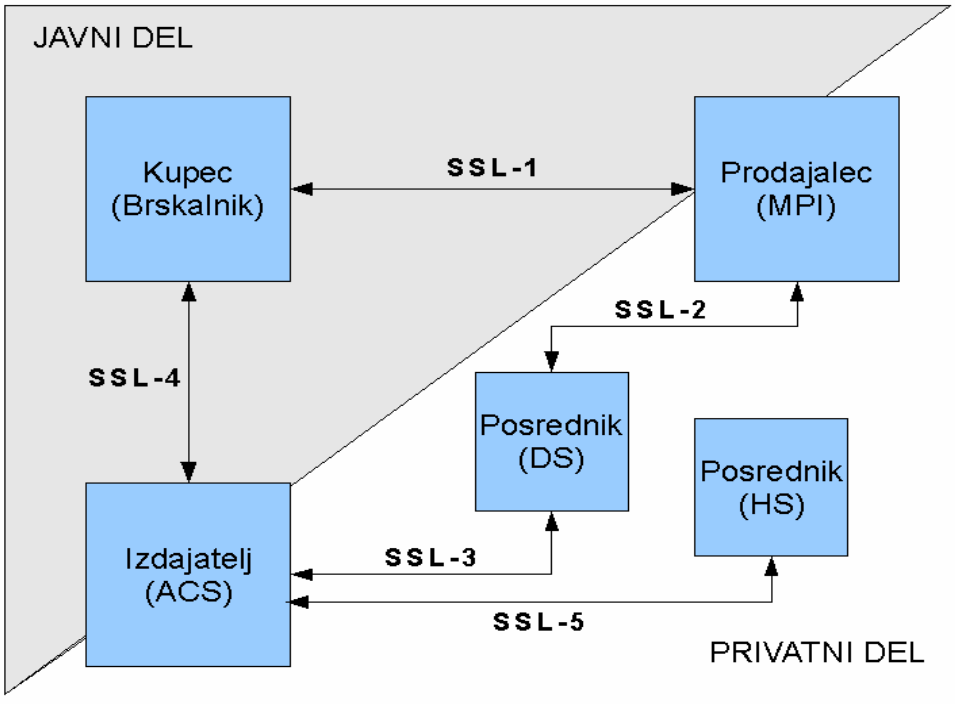
**Strežnik zgodovinskih podatkov**

Strežnik zgodovinskih podatkov je prisoten le v VBV programu. Strežnik shranjuje podatke 3-D Secure transakcij, ki mu jih pošlje izdajateljev strežnik za upravljanje z dostopi preko sporočila PATransReq (glej poglavje 3.7.7). Zgodovinski podatki se uporabljajo za izvajanje statistike in so na voljo tudi izdajatelju in pridobitelju transakcije (Visa Int., 2001b).

## 3.4 Povezave

Komponente v 3-D Secure sistemu varno komunicirajo preko SSL protokola. Kot je razvidno iz Slike 14 razdelimo povezave na dva dela. Na javni del povezav, za katere se uporabljajo certifikati komercialnih ponudnikov, ter privatni del, za katere izdajata certifikate MasterCard-ov ali Visin CA.

***Slika 14: Prikaz povezav 3-D Secure***




*Vir: Visa Int., 3-D Secure Implementation Guide, 2001c.*

**Javni del**

V javnem delu so povezave, kjer gre za komunikacije izključno s kupčevim brskalnikom (SSL-1 in SSL-4, Slika 14):

- SSL-1 povezavo vzpostavi brskalnik z MPI. MPI se predstavi s strežniškim certifikatom komercialne CA;
- SSL-4 povezavo vzpostavi brskalnik z ACS. ACS se predstavi s strežniškim certifikatom.

Kupcu ni potrebno predložiti certifikata za vzpostavitev povezav SSL-1 in SSL-4.

**Privatni del**

V privatnem delu so povezave ko gre za komunikacijo med zaključeno množico uporabnikov (povezave SSL-2, SSL-3 in SSL-5, Slika 14):

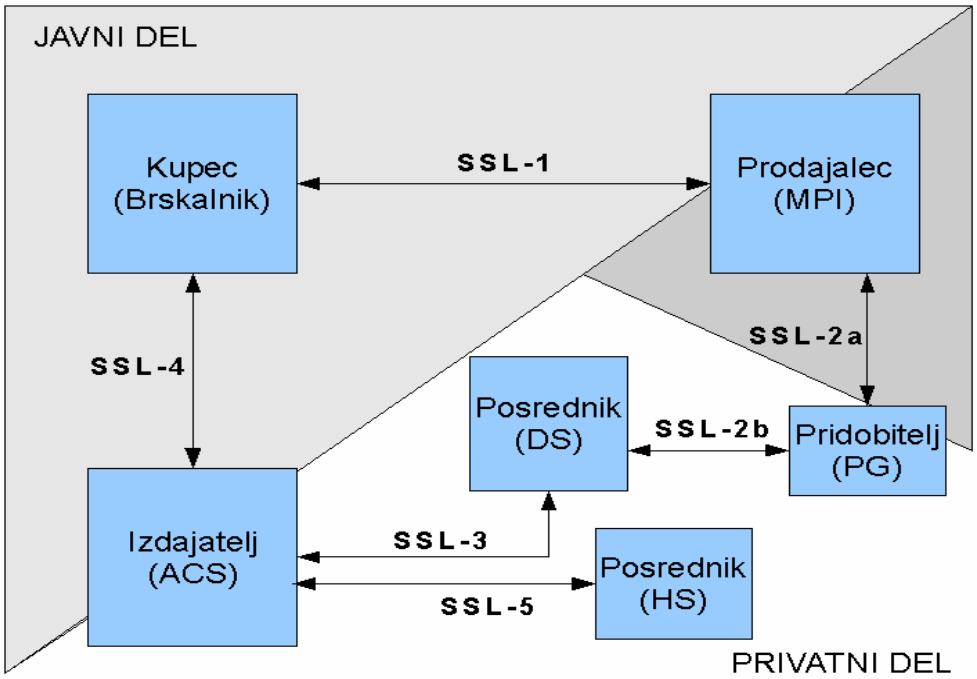
- SSL-2 povezavo vzpostavi MPI do DS. DS se predstavi s svojim strežniškim, MPI pa s svojim odjemalčevim certifikatom;
- SSL-3 povezavo vzpostavi DS do ACS. ACS se predstavi s svojim strežniškim, DS pa s svojim odjemalčevim certifikatom;
- SSL-5 povezavo vzpostavi ACS do HS. HS se predstavi s svojim strežniškim, ACS pa s svojim odjemalčevim certifikatom.

**Izboljšane povezave**

Vzpostavitev povezave SSL-2 je lahko problematična, saj bi morala MasterCard ali Visa za vsakega prodajalca izdelati odjemalčev certifikat. SSL-2 povezavi se lahko izognemo tako, da ima pridobiteljev PG odjemalčev certifikat za povezavo na DS, MPI pa odjemalčev certifikat izdan iz pridobiteljevega CA-ja. Sprememba povezav je razvidna iz Slike 15. Povezavo SSL-2 zamenjata povezavi SSL-2a in SSL-2b:

- SSL-2a povezavo vzpostavi MPI do PG. PG se predstavi s svojim strežniškimi, MPI pa s svojim odjemalčevim certifikatom;
- SSL-2b povezavo vzpostavi PG do DS. DS se predstavi s svojim strežniškim, PG pa s svojim odjemalčevim certifikatom.

*Slika 15: Prikaz izboljšanih povezav 3-D Secure*




*Vir: lasten.*

## 3.5 Vključitev imetnika kartice

Imetnik kartice se po svoji volji odloči ali se bo prijavil v 3-D Secure program. Če imetnik kartice prijavi svojo kartico v program, pravimo, da je kartica 3-D Secure varna. Kartica je varna zato, ker se bo za vsako njeno uporabo na internetu overilo imetnika kartice. Overitev imetnika se izvrši le, če sta prodajalec in imetnik kartice vključena v 3-D Secure program. Prav ta (za mnoge) pomanjkljivost ne prepriča ene ali druge strani v vključitev. Prodajalec naj ne bi imel interesa, ker je malo kartic 3-D Secure varnih, imetnik kartice pa zato, ker malo prodajalcev omogoča 3-D Secure. Obe strani bi moralo v vključitev prepričati dejstvo, da stroške zlorabe kartice nosi prodajalec ali imetnik kartice, ki ni prijavljen v 3-D Secure.

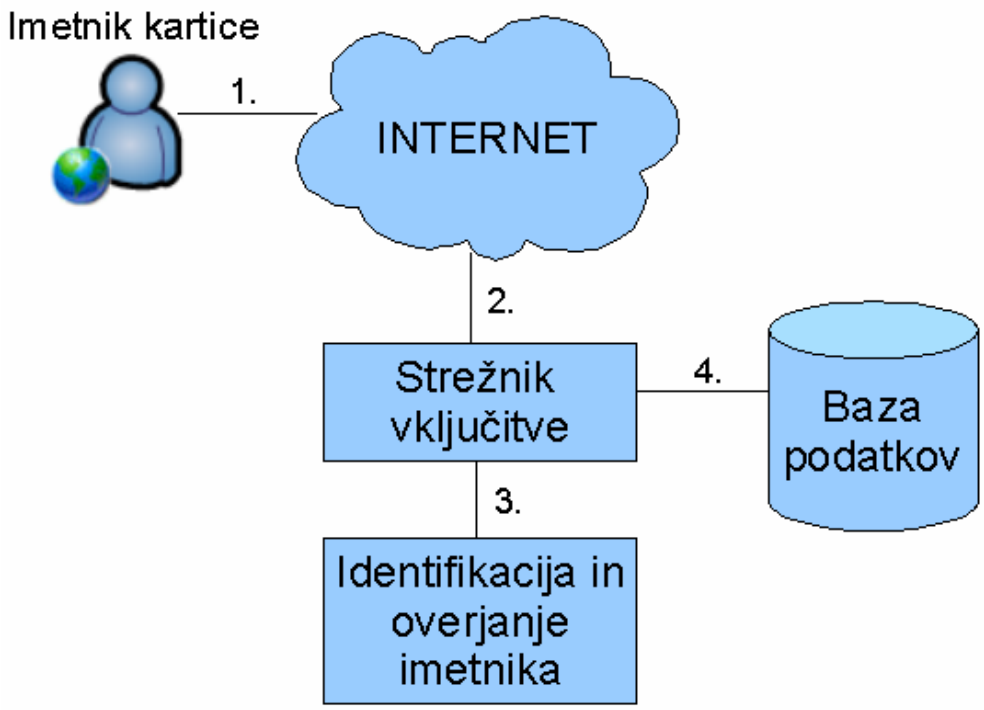
Osrednja komponenta za vključitev imetnika kartice v 3-D Secure program je izdajateljev strežnik vključitve. Strežnik je tesno povezan z izdajateljevim strežnikom za upravljanje s prijavami. Strežnikove naloge so:

- preverjanje ali je za številko kartice možna vključitev v program;
- overjanje imetnika kartice;
- upravljanje kartice;
- shranjevanje podatkov vključitve.

**Postopek vključitve (potek je prikazan na Sliki 16):**

1. Imetnik kartice obišče izdajateljevo spletno stran za vključitev v program. Spletna stran je lahko odprta ali zaprta. Odprto spletno stran lahko obišče vsakdo, zaprto pa lahko obiščejo samo nekateri uporabniki (recimo uporabniki spletne banke);
2. Imetnik kartice se strežniku identificira tako, da vnese svoje podatke. Med vnosom si izbere svoje pozdravno sporočilo, ki ga pozdravi ob vsaki 3-D Secure overitvi;
3. Izdajatelj kartice preveri podatke, ki jih je imetnik vnesel. To se lahko opravi s kasnejšo obdelavo podatkov ali s takojšnim preverjanem (avtomatični način);
4. Izdajatelj kartice obvesti imetnika o rezultatu vključitve. Podatke vključitve si izdajatelj shrani v bazo podatkov.

***Slika 16: Postopek vključitve imetnika kartice v 3-D Secure program***



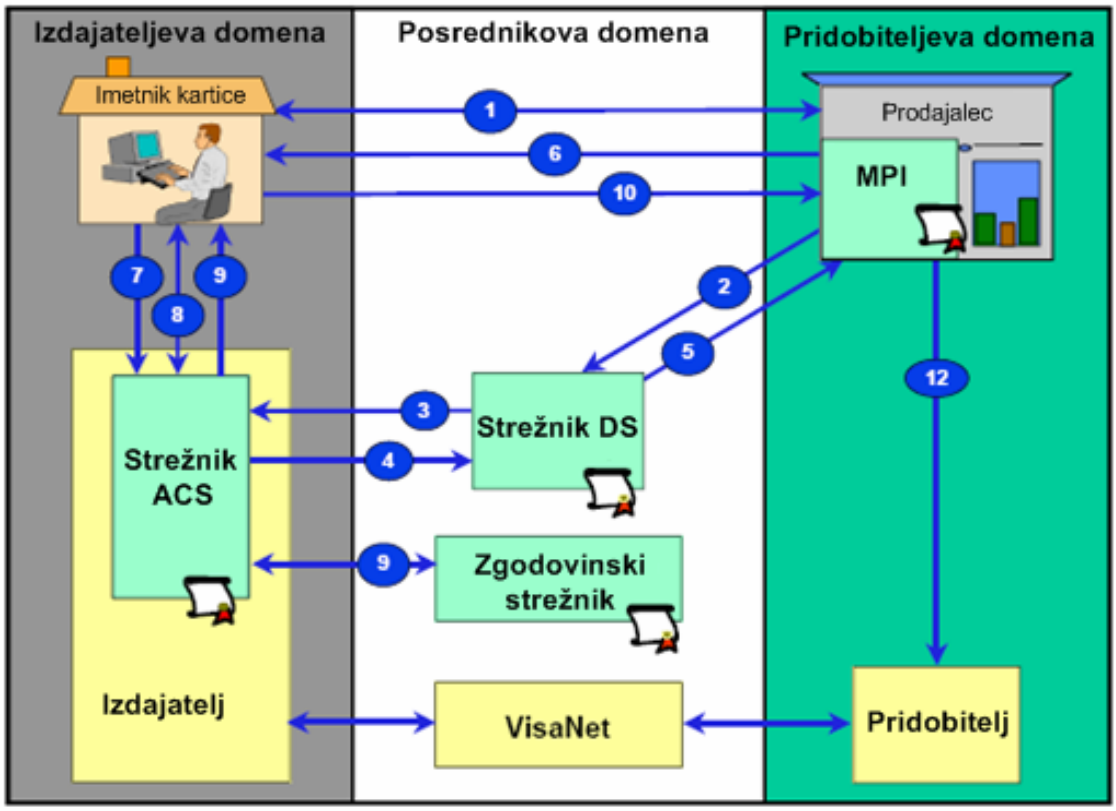

*Vir: MasterCard Int., 3-D Secure Member Enrollment and Implementation guide, 2004.*

Kartica je lahko avtomatično vključena v 3-D Secure program, če izdajatelj kartice zagotovi vsem imetnikom poznavanje svojega gesla. Uporaba pametne kartice in enkratnih gesel je ena od možnosti za avtomatično vključitev, vendar mora izdajatelj kartice zagotoviti vsem imetnikom kartic čitalnik za pametne kartice. Ena od možnosti bi lahko bila tudi izdelava gesel in pošiljanja obvestil vsem imetnikom kartic o 3-D Secure vključitvi. 3-D Secure protokol omogoča tudi vključitev med nakupom. Na ta način se imetnik kartice prijavi v sistem kar med nakupom.

## 3.6 Potek nakupa

Potek nakupa v 3-D Secure sistemu je postopek, pri katerem so udeleženi vsi uporabniki sistema ter njihove komponente. Slika 17 prikazuje potek nakupa v sistemu 3-D Secure (Visa Int., 2004b).

***Slika 17: Potek nakupa v sistemu 3-D Secure***




*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

1. Komunikacija: Imetnik kartice - Prodajalec (HTTP POST ukaz na povezavi SSL-1):

   a) Imetnik kartice obišče spletno stran preko brskalnika in izbere izdelke za nakup;
   b) Imetnik kartice potrdi nakup in vpiše podatke za izvedbo plačila. V tem trenutku ima MPI vse informacije vključno s številko kartice - PAN, veljavnost kartice, CVC kartice in podatke o kupcu.

2. Komunikacija: MPI – DS (HTTP POST ukaz na povezavi SSL-2)

   a) MPI izdela sporočilo VEReq;
   b) MPI preveri če ima že vzpostavljeno SSL-2 povezavo z DS. V kolikor je nima, jo poizkuša vzpostaviti. Če povezava ne uspe, se nakup nadaljuje s korakom 12;
   c) MPI naredi HTTP POST ukaz in pošlje VEReq sporočila na DS.

3. Komunikacija: DS – ACS (HTTP POST ukaz na povezavi SSL-3):

a) DS preveri sintakso VEReq sporočil. Če sintaksa VEReq ne ustreza pogojem, pošlje DS Error sporočilo nazaj do MPI. DS preveri vsebino VEReq sporočila. Če vsebina ne ustreza pogojem, pošlje VERes sporočilo do DS. VERes sporočilo označuje, da overitev imetnika kartice ni možna zaradi napake v vsebini sporočila VEReq;
b) DS v svoji bin tabeli preveri ali je bin kartice vključen v program. Če bin ni vključen v program, pošlje VERes sporočilo do MPI. Sporočilo označuje, da overitev imetnika kartice ni možna, ker imetnik ni prijavljen v program;
c) DS preveri če ima že vzpostavljeno SSL-3 povezavo z ACS. V kolikor je nima, jo poizkuša vzpostaviti. Če povezava na primarni naslov ACS ne uspe, poizkuša DS vzpostaviti povezavo s sekundarnim naslovom ACS. Če povezava ne uspe, pošlje VERes sporočilo do MPI. Sporočilo označuje, da overitev imetnika kartice ni možna, ker imetnik ni prijavljen v program;
d) DS preusmeri s HTTP POST ukazom VEReq sporočilo do ACS.

4. Komunikacija: ACS – DS (Odgovor na HTTP POST na povezavi SSL-3):

a) ACS preveri sintakso VEReq sporočil. Če sintaksa VEReq ne ustreza pogojem, pošlje nazaj Error sporočilo. ACS preveri vsebino VEReq sporočila. Če vsebina ne ustreza pogojem, pošlje nazaj VERes sporočilo, ki označuje, da overitev imetnika kartice ni možna zaradi napake v vsebini sporočila VEReq;
b) ACS pregleda svojo bazo podatkov ali je kartica iz VEReq sporočila prijavljena v program;
c) Če kartica ni prijavljena v program, odgovori z VERes sporočilom, ki označuje, da overitev imetnika kartice ni možna, ker imetnik ni prijavljen v program;
d) Če je kartica prijavljena v program, odgovori z VERes sporočilom, ki označuje, da je overitev imetnika kartice možna. ACS izračuna številko računa VEReq sporočila in jo vpiše v VERes sporočilo.

5. Komunikacija: DS – MPI (Odgovor na HTTP POST na povezavi SSL-2):

a) DS preveri sintakso VERes sporočil. Če sintaksa VERes ne ustreza pogojem, pošlje Error sporočilo nazaj do ACS;
b) Če je VERes sporočilo sintaktično pravilno, se sporočilo preusmeri do MPI (MPI-ju se lahko odgovori s sporočilom Error – točka 3a);
c) Če VERes sporočilo ni sintaktično pravilno, pošlje VERes sporočilo, ki označuje da overitev imetnika kartice ni možna do MPI;
d) Če MPI dobi sporočilo Error, se potek nakupa nadaljuje s korakom 12.

6. Komunikacija: MPI – Imetnik kartice (Odgovor na HTTP POST na povezavi SSL-1):

a) Če prejeto VERes sporočilo označuje, da PAN ne omogoča overjanja, se potek nakupa nadaljuje s korakom 12;
b) MPI zgradi PAReq sporočilo, v katerega vključi številko računa iz VERes sporočila (korak 4d);
c) MPI PAReq sporočilo stisne in predela v Base64 obliko. Rezultat je PaReq (mala črka a označuje razliko) sporočilo;
d) MPI izdela spletno okno, ki vsebuje PaReq, TermURL (naslov MPI, na katerega mora biti poslano PaRes sporočilo) in MD (prodajalčevi dodatni podatki) polja;
e) Izdelano spletno okno preko imetnikovega brskalnika izvrši preusmeritev (HTTP POST zahteva) polj PaReq, TermURL in MD na ACS URL podan v sporočilu VERes. Izvršitev se tipično izvede preko uporabe JavaScript[12] ukaza ob odpiranju spletnega okna.

7. Komunikacija: Imetnik kartice – ACS (HTTP POST ukaz na povezavi SSL-4):

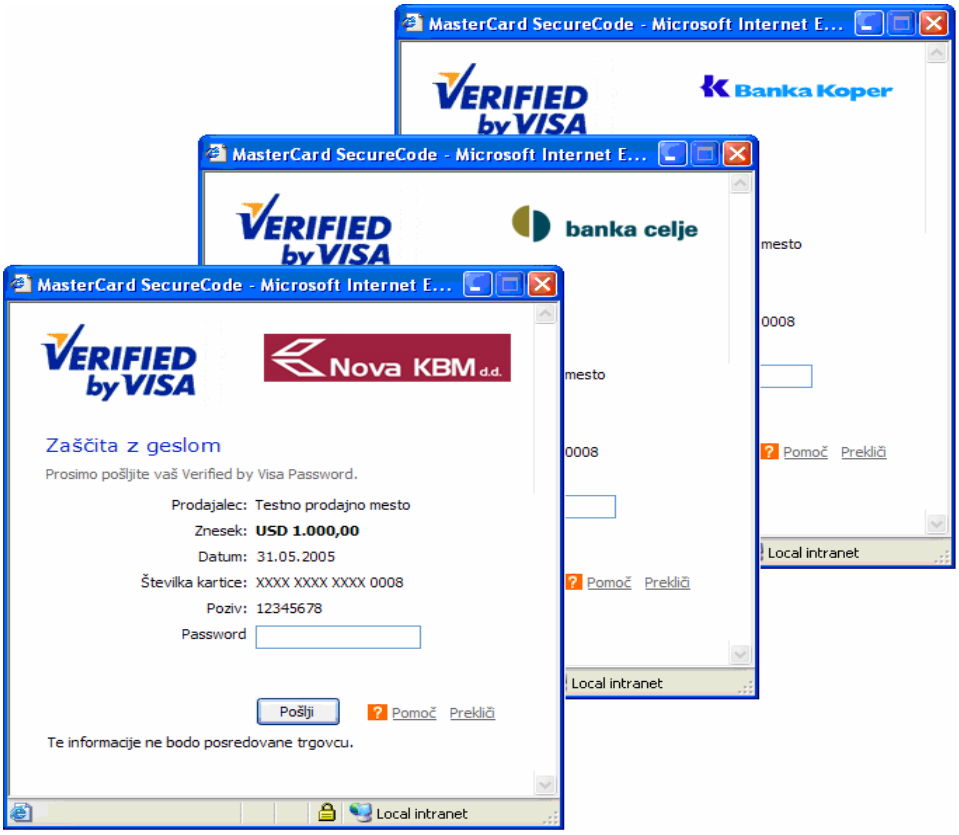
a) ACS naredi obratni proces točke 6c, tako da dobi iz PaReq polja nazaj PAReq sporočilo;
b) ACS preveri sintakso PAReq sporočila. Če sporočilo ne ustreza sintaksi, pošlje Error sporočilo na TermURL naslov. ACS preveri vsebino PAReq sporočila, tako da ga poveže z VERes sporočilom. Če preverjanje ne uspe, izdela in pošlje PARes sporočilo na TermURL naslov (korak 10);
c) ACS odgovori na ukaz HTTP POST s HTML spletno stranjo (okno za overjanje). Primeri oken za overjanje so prikazani na Sliki 18.

8. Komunikacija: Imetnik kartice – ACS – Imetnik kartice (več HTTP POST zahtev in odgovorov na povezavi SSL-4):

a) Imetnik kartice na oknu za overjanje vpiše svoje geslo;
b) ACS preveri geslo (v kolikor geslo ni pravilno, se lahko proces vnosa in preverjanja ponovi);
c) ACS izdela PARes sporočilo, ki označuje rezultat overjanja imetnika kartice;
d) ACS digitalno podpiše PARes sporočilo.

**12** JavaScript je objektni skriptni programski jezik, ki ga je razvil Netscape z namenom, da omogoči spletnim programerjem ustvarjanje interaktivnih spletnih strani (Wikipedia, 2008g).

*Slika 18: Primeri overitvenih oken 3-D Secure*




*Vir: Interna gradiva podjetja, 2007.*

9. Komunikacija: ACS – Imetnik kartice (HTTP POST zahteva na povezavi SSL-4 in SSL-5)

   a) ACS PARes sporočilo stisne in pretvori v Base64 format ter tako dobi PaRes sporočilo;
   b) ACS v spletno okno vključi polja PaRes in MD (enaka vsebina kot jo je MPI poslal);
   c) Spletno okno preko imetnikovega brskalnika izvrši preusmeritev (HTTP POST zahteva) polj PaRes in MD na TermURL. Preusmeritev se tipično izvrši z JavaScript ukazom. ACS izdela PATransReq sporočilo in ga preko HTTP POST zahteve pošlje na strežnik HS. Strežnik HS mu odgovori s sporočilom PATransRes, ki označuje ali je zahtevek uspešno obdelal.

10. Komunikacija: Imetnik kartice – MPI (HTTP POST zahteva na povezavi SSL-1)

   a) MPI prebere PaRes sporočilo in izvrši obratni postopek točke 9a, tako da iz PaRes sporočila dobi PARes sporočilo;
   b) Če je MPI prejel Error sporočilo, se potek nakupa nadaljuje s korakom 12;
   c) MPI preveri sintakso PARes sporočila. V primeru napake, se nakup nadaljuje s korakom 12.

11. MPI preveri digitalni podpis PARes sporočila. Preverjanje se izvrši v DSVS komponenti (glej poglavje 3.2).

12. Komunikacija: MPI – pridobitelj transakcije

V zadnjem koraku poteka nakupa se opravi avtorizacija transakcije. Avtorizacija transakcije poteka na poti pridobitelj – posrednik – izdajatelj. Pridobitelj transakcije v avtorizacijo vključi tudi rezultat overitve imetnika kartice - CAVV podatek iz PARes sporočila. Poleg klasičnih preverjanj avtorizacije transakcije izdajatelj kartice preveri tudi CAVV podatek. Avtorizacijo izdajatelj kartice odobri ali zavrne.

**Proces prednaložitve bin tabele**

Pred samim nakupom se lahko na prodajalčevi strani neprestano izvaja proces prednaložitve bin tabele kartic vključenih v 3-D Secure program. Prednaložitev bin tabele odstranjuje potrebo po koraku 2 iz poteka nakupa, ko MPI pošlje VEReq sporočilo do DS v primeru, da celoten rang kartic ni vključen v program. Odstranitev koraka 2 pri rangih kartic, ki niso vključeni, zmanjšuje obremenitev strežnikov. V procesu prednaložitve prodajalčev MPI neprestano pošilja (na nastavljen interval, ki je največ 24 ur) sporočilo CEReq do DS. Ta mu odgovori s sporočilom CERes, ki vsebuje vse bine kartic vključenih v 3-D Secure program. Bine si MPI shrani za uporabo pri izvedbi vsake transakcije.

## 3.7 Sporočila

Sporočila sistema 3-D Secure so se od začetka že spremenila in so v času pisanja dela bila v različici 1.0.2 Sistem s podporo sporočil 1.0.2 mora biti nazaj združljiv, kar pomeni, da zna delovati tudi s sporočili predhodnih različic (na primer različica 1.0.1). Sporočila 3-D Secure so v XML[13] obliki. Sistem pozna naslednja sporočila:

- **CRReq** (Card Range Request) sporočilo za pridobitev bin tabele vključenih kartic;
- **CRRes** (Card Range Response) odgovor na CRReq sporočilo;
- **VEReq** (Verify Enrollment Request) sporočilo preverjanja vključenosti v program;
- **VERes** (Verify Enrollment Response) odgovor na VEReq sporočilo;
- **PAReq** (Payer Authentication Request) sporočilo overitve imetnika kartice;
- **PARes** (Payer Authentication Response) odgovor na PAReq sporočilo;
- **PATransReq** (Payer Authentication Transaction Request) sporočilo obveščanja zgodovinskega strežnika o transakciji;

[13] XML je preprost računalniški jezik podoben HTML-ju, ki omogoča opisovanje strukturiranih podatkov (Wikipedia, 2008h).

- **PATransRes** (Payer Authentication Transaction Response) odgovor na PATransReq sporočilo.

3-D Secure sporočilo se vedno začne s korenskim elementom ThreeDSecure. Pod korenskim elementom se nahaja Message element z atributom Id. Pod elementom Message se nahaja vsebina sporočila. Primer 3-D Secure sporočila VEReq v XML obliki:

```
<ThreeDSecure>
  <Message id="ZSiwxoq58wi6G1fJN2OAGaULV6M=">
    <VEReq>
      <version>1.0.2</version>
      <pan>6762140000123456789</pan>
      <Merchant>
        <acqBIN>545042</acqBIN>
        <merID>02855879163-TINT0001</merID>
      </Merchant>
    </VEReq>
  </Message>
</ThreeDSecure>
```

### Id atribut sporočila

Vsako 3-D Secure sporočilo ima svojo identifikacijsko številko id. XML atribut Id se nahaja v XML elementu Message. Sporočili zahteve in odgovora imata enako identifikacijsko številko. Pošiljatelj sporočila izdela id atribut na podlagi algoritma, ki izdela unikatne vrednosti. Vsaka id vrednost mora izpolnjevati zahteve, ki so definirane v dokumentu Extensible Markup Language (XML) W3C Recommendation (Visa Int., 2004b).

### Digitalni podpis

PARes sporočilo je edino sporočilo v 3-D Secure sistemu, ki je digitalno podpisano. Digitalni podpis se nahaja zunaj sporočila PARes neposredno pod elementom Message (angl. *detached xml signature*). Tabela 7 in Tabela 8 prikazujeta zahteve za digitalni podpis PARes sporočila (Visa Int., 2004b).

***Tabela 7: XML elementi digitalnega podpisa 3-D Secure sporočila***

| Ime XML elementa | Zahteva za element |
|---|---|
| **Signature** | Element vsebuje enega otroka KeyInfo |
| **CanonicalizationMethod** | Element ima atribut Algorithm in nima otrok |
| **SignatureMethod** | Element ima atribut Algorithm in nima otrok |
| **Transforms** | Element ni prisoten |
| **DigestMethod** | Element ima atribut Algorithm in nima otrok |
| **KeyInfo** | Element ima enega otroka X509Data |
| **X509Data** | Element ima X509Certificate otroka za vsak certifikat v verigi |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

*Tabela 8: Algoritmi digitalnega podpisa PARes sporočila*

| Tip algoritma | Identifikacija |
|---|---|
| **Canonicalization** | http://www.w3.org/TR/2001/REC-xml-c14n-20010315 |
| **Digest** | http://www.w3.org/2000/09/xmldsig#sha1 |
| **Encoding** | http://www.w3.org/2000/09/xmldsig#base64 |
| **MAC** | http://www.w3.org/2000/09/xmldsig#hmac-sha1 |
| **Signature** | http://www.w3.org/2000/09/xmldsig#rsa-sha1 |
| **Transform** | Brez |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### Primer digitalnega podpisa PARes sporočila

```
<ThreeDSecure>
  <Message id="ZSiwxoq58wi6G1fJN2OAGaULV6M=">
    <PARes id="PaResM000149">
      ...
    </PARes>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
c14n-20010315" />
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
sha1" />
        <Reference URI="#PaResM000149">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
          <DigestValue>p1MIn/G/BeyA1Jjv+HaLM+G1Dz0=</DigestValue>
        </Reference>
      </SignedInfo>
      <SignatureValue>gxI2aJmaCAcq+.....</SignatureValue>
      <KeyInfo>
        <X509Data>
          <X509Certificate>....</X509Certificate>
          <X509Certificate>....</X509Certificate>
          <X509Certificate>....</X509Certificate>
        </X509Data>
      </KeyInfo>
    </Signature>
  </Message>
</ThreeDSecure>
```

### Preverjanje sporočil

Sprejemnik 3-D Secure sporočila mora preveriti ali XML sporočilo ustreza specifikacijam:

- XML sporočilo mora biti pravilno sestavljeno (XML pravilno);
- korenski element XML je ‘ThreeDSecure’;
- otrok korenskega elementa je element ‘Message’;
- otrok elementa ‘Message’ je sporočilo, ki ga komponenta pričakuje (npr. ACS lahko sprejme le sporočilo VEReq, PAReq ali Error, vsa ostala sporočila ACS zavrne);
- vsi zahtevani elementi poslanega sporočila morajo biti prisotni;

- id atribut sporočil odgovorov VERes, PARes in PATransRes mora biti enak id-ju sporočila zahtev.

**Razširitev sporočil**

3-D Secure sporočila je možno nadgraditi s poljem razširitev sporočil. V polju razširitev sporočil se lahko dodajajo polja po naslednji obliki

<Extension id = X  critical = false>...</Extension>.

Id atribut je identifikacijska številka razširitve. Critical atribut vsebuje vrednosti true (kritična razširitev) ali false (nekritična razširitev) kar označuje ali mora sprejemnik sporočila poznati razširitev. V kolikor je razširitev kritična in sprejemnik sporočila ne pozna razširitve, mora sprejemnik odgovoriti z odgovorom na sporočilo, ki označuje, da je prišlo do neznane zahteve.

**Opis vsebine sporočil**

V magistrskem delu sem sporočila opisal v tabelah. Tabele vsebujejo naslednje stolpce.

- Ime polja (kratko ime polja v sporočilu);
- DTD[14] (angl. *Document type Definition*) element (ime elementa v XML sporočilu);
- Prisotnost polja
  - R, obvezno polje;
  - O, opcijsko polje;
  - C, pogojno polje;
- Opis (daljši opis polja, namen polja, vsebina polja, itd.).

[14] DTD je jezik, ki omogoča opis XML strukture.

### 3.7.1 CReq

CRReq je sporočilo za pridobitev bin tabele vključenih kartic. Tabela 9 opisuje vsebino CReq sporočila.

***Tabela 9: Opis CReq sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Različica sporočila, npr. "1.0.2". Format: n+.n+[.n+]*. |
| Pridobiteljev bin | Merchant. acqBIN | R | Pridobiteljeva identifikacijska številka, določena s strani kartičnih inštitucij. DS na podlagi številke prepozna pridobitelja transakcije. |
| Prodajalčeva identifikacija številka | Merchant.merID | R | Prodajalčeva identifikacijska številka, ki jo določi pridobitelj transakcije. Se ne uporablja v različici 1.0.2. |
| Geslo | Merchant. password | C | Prodajalčevo geslo služi pridobitelju transakcije. Polje se ne uporablja v različici 1.0.2. |
| Serijska številka | serialNumber | O | Vrednost iz zadnjega CRes sporočila. Če je polje prazno, odgovor na CReq sporočilo vsebuje celotno bin tabelo. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.2 CRes

CRRes sporočilo je odgovor na sporočilo za pridobitev bin tabele vključenih kartic. Tabela 10 opisuje vsebino CRes sporočila.

***Tabela 10: Opis CRes sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. |
| Rang kartic | CR | C | Če CReq ne vsebuje serijske številke nosi sporočilo vse range vključenih kartic. |
| Prva številka v rangu kartic | CR.begin | R | Začetna številka ranga kartic. |
| Zadnja številka v rangu kartic | CR.end | R | Končna številka ranga kartic. |
| Akcija | CR.action | R | Če CReq vsebuje serijsko številko, vsebuje polje akcijo, ki jo je potrebno izvršit glede na zadnjo serijsko številko bin tabele. A – dodaj rang kartic, D – izbriši rang kartic. |
| Serijska številka | serialNumber | C | Serijska številka poslane bin tabele. |
| Podatki o neznani zahtevi | IReq | C | Polje je obvezno, če DS ni zmožen obdelati CReq sporočilo zaradi poslovnih pravil 3-D Secure sistema iz Tabele 18. |
| Šifra neznane zahteve | IReq.iReqCode | R | Koda, neznane zahteve. Tabela 18 vsebuje razloge, ki lahko privedejo do neznane zahteve. |
| Podrobnosti neznane zahteve | IReq.iReqDetail | C | Podroben opis napake. |
| Šifra proizvajalca | IReq. vendorCode | O | Koda napake proizvajalca programske opreme. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.3 VEReq

VEReq je sporočilo, s katerim preverimo vključenost imetnika kartice v program. Tabela 11 opisuje vsebino VEReq sporočila.

***Tabela 11: Opis VEReq sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. |
| Številka kartice | pan | R | Številka kartice, ki jo je podal imetnik kartice pri potrditvi nakupa. |
| Pridobiteljeva bin | Merchant. acqBIN | R | Glej opis CReq sporočila. |
| Prodajalčeva identifikacijska številka | Merchant.merID | R | Glej opis CReq sporočila. |
| Geslo | Merchant. password | C | Glej opis CReq sporočila. |
| Tip naprave | Browser. deviceCategory | O | Označuje tip naprave, ki uporablja imetnik kartice: 0 – osebni računalnik, 1 - mobilni telefon, 2 – mobilna naprava z uporabo SMS sporočil, 3 - govorni kanal. Če ACS ne omogoča preverjanje s podano napravo, pošlje v sporočilu VERes Status enak U. |
| Omogočene glave http | Browser. accept | C | Polje vsebuje podatke brskalnika. S pomočjo polja ACS ugotovi ali zna prikazati okno za overjanje ter v VERes sporočilu izbere pravilni ACS URL. |
| Uporabnikov agent | Browser. userAgent | C | Polje se ne uporablja v različici 1.0.2. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno obdelavo VEReq sporočila in niso definirana v samem VEReq sporočilu. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.4 VERes

VERes je sporočilo odgovora na sporočilo preverjanja vključenosti v program. Tabela 12 opisuje vsebino VERes sporočila.

***Tabela 12: Opis VERes sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. Različica sporočila mora biti enaka kot v VEReq sporočilu. |
| Status | CH. enrolled | R | Status, ki označuje ali je imetnika kartice možno overiti. Y – overitev je možna, N – imetnik kartice ni vključen v program, U – imetnika kartice ni možno overiti zaradi tehničnih težav. |
| Številka računa | CH.acctID | C | Številka računa, ki identificira VEReq sporočilo in se uporablja v sporočilih PAReq, PATransReq.<br>Polje je obvezno, če je status odgovora preverjanja Y. |
| ACS URL | url | C | URL naslov, na katerega mora MPI poslati PAReq sporočilo. Polje je obvezno, če je Status enak Y. |
| Plačilni protokol | protocol | C | Polje vsebuje vedno vrednost ‘ThreeDSecure’. |
| Podatki o neznani zahtevi | IReq | C | Polje je obvezno, če ACS ni zmožen obdelati VEReq sporočilo zaradi poslovnih pravil 3-D Secure (Tabela 18). |
| Šifra neznane zahteve | IReq.iReqCode | R | Glej opis CReq sporočila. |
| Podrobnosti neznane zahteve | IReq.iReqDetail | C | Glej opis CReq sporočila. |
| Šifra proizvajalca | IReq. vendorCode | O | Glej opis CReq sporočila. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno obdelavo VERes sporočila in niso definirana v samem VERes sporočilu. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.5 PAReq

PAReq je sporočilo, s katerim zahtevamo overjanje imetnika kartice. Tabela 13 opisuje vsebino PAReq sporočila.

***Tabela 13: Opis PAReq sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. Različica sporočila mora biti enaka kot v VEReq sporočilu. |
| Pridobiteljev bin | Merchant. acqBIN | R | Glej opis CReq sporočila. Polje mora imeti enako vrednost kot v sporočilu VEReq. |
| Prodajalčeva identifikacija številka | Merchant.merID | R | Glej opis CReq sporočila. Polje mora imeti enako vrednost kot v sporočilu VEReq. |
| Prodajalčevo ime | Merchant.name | R | Vrednost uporabi ACS za prikaz na oknu za overjanje. |
| Prodajalčeva država | Merchant. country | R | Šifra države prodajalca, po ISO 3166 kodni tabeli. Če šifra ne obstaja, ACS odgovori s PARes sporočilom, IreqCode = 54. |
| Prodajalčev URL | Merchant.url | R | Celotni URL naslov prodajalčeve spletne strani. |
| Številka transakcije | Purchase.xid | R | Identifikacijska številka transakcije kot jo določi prodajalec. Vrednost je zapisana v Base64 formatu. |
| Datum in čas transakcije | Purchase.date | R | Datum in čas transakcije, po GMT časovni coni. Format: YYYYMMDD HH:MM:SS. ACS uporabi vrednost za prikaz na oknu za overjanje. |
| Znesek za prikaz | Purchase. amount | R | Polje se v verziji 1.0.2. ne uporablja. |
| Znesek nakupa | Purchase. purchAmount | R | Znesek nakupa brez decimalne vejice. Vrednost 123.45 je zapisana kot 12345. ACS uporabi za prikaz na oknu za overjanje. |
| Valuta nakupa | Purchase. currency | R | Šifra valute, po ISO 4217 kodni tabeli. ACS uporabi za prikaz na oknu za preverjanje. Če šifra ne obstaja, ACS odgovori s PARes sporočilom, IreqCode = 54. |

»se nadaljuje«

»nadaljevanje«

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Eksponenta valute | Purchase. exponent | R | Število decimalk, ki jih predpisuje valuta po kodni tabeli ISO 4217. Primer: EUR ima vrednost 2, Japonski Yen pa vredno 0. ACS uporabi za prikaz na oknu za preverjanje. |
| Opis nakupa | Purchase.desc | O | Kratek opis nakupa. |
| Podatki ponavljajočega plačila | Purchase.Recur | C | Polja ponavljajočega plačila so obvezna, če sta se prodajalec in kupec dogovorila za ponavljajoči nakup (npr. naročnina na revijo). |
| Frekvenca plačil | Recur. frequency | R | Število dni med ponavljajočimi plačili. |
| Zapadlost plačil | Recur. endRecur | R | Datum zadnjega ponavljajočega plačila. |
| Podatki obročnega plačila | Purchase.install | C | Polje vsebuje število obrokov plačila. |
| Številka računa | CH.acctID | R | Podatek je enak kot v VERes sporočilu. Če ACS ne najde VERes sporočilo z enakim acctID, odgovori s sporočilom PARes, IreqCode = 55. |
| Zapadlost kartice | CH.expiry | R | Datum zapadlosti kartice. Format: YYMM. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno izvedbo PAReq sporočila in niso definirana v samem PAReq sporočilu. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.6 PARes

PARes je odgovor na sporočilo, s katerim zahtevamo overjanje imetnika kartice. Tabela 14 opisuje vsebino PARes sporočila.

***Tabela 14: Opis PARes sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. Različica sporočila mora biti enaka kot v PAReq sporočilu. |
| Pridobiteljeva identifikacija | Merchant. acqBIN | R | Enaka vrednost kot v PAReq sporočilu. |
| Prodajalčeva identifikacijska številka | Merchant.mer ID | R | Enaka vrednost kot v PAReq sporočilu. |
| Številka transakcije | Purchase.xid | R | Enaka vrednost kot v PAReq sporočilu. |
| Datum in čas nakupa | Purchase.date | R | Enaka vrednost kot v PAReq sporočilu. |
| Znesek nakupa | Purchase. purchAmount | R | Enaka vrednost kot v PAReq sporočilu. |
| Valuta nakupa | Purchase. currency | R | Enaka vrednost kot v PAReq sporočilu. |
| Eksponenta valute | Purchase. exponent | R | Enaka vrednost kot v PAReq sporočilu. |
| Številka kartice | pan | R | Če je rezultat overjanja Y ali A, vsebuje polje samo zadnje 4 številke kartice (manjkajoče številke se nadomestijo z ničlami). Za rezultata overjanja N in U vsebuje samo ničle. |
| Čas digitalnega podpisa | TX.time | R | Datum in čas digitalnega podpisa, po GMT časovni coni. Format: YYYYMMDD HH:MM:SS. |
| Rezultat overjanja | TX.status | R | Y – overitev imetnika je uspela, N – overitev imetnika ni uspela, U – overitev imetnika ni uspela zaradi tehničnih težav, A – prišlo je samo do poizkusa overjanja imetnika. |
| Podatki preverjanja imetnika | TX.cavv | C | Polje je obvezno, če je status transakcije Y ali A. CAVV vrednost izračuna izdajatelj kartice s pomočjo podatkov transakcije in skritega ključa. |

»se nadaljuje«

»nadaljevanje«

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Številka elektronskega poslovanja | TX.eci | C | Številka elektronskega poslovanja je obvezna, če je status transakcije Y ali A. Če je rezultat overjanja Y, vsebuje 05 v VBV ter 02 v MSC programu. Če je rezultat overjanja A, vsebuje 06 v VBV ter 01 v MSC programu. |
| CAVV algoritem | TX. cavvAlgorithm | C | Označuje algoritem uporabljen za izračun polja CAVV: 0 - HMAC (ni v 1.0.2 različici), 1 - CVV (ni v 1.0.2 različici), 2 - CVV z ATN (VBV program), 3 - MasterCard SPA algoritem. |
| Podatki o neznani zahtevi | IReq | C | Polje je obvezno, če ACS ni zmožen obdelati PAReq sporočilo zaradi poslovnih pravil definiranih v Tabeli 18. |
| Šifra neznane zahteve | IReq.iReqCode | R | Glej opis CReq sporočila. |
| Podrobnosti neznane zahteve | IReq.iReqDetail | C | Glej opis CReq sporočila. |
| Šifra proizvajalca | IReq. vendorCode | O | Glej opis CReq sporočila. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno obdelavo PARes sporočila in niso definirana v samem PARes sporočilu. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

### 3.7.7 PATransReq

PATransReq je sporočilo, s katerim obvestimo zgodovinski strežnik o 3-D Secure transakciji. Tabela 15 opisuje vsebino PATransReq sporočila.

***Tabela 15: Opis PATransReq sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. Različica sporočila mora biti enaka kot v PARes sporočilu. |
| Prodajalčevo ime | Merchant.name | R | Enaka vrednost kot v PAReq sporočilu. |
| Prodajalčeva država | Merchant.country | R | Enaka vrednost kot v PAReq sporočilu. |
| Prodajalčev URL | Merchant.url | R | Enaka vrednost kot v PAReq sporočilu. |
| Znesek za prikaz | Purchase.amount | R | Enaka vrednost kot v PAReq sporočilu. |
| Opis nakupa | Purchase.desc | R | Enaka vrednost kot v PAReq sporočilu. |
| Podatki obročnega plačila | Purchase.Recur | R | Enaka vrednost kot v PAReq sporočilu. |
| Frekvenca obrokov | Recur.frequency | R | Enaka vrednost kot v PAReq sporočilu. |
| Zapadlost obrokov | Recur.endRecur | R | Enaka vrednost kot v PAReq sporočilu. |
| Podatki plačila z zamikom | Purchase.install | R | Enaka vrednost kot v PAReq sporočilu. |
| Ime imetnika kartice | CH.name | R | Ime in priimek imetnika kartice. |
| Številka kartice | CH.fullPAN | R | Enaka vrednost kot v VEReq sporočilu. |
| Zapadlost kartice | CH.expiry | R | Enaka vrednost kot v PAReq sporočilu. |
| Šifra ACS | ACSAuth.acsId | R | Polje se v različici 1.0.2 ne uporablja. |
| ACS uporabniško ime | ACSAuth.loginId | R | Polje se v različici 1.0.2 ne uporablja. |
| ACS geslo | ACSAuth.password | R | Polje se v različici 1.0.2 ne uporablja. |
| PARes | SignedPARes | R | Digitalno podpisano PARes sporočilo. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno obdelavo PATransReq sporočila in niso definirana v samem PATransReq sporočilu. |

*Vir: Visa Int., 3-D Secure Functional Requirements, Access Control Server, 2004a.*

### 3.7.8 PATransRes

PATransRes je odgovor na sporočilo, s katerim obvestimo zgodovinski strežnik o 3-D Secure transakciji. Tabela 16 opisuje vsebino PATransRes sporočila.

***Tabela 16: Opis PATransRes sporočila***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. Različica sporočila mora biti enaka kot v PATransReq sporočilu. |
| Podatki o neznani zahtevi | IReq | C | Polje je obvezno, če zgodovinski strežnik ni zmožen obdelati PATransReq sporočilo zaradi poslovnih pravil 3-D Secure iz Tabele 18. |
| Šifra neznane zahteve | IReq.iReqCode | R | Glej opis CReq sporočila. |
| Podrobnosti neznane zahteve | IReq.iReqDetail | C | Glej opis CReq sporočila. |
| Šifra proizvajalca | IReq. vendorCode | O | Glej opis CReq sporočila. |
| Razširitev sporočila | Extension | O | Vsa dodatna polja, ki so pomembna za pravilno obdelavo PATransRes sporočila in niso definirana v samem PATransRes sporočilu. |

*Vir: Visa Int., 3-D Secure Functional Requirements, Access Control Server, 2004a.*

### 3.7.9 Error

Komponenta pošlje Error sporočilo, ko prejeto sporočilo ne more biti obdelano na nivoju protokola (na primer napačen XML). Tabela 17 opisuje vsebino Error sporočila.

***Tabela 17: Opis sporočila Error***

| Ime polja | DTD element | Prisotnost | Opis |
|---|---|---|---|
| Različica sporočila | version | R | Glej opis CReq sporočila. |
| Šifra napake | errorCode | R | Glej šifrant napak.. |
| Opis napake | errorMessage | R | Glej šifrant napak. |
| Podrobnosti napake | errorDetail | R | Podrobnost napake. |
| Šifra proizvajalca | vendorCode | O | Glej opis CReq sporočila. |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

Prejemnik Error sporočila mora vedno odgovoriti z odgovorom HTTP 200 OK. Če je komponenta iz napačnega sporočila uspela prebrati id sporočila, mora sporočilo Error imeti

enako id številko napačnega sporočila. V nasprotnem primeru komponenta sama ustvari unikatno vrednost id sporočila. Razlogi vseh možnih napak so opisani v Tabeli 18.

***Tabela 18: Šifrant napak***

| Šifra napake | Opis napake (angleški jezik) | Opis napake (prevod) |
|---|---|---|
| 1 | Root element invalid. | Napačen korenski element XML sporočila. |
| 2 | Message element not a defined message | Poslani XML ne vsebuje pričakovanega sporočila. |
| 3 | Required element missing. | Zahtevan element sporočila manjka. |
| 4 | Critical element not recognized. | Kritična razširitev sporočila ni prepoznana. |
| 5 | Format of one or more elements is invalid according to the specification. | Format enega ali več elementov sporočila ne ustreza specifikaciji. |
| 6 | Protocol version too old. | Različica sporočila je prestara. |
| 98 | Transient system failure. | Trenutna napaka na sistemu (na primer sistem ne uspe obdelati sporočila zaradi prezasedenosti). |
| 99 | Permanent system failure. | Trajna napaka na sistemu (na primer ob napaki na bazi podatkov). |

*Vir: Visa Int., 3-D Secure Protocol Specifications, Core Functions, 2004b.*

## 3.8 Izpolnjevanje zahtev elektronskih plačilnih sistemov

Obstoj elektronskega plačilnega sistema je v veliki meri odvisen od načina izpolnjevanja zahtev elektronskih plačilnih sistemov iz poglavja 2.3.2. V nadaljevanju so podane ugotovitve kako 3-D Secure izpolnjuje zahteve elektronskih plačilnih sistemov.

3-D Secure sistem uporablja standarden način prenosa šifriranih podatkov z uporabo SSL/TLS protokola. Neokrnjenost podatkov je zagotovljena z avtorizacijo plačilnih podatkov in digitalnim podpisom izdajatelja kartice. V sistemu kupec identificira prodajalca preko strežniškega certifikata, medtem ko ga pridobitelj transakcije identificira preko odjemalčevega certifikata, ki ga prodajalec predloži pri vzpostavitvi povezave. Overitev imetnika kartice omogoča prodajalcu, da zaupa v kupca. MasterCard in Visa sta s pravili zavračanja transakcij jasno določila odgovornosti v primeru zlorab. Preprečitev tajenja komunikacije je zagotovljena s pomočjo infrastrukture javnih ključev. Napad v javnem delu komunikacij, v katerem se pošiljata sporočili PAReq in PARes, je nemogoč, saj je za izdelavo PAReq sporočila potrebna številka računa, ki se jo izmenjuje v privatnem delu komunikacij s sporočilom VERes. Pomembno je tudi preverjanje ali PAReq sporočilo vsebuje enake podatke kot VEReq sporočilo.

Glavna prednost 3-D Secure sistema pred svojimi predhodniki je v izpolnjevanju implementacijskih zahtev. Za prodajalca je sistem boljši, saj lahko ohrani enak potek nakupa kot pri uporabi SSL/TLS načina plačila. Prodajalcu je sistem prijaznejši in cenejši, saj je za podporo sistemu potrebno namestiti samo vtičnik (MPI). Imetnik kartic za razliko od sistema SET uporablja samo brskalnik oziroma tudi pametno kartico. Nameščanje dodatnih nestandardnih aplikativnih komponent sistema povzroča večjo kompleksnost in otežuje uporabo imetnikom kartice ter s tem zmanjšuje uporabnost sistema. Zaradi manj kompleksnih mehanizmov je transakcija v 3-D Secure sistemu hitrejša kot pri njegovih predhodnikih. Še vedno pa za 3-D Secure sistem velja, da je hitrost izvedbe transakcije odvisna od hitrosti izvedbe vsake komponente sistema. Sistem uporablja standarden format sporočil XML, standarden protokol komunikacije HTTP preko SSL/TLS, omogoča uporabo različnih naprav pri izvedbi transakcije in različne mehanizme overjanja. Taka standardizacija omogoča lažje razumevanje sistema in hkrati lažje obvladovanje napak.

# 4 RAZVOJ IN IMPLEMENTACIJA IZDAJATELJEVIH KOMPONENT

Do projekta razvoja izdajateljevih 3-D Secure komponent je prišlo zaradi zamenjave zastarelih plačilnih vrat, ki smo jih v podjetju uporabljali za pridobivanje transakcij na internetu. Pri iskanju novih plačilnih vrat smo se prvič soočili s tehnologijo 3-D Secure. Podpora 3-D Secure tehnologiji kot pridobitelju transakcij je brez vključenih imetnikov kartic nezanimiva. Ker se podjetje ukvarja s pridobivanjem transakcij in izdajanjem kartic, smo se v podjetju odločili za podporo tehnologiji iz obeh strani. Iskanje ponudnikov komponent 3-D Secure tehnologije je pripeljalo do ugotovitve, da noben ponudnik v osnovi ne ponuja razširljivo rešitev, ki bi izdajatelju kartic omogočala uporabo zunanjega mehanizma za overitev imetnika. V primeru našega podjetja je bil to mehanizem overjanja z uporabo pametne kartice. Zaradi slabih ponudb in dovolj usposobljenega kadra v razvoju smo se v podjetju odločili za lasten razvoj. V času implementacije izdajateljevih komponent ni bilo izdajatelja kartic, ki bi kot mehanizem overjanja v 3-D Secure tehnologiji uporabljal pametno kartico. Tako smo se kot v mnogih drugih primerih v podjetju izkazali kot pionir v novih tehnologijah.

## 4.1 Metodologija razvoja

Metodologija je skupek postopkov, tehnik, orodij in dokumentacijskih pripomočkov, ki jih uporabljajo razvijalci sistema pri načrtovanju in implementiranju informacijskega sistema. Sestavljena je iz faz in podfaz, ki vodijo razvijalce sistema pri izbiri primernih tehnik v vsaki fazi projekta. Pomagajo jim tudi pri načrtovanju, upravljanju, kontroliranju in vrednotenju projektov izgradnje informacijskih sistemov (Avison, Fitzgerald, 1996).

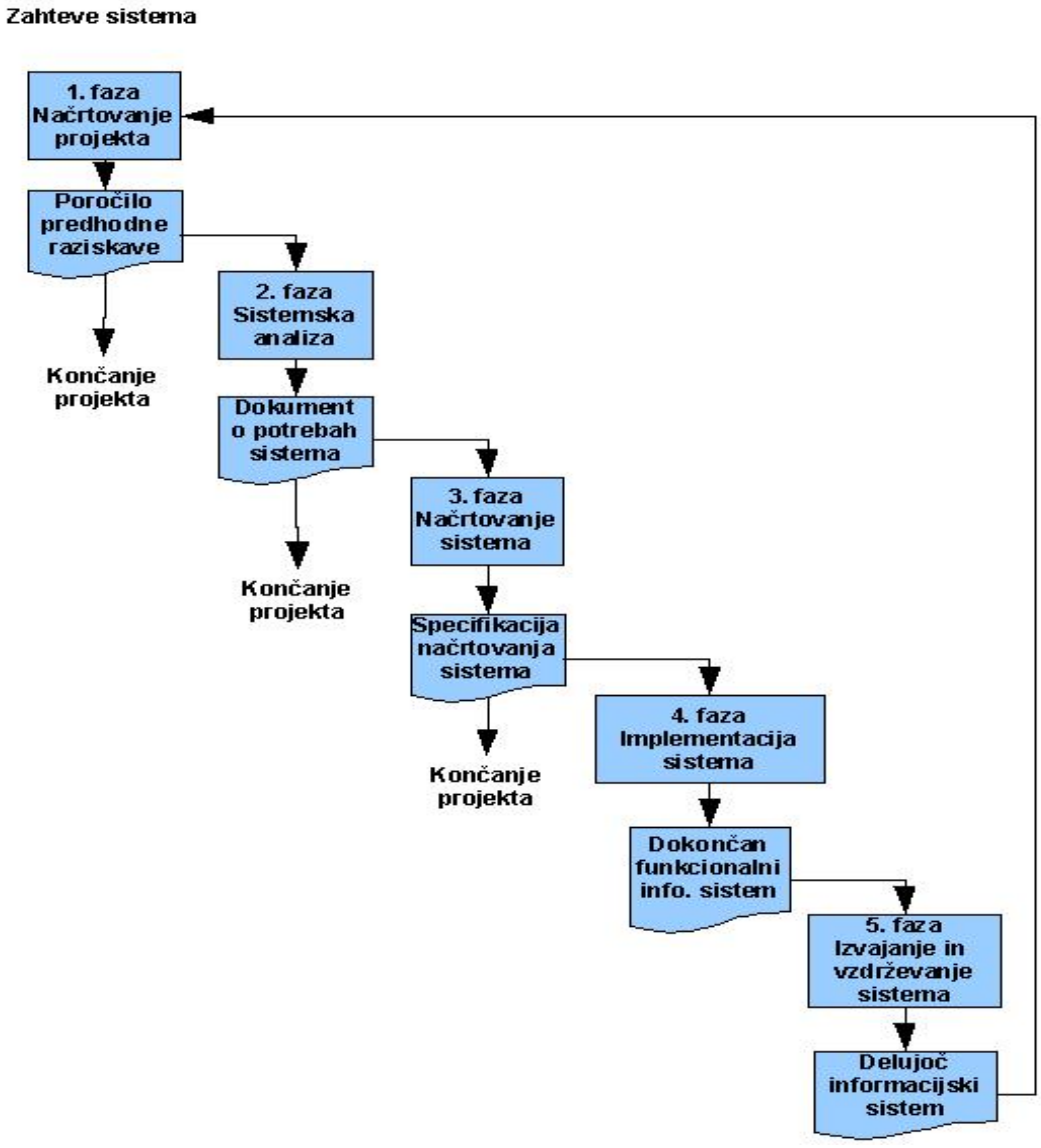
Metodologija življenjskega cikla (angl. *System Development Life Cycle*), ali drugače kaskadni model razvoja je najbolj primerna za izgradnjo velikih informacijskih sistemov, ki bodo v uporabi dlje časa. Življenjski cikel razvoja sistema ima pet faz, ki si sledijo zaporedno (Shelly, Cashman, Rosenblatt, 2001) in so prikazane na Sliki 19:

- **načrtovanje -** v tej fazi analiziramo izvedljivost projekta, postavimo roke in dodelimo odgovornosti;
- **analiza -** tu pregledamo zahteve, jih analiziramo in na koncu predlagamo rešitev;
- **oblikovanje -** za to fazo so značilni oblikovanje izhodov, vhodov ter baza podatkov;
- **izvedba -** sledijo razvoj in namestitev ter ocena dela;
- **delovanje in vzdrževanje -** po zaključku projekta sistem deluje in ga je potrebno vzdrževati.

Seveda je nerealno pričakovati, da se v razvoju ne bi nikoli vrnili v predhodno fazo. V praksi se v posamezni fazi odkrivajo napake, ki so bile storjene v prejšnjih, zato je vračanje nekaj normalnega.

Metoda življenjskega cikla je bila najbolj primerna metoda za razvoj 3-D Secure izdajateljevih komponent zaradi njene linearnosti in dejstva, da so bile že vnaprej definirane zahteve sistema. Narediti je bilo potrebno začetno analizo, oblikovanje sistema, izdelavo sistema, overitev in implementacijo sistema v produkcijskem okolju.

***Slika 19: Kaskadni model razvoja informacijskega sistema***




*Vir: Shelly, Cashman, Rosenblatt, Systems Analysis and Design, 2001.*

## 4.2 Načrtovanje projekta

Namen prve faze je, da se točno identificira celotno področje problema. V tej fazi izvedemo predhodno raziskavo, ki je ključnega pomena, saj bo rezultat tega dela vplival na celotni proces razvoja. Analitik mora biti v celoti seznanjen kaj se od novega sistema pričakuje in zahteva (Shelly, Cashman, Rosenblatt, 2001).

Prednosti 3-D Secure sistema so bile že vnaprej znane, potrebno je bilo le oceniti ali bo sistem sprejet med imetniki kartic ter ali bo projekt povrnil stroške izdelava programske opreme in nabave ustrezne strojne opreme. Pri analizi tehnične izvedljivosti projekta je bilo ugotovljeno, da v podjetju razpolagamo z dovolj tehničnega znanja ter da je informacijska infrastruktura podjetja ustrezno pripravljena za podporo projekta. Analiza ekonomske izvedljivosti projekta je pokazala, da se vlaganje v projekt izplača, da je lasten razvoj cenejši kot nakup programske opreme. Operativna izvedljivost projekta je pokazala, da bi bilo z ustreznim številom človeških virov možno izvesti projekt v treh mesecih. Za vzpodbuditev prodajalcev in imetnikov kartic smo ob zaključku projekta načrtovali konferenco, na kateri bi predstavili 3-D Secure tehnologijo.

## 4.3 Sistemska analiza

V drugi fazi se sistemski analitik točno seznani z zahtevami sistema ter išče ustrezne rešitve. Na podlagi tega razvije logični model predlaganega sistema (Shelly, Cashman, Rosenblatt, 2001). V podjetju smo najprej strukturirali potrebe projekta, nato pa ugotovljene potrebe analizirali.

### 4.3.1 Strukturiranje potreb projekta

Strukturiranje potreb projekta je ključnega pomena, saj bo rezultat vplival na lastnosti novega informacijskega sistema. Eden od najbolj pogostih in učinkovitih načinov zbiranja informacij o potrebah informacijskega sistema so intervjuji in pregled dokumentacije. Strukturirane tehnike za razvoj informacijskih sistemov so se razvile v sedemdesetih letih (Gradišar, Resinovič, 2001), njihov glavni cilj pa je bil:

- povečanje produktivnosti pri razvoju;
- zmanjšanje števila napak;
- odkrivanje napak v zgodnejših fazah razvoja;
- boljša komunikacija razvijalcev z uporabniki;
- krajši čas razvoja;
- večja kvaliteta razvitega sistema.

Večina potreb 3-D Secure sistema smo v podjetju ugotovili s prebiranjem dokumentacije. Za nejasne zahteve sistema smo povprašali zadolžene za 3-D Secure projekt na strani MasterCard-a

in Vise. Izdajatelj kartic mora za popolno podporo 3-D Secure sistemu izdelati strežnik za vključitev v sistem, strežnik za upravljanje z dostopi ter strežnik za overjanje podatkov 3-D Secure.

Strežnik vključitve mora omogočati:

- spletno stran za imetnika kartice, zavarovano s strežniškim certifikatom;
- vključitev imetnikov Visa in MasterCard kartic;
- možnost lastne izdelave spletnega vmesnika s strani partnerja podjetja (banke);
- overitev imetnika kartice
  - preverjanje enkratnih gesel pametne kartice;
  - preverjanje podatkov kartice (datum veljavnosti, CVC koda);
- začetni vnos in kasnejše upravljanje s podatki imetnika kartice

Strežnik za upravljanje z dostopi mora omogočati:

- varno komunikacijo preko SSL;
- obdelavo VEReq in PAReq sporočil;
- upravljanje s ključi in certifikati;
- pošiljanje PATransReq sporočil na zgodovinski strežnik;
- podporo za Visa in MasterCard kartice;
- podporo različnim partnerjem podjetja;
- visoko razpoložljivost sistema;
- overitev imetnika kartice
  - preverjanje enkratnih gesel pametne kartice;
- administracijo sistema.

Strežnik overjanja podatkov 3-D Secure mora omogočati:

- povezavo z avtorizacijskim strežnikom;
- preverjanje podatka CAVV.

### 4.3.2 Analiza potreb projekta

Ko zberemo vse zahteve, jih je treba skrbno analizirati in izdelati podroben načrt za rešitev problemov (Shelly, Cashman, Rosenblatt, 2001).

**Analiza potreb vključitvenega strežnika**

Del vključitvenega strežnika je javna spletna stran, na kateri se imetniki kartic prijavijo v 3-D Secure program. Javna spletna stran omogoča prijavo imetnikov kartic različnih partnerjev našega podjetja. Na javni spletni strani se prikazuje le logotip blagovne znamke našega podjetja

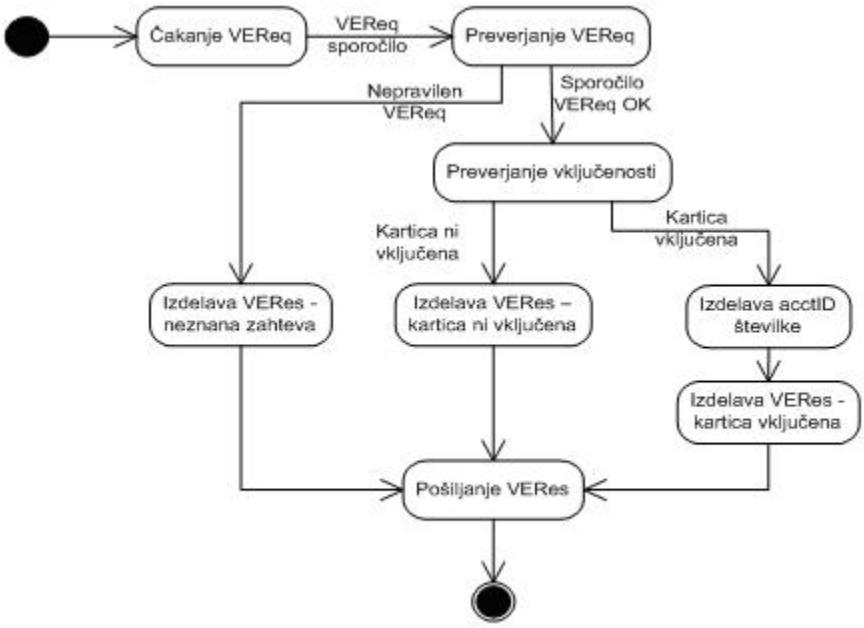
in ne logotip posameznega partnerja. Komunikacija z javno spletno stranjo je zaščitena s strežniškim certifikatom, izdanim s strani ene od komercialnih CA. Zaradi pravil sistema mora biti spletna stran vključitve v sistem ločena za imetnike kartic Visa in MasterCard (Visa Int., 2001d). Posameznemu partnerju mora biti omogočena izdelava lastnega vmesnika za vključitev v sistem zaprte narave, na primer v lastni spletni banki. V tem primeru se partnerjev spletni vmesnik ob izvedbi prijave v 3-D Secure sistem povezuje na vključitveni strežnik našega podjetja. Vključitveni strežnik mora overiti imetnika kartice. Spletna stran za prijavo najprej zahteva vnos številke kartice, datum veljavnosti in CVC kodo kartice. Vključitveni strežnik mora znati preveriti ali so podatki kartice pravilni. Imetnik kartice se v nadaljevanju predstavi tako, da svojo pametno kartico vstavi v čitalnik za izdelavo enkratnih gesel, vnese pozivno številko, ki mu jo je spletna stran prikazala, vnese PIN v čitalnik in prepiše izdelano enkratno geslo v spletni vmesnik. Spletni vmesnik geslo preveri in v primeru uspešnosti nadaljuje s postopkom prijave. V nadaljevanju imetnik kartice vpiše svoje podatke (ime, priimek, naslov, elektronska pošta, telefonska številka) in izbere svoje pozdravno sporočilo, ki ga bo pozdravilo na oknu za overjanje pri izvedbi 3-D Secure transakcije. Vključitveni strežnik mora omogočiti imetniku kartice upravljanje svojih podatkov.

**Analiza potreb strežnika za upravljanje z dostopi**

Strežnik za upravljanje z dostopi mora znati komunicirati preko varne SSL povezave po HTTP protokolu. Ko gre za javni del komunikacij, strežnik vzpostavi povezavo s predložitvijo svojega strežniškega certifikata izdanega s strani komercialnega CA-ja in ne zahteva odjemalčevega certifikata. V privatnem delu komunikacij strežnik vzpostavi povezavo s predložitvijo strežniškega certifikata izdanega s strani MasterCard-a ali Vise ter zahteva predložitev odjemalčevega certifikata, ki je prav tako izdan s strani MasterCard-a ali Vise. Vsi certifikati, ki jih strežnik za upravljanje z dostopi uporablja pri vzpostavitvi komunikacije, morajo biti izdelani v varnem okolju, privatni ključi certifikatov pa morajo biti shranjeni na HSM napravi (MasterCard Int., 2005b). Privatni ključ ne sme nikoli zapustiti okolja izdelave oziroma se ne sme nikoli pojaviti v čisti obliki.

Strežnik mora znati obdelati VEReq XML sporočilo tako, da preveri sintaktično in vsebinsko pravilnost sporočila. Če je preverjanje uspešno, mora strežnik preveriti ali je imetnik kartice vključen v sistem, tako da pregleda podatke vključitvenega strežnika. V primeru, da je imetnik vključen v sistem, mora strežnik izdelati številko računa acctID, ki je enolično določena na VEReq sporočilo. Strežnik VEReq sporočilo shrani v bazo podatkov, saj mora v nadaljevanju pri obdelavi PAReq sporočila v primeru vključenosti imetnika uporabiti podatke VEReq sporočila. Zaradi reklamacij in preglednosti sistema se morajo vsa VEReq sporočila shraniti v bazo podatkov. Na koncu mora strežnik odgovoriti z VERes sporočilom, ki vsebuje podatke o obdelavi VEReq sporočila in rezultat ali je imetnik kartice vključen v sistem. Slika 20 prikazuje obdelavo VEReq sporočila v obliki diagrama stanj.

*Slika 20: Diagram stanj obdelave sporočila VEReq*

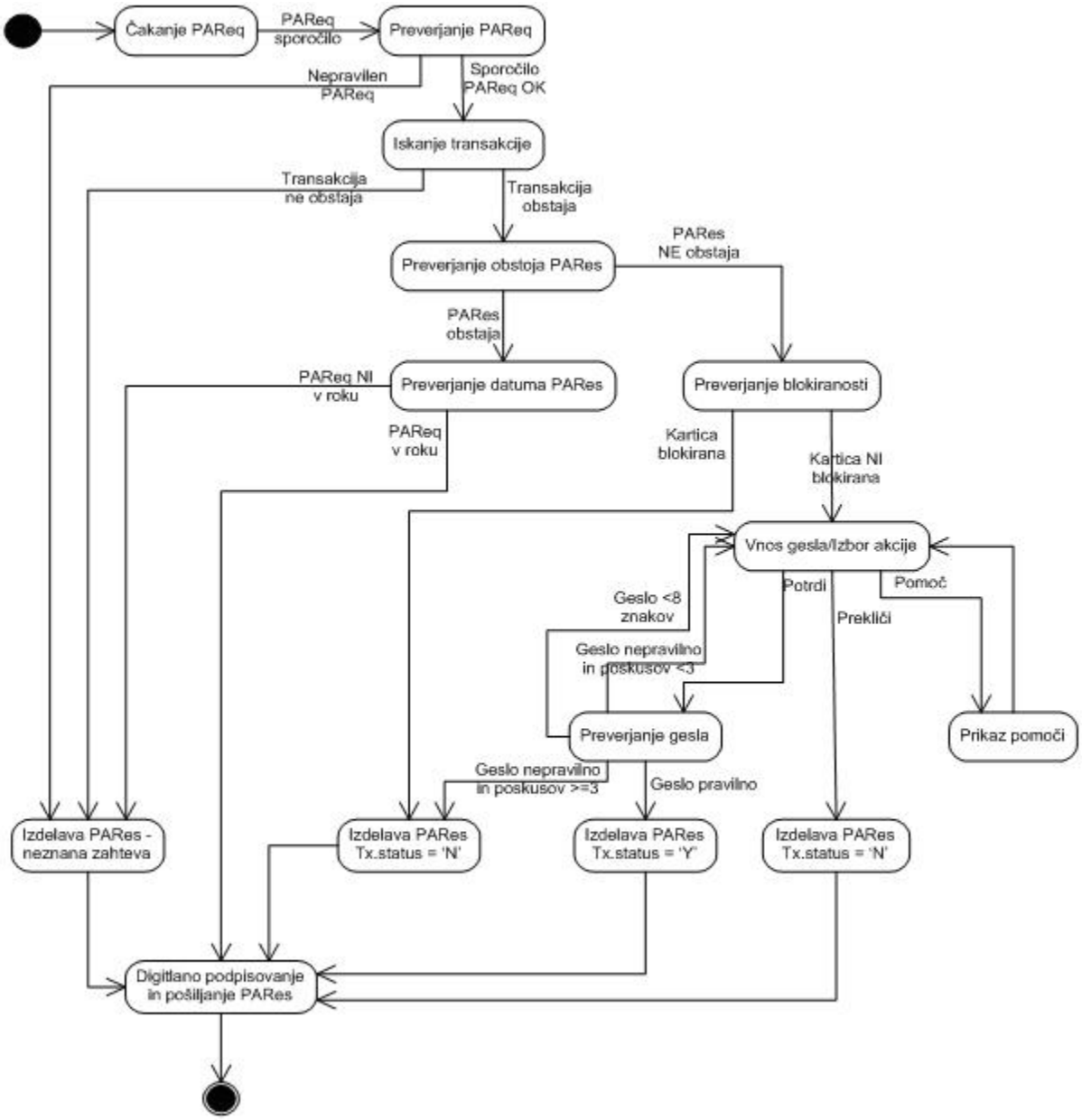



*Vir: lasten.*

Če je v VERes sporočilu zapisano, da je imetnik kartice vključen v program, prejme ACS sporočilo PAReq. Strežnik mora znati spreminjati sporočila iz Base64 v ASCII obliko in obratno. Prav tako mora znati sporočila stisniti in odtisniti po algoritmu ZLIB iz dokumenta RFC1951. Po pretvorbi sporočila mora strežnik preveriti sintaktično in vsebinsko pravilnost PAReq sporočila. Strežnik preko acctID podatka v sporočilu preveri, če obstaja VEReq sporočilo s podano številko računa. Zaradi specifik spletnih strani je možno, da bi sporočilo PAReq že predhodno obdelali in poslali PARes sporočilo. Strežnik mora preveriti obstoj PARes sporočila in v primeru obstoja poslati enako sporočilo nazaj na TermURL naslov. Pravila sistema določajo, da lahko tako PAReq sporočilo prispe do ACS najkasneje minuto po izdelavi PARes sporočila. Če je s PAReq sporočilom vse v redu mora strežnik izdelati spletno okno, na katerem se imetnik kartice identificira z vnosom enkratnega gesla, izdelanega s pomočjo pametne kartice. ACS na spletnem oknu prikaže podatke transakcije iz PAReq sporočila, pozdravno sporočilo imetnika kartice in pozivno številko, ki jo imetnik kartice uporabi za izdelavo enkratnega gesla. Imetnik kartice ima tri poskuse za vnos pravilnega gesla, nakar se njegova kartica za nastavljen čas blokira. Blokacija kartice se lahko izvede dvakrat zapored, nakar se kartica blokira za vedno oziroma do ročne deblokacije kartice. Spletno okno, ki ga strežnik izdela, mora omogočiti imetniku kartice preklic overjanja s pritiskom na gumb ‘prekliči’. Okno za overjanje mora prav tako nuditi pomoč pri identifikaciji (MasterCard Int., 2005a). Po zaključku overjanja izdela strežnik sporočilo PARes. Če je bil imetnik kartice uspešno overjen, mora strežnik izdelati podatek overjanja - CAVV in ga vključiti v sporočilo PARes. Strežnik ACS mora znati sporočilo digitalno podpisati s certifikatom za podpisovanje, ki je shranjen v HSM napravi. Tako izdelano sporočilo mora ACS poslati na TermURL naslov preko HTTP POST ukaza, ki ga

izvede javascript ukaz, nastavljen v oknu za overjanje. Podatki PAReq in PARes sporočila se morajo shraniti v bazo podatkov zaradi kasnejših reklamacij oziroma za pregled dogodkov overjanja. Slika 21 prikazuje obdelavo PAReq sporočila v obliki diagrama stanj.

***Slika 21: Diagram stanja obdelave sporočila PAReq***




*Vir: lasten.*

Strežnik ACS mora v primeru transakcije z Visa kartico poslati PATransReq sporočilo na zgodovinski strežnik. Če zgodovinski strežnik ne odgovori s PATransRes sporočilom, mora strežnik na vnaprej določen interval postopek ponoviti. MasterCard ne uporablja zgodovinskega strežnika, zato v primeru MasterCard transakcij ni potrebno pošiljati PATransReq sporočila. Strežnik ACS mora hkrati obvladati specifike VBV in MSC programa. Strežnik mora znati

upravljati z različnimi logotipi programov na oknu za overjanje ter uporabljati ustrezne certifikate za vzpostavitev povezave z Visa oziroma MasterCard privatnim delom komunikacije. ACS mora znati izdelati podatek overitve (CAVV) po algoritmu Vise in MasterCard-a. Pri prikazu okna za overjanje mora znati ACS prikazati logotip različnih partnerjev kartice. Kako to stori ACS, je razvidno iz Slike 18.

**Analiza potreb strežnika za overitev podatkov 3-D Secure**

Avtorizacijski strežnik prejme pri avtorizaciji transakcije 3-D Secure tudi podatek CAVV. Ker sam avtorizacijski strežnik ne obvlada overjanja CAVV, mora to izvesti strežnik za overjanje podatkov 3-D Secure. Strežnik mora omogočiti integracijo/komunikacijo z obstoječim avtorizacijskim strežnikom našega podjetja. CAVV podatek je izdelan z AAV (Visa) ali UCAF (MasterCard) algoritmom. Pri izdelavi podatka se uporabi številka transakcije iz PAReq sporočila, rezultat overjanja iz PARes sporočila, številka kartice in ključ, ki se uporablja samo za CAVV izračun.

## 4.4 Oblikovanje sistema

Cilj oblikovanja sistema je načrt, ki bo omogočal izdelati učinkovit, zanesljiv ter razširljiv informacijski sistem. Z njim izdelamo fizični model informacijskega sistema, ki mora zadoščati kriterijem iz dokumenta o potrebah sistema. Osnova za izdelavo fizičnega modela, ki pove, kako potrebe doseči, je logični model iz prejšnje faze, zato nam mora biti njegov koncept popolnoma jasen (Shelly, Cashman, Rosenblatt, 2001).

### 4.4.1 Platforma in orodja razvoja

Izbira okolja razvoja 3-D Secure tehnologije ni bila težavna, saj je izbrano okolje tipično okolje, ki ga v podjetju uporabljamo za razvoj informacijskega sistema.

3-D Secure sistem smo razvili za Microsoft Windows platformo. Windows smo si izbrali zaradi poznavanja tehnologije in predhodnih izkušenj s platformo. Za komuniciranje preko HTTP protokola po SSL/TLS povezavi smo si izbrali spletni strežnik Microsoft IIS 6.0, ki je vključen že v sam operacijski sistem Microsoft Windows Server 2003. Razvoj je potekal v Microsoftovem ogrodju .NET 2.0. Ogrodje .NET 2.0 omogoča izdelavo aktivnih spletnih strani (angl. *Active server pages* ali ASP.NET), spletnih servisov [15], Windows servisov in namiznih aplikacij. Za razvoj smo si izbrali programski jezik C#. Jezik C# smo si izbrali zaradi poznavanja in pozitivnih izkušenj. Razvoj je potekal v okolju Visual Studio 2005. Uporabljali smo repozitorij programske

[15] Spletni servis (angl. *Web Services*) je standard, definiran s strani W3C. Definiran je kot programski vmesnik, izdelan za podporo več uporabnosti med različnimi okolji, ki komunicirajo preko mreže (Wikipedia, 2008d).

kode Visual SourceSafe 6.0, ki je tesno povezan z razvojnim okoljem Visual Studio in je primeren za razvoj v skupinah. Baza podatkov, ki smo si jo izbrali, je IBM DB2 različica 8.0.

### 4.4.2 Komponente sistema

V načrtu sistema smo določili pet komponent, ki sestavljajo 3-D Secure komponente izdajatelja kartice. Te komponente so:

- **ACS spletna stran** - predstavitveni del 3-D Secure sistema;
- **ACS spletni servis** - poslovna komponenta, ki povezuje vse komponente sistema ter ima dostop do baze podatkov;
- **ACS servis** – komponenta, ki opravlja dostop do HSM naprave ter dostop do zgodovinskega strežnika;
- **ACS odjemalec –** omogoča vzdrževalcem sistema enostaven pregled in administracijo podatkov;
- **SCA servis** – s pomočjo HSM naprave upravlja s ključi sistema ter izračunava razne vrednosti na podlagi kriptografskih algoritmov.

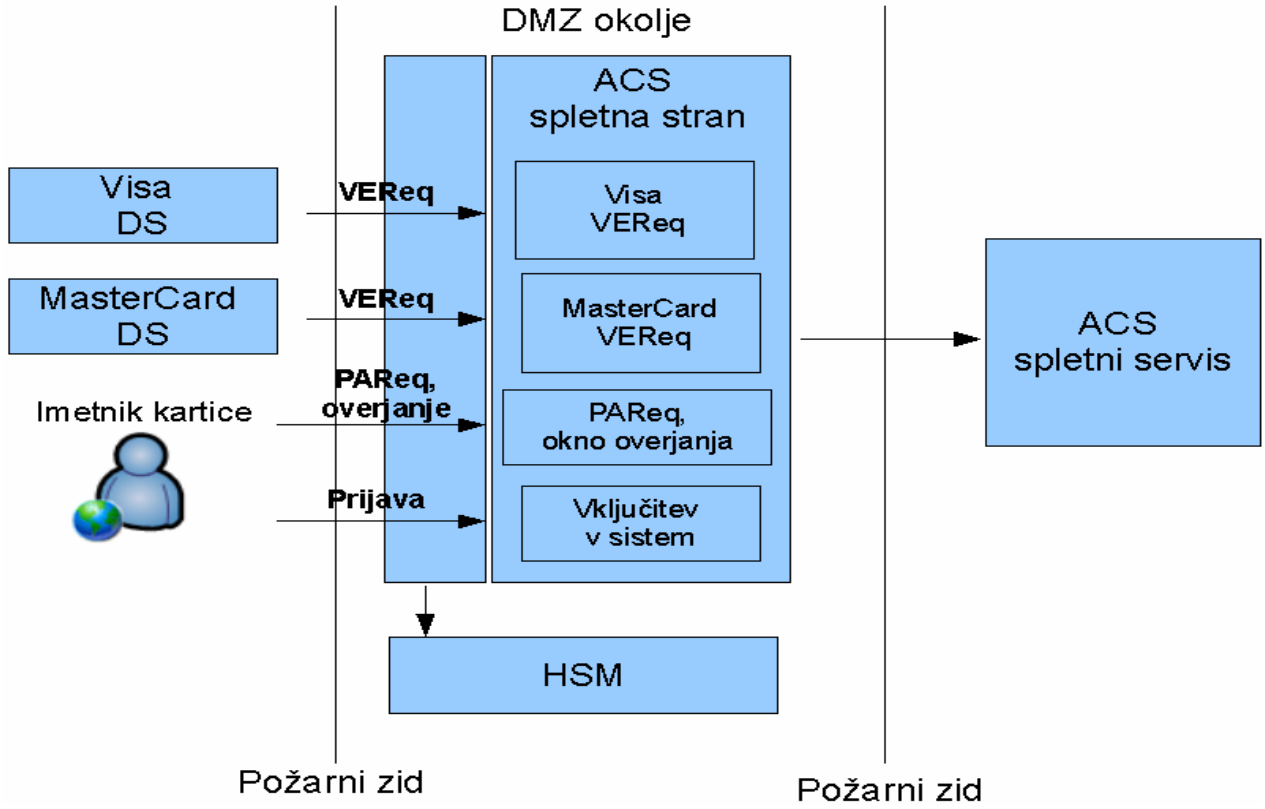
**ACS spletna stran**

ACS spletna stran se izvaja na spletnem strežniku IIS. Komponenta je vmesnik na internetu, preko katere zunanje okolje komunicira z našim podjetjem. ACS spletna stran je sestavljena iz štirih spletnih strani.

Prvi dve spletni strani sta v privatnem delu komunikacije in služita za prejemanje VEReq sporočil s strani Visa DS oziroma MasterCard DS. Spletni strani se predstavita s certifikatom Visa oziroma MasterCard. DS mora predložiti svoj odjemalčev certifikat, ki je lahko izdan le s strani Vise oziroma MasterCard-a. Tretja in četrta spletna stran sta v javnem delu komunikacij. Spletni strani se predstavita s strežniškim certifikatom in za prijavo ne zahtevata predložitve odjemalčevega certifikata. Tretja spletna stran služi za prejemanje PAReq sporočila in prikaz okna za overjanje. Imetniki kartic se lahko prijavijo v sistem preko četrte spletne strani, namenjene vključitvi v sistem. Slika 22 prikazuje umestitev ACS spletne strani med zunanjim okoljem in okoljem podjetja.

ACS spletna stran se nahaja v DMZ okolju za požarnim zidom in komunicira z ACS spletnim servisom v okolju podjetja. Certifikati, ki jih uporablja IIS za komunikacijo so izdelani v HSM napravi podjetja nCipher.

*Slika 22: Umestitev ACS spletne strani*




*Vir: lasten.*

**ACS spletni servis**

ACS spletni servis je poslovna komponenta strežnika za upravljanje s prijavami. Tehnologija spletnega servisa nam omogoča uporabo komponent iz različnih okolij. Komponenta ne vzdržuje spomina, kar pomeni, da je vsak priklic metode spletnega servisa obravnavan ločeno. Spletni servis je osrednja komponenta sistema, kar je razvidno iz Slike 23.

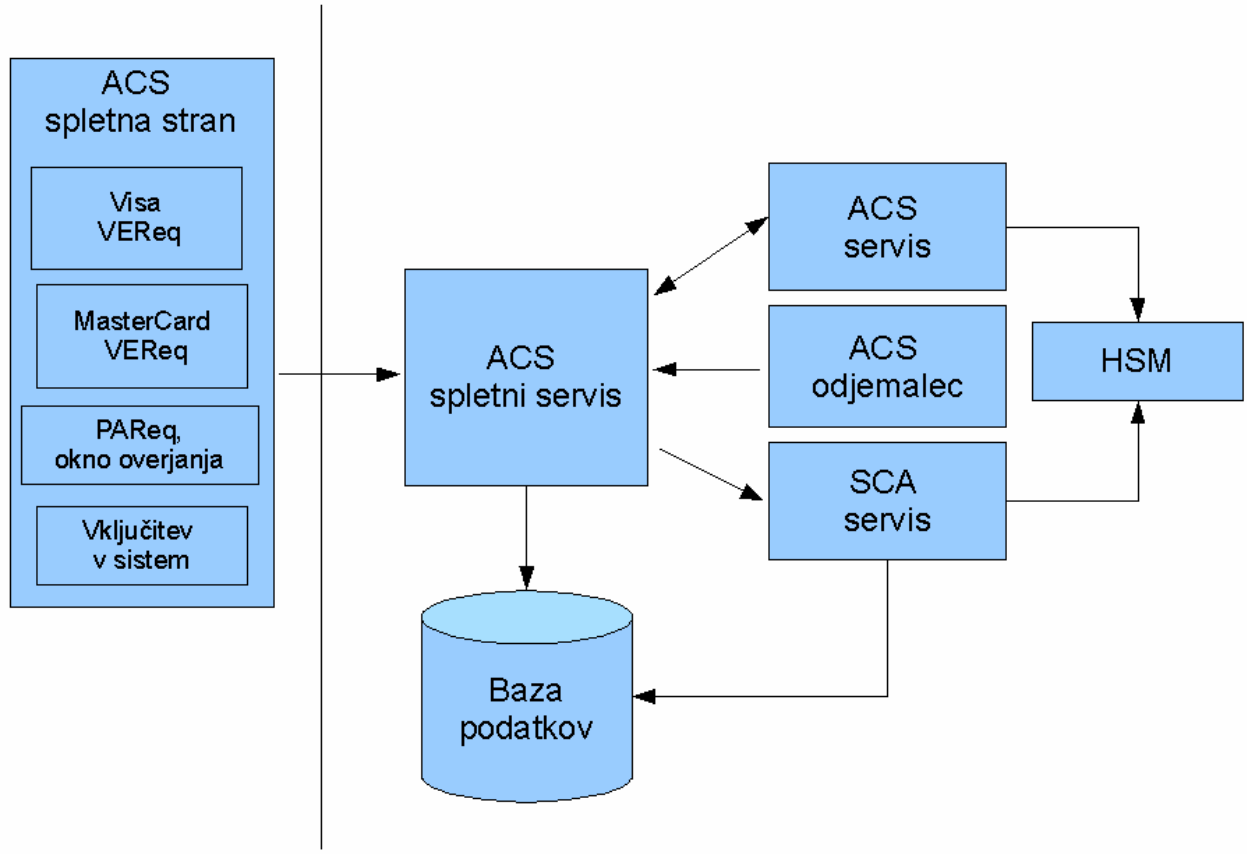
Metode spletnega servisa delimo na metode za prijavo v sistem, metode za izvedbo overjanja in odjemalčeve metode .

Metode prijave v sistem so:

- VerifyCVC – metoda preveri ali podani številki kartice ustreza CVC številka. Spletni servis prikliče funkcijo na SCA servisu, ki s pomočjo HSM naprave preveri ali CVC številka ustreza. Zaradi varnosti CVC številke niso shranjene v bazi podatkov;
- VerifyExpire – metoda s pomočjo baze podatkov kartic preveri ali podani številki kartice ustreza datum veljavnosti;
- VerifyPAN – metoda s pomočjo baze podatkov kartic preveri ali številka kartice obstaja in pregleda ali status kartice dovoljuje uporabo;

- AuthenticateSecureCode – metoda preveri ali enkratno geslo, ki ga je izdelala kartica, ustreza. Preverjanje se izvede v SCA servis komponenti, ki s pomočjo svoje baze podatkov in HSM naprave preveri geslo;
- UpdateCard – metoda omogoča upravljanje podatkov kartice;
- IsCardEnrolled – metoda vrne rezultat ali je podana kartica vključena v sistem;
- InsertCard – metoda doda kartico v sistem. Kartica je po uspešnem klicu metode prijavljena v sistem;
- GetCardData – metoda vrne podatke kartice.

***Slika 23: Umestitev ACS spletnega servisa v sistem***




*Vir: lasten.*

Metode izvedbe overjanja so:

- GetAllCerts - metoda vrne podatke certifikatov, ki se uporabljajo v sistemu. Metoda služi ACS servisu za začetno vzpostavitev certifikatov;
- GetAllUnSentPATransReq – metoda vrne vsa neodposlana PATransReq sporočila za zgodovinski strežnik. ACS servis je uporabnik te metode;
- PATransResProcess - metoda obdela PATransRes sporočilo in označi ustrezno PATransReq sporočilo kot poslano. ACS servis je uporabnik te metode;

- VEReqProcess – metoda obdela VEReq sporočilo. ACS spletna stran (Visa/MasterCard VEReq del) prikliče metodo po prejetju sporočila;
- PAReqProcess – metoda obdela PAReq sporočilo. ACS spletna stran (PAReq del) prikliče metodo po prejetju sporočila;
- Authenticate – metodo sproži ACS spletna stran po pritisku gumba ‘prijava' na oknu za overjanje;
- ProcessCancel - metodo sproži ACS spletna stran po pritisku gumba ‘prekliči’ na oknu za overjanje;

**ACS servis**

ACS servis je Windows Servis aplikacija, ki vzdržuje spomin (podatke prednaloži) in tako pospeši izvajanje določenih operacij.

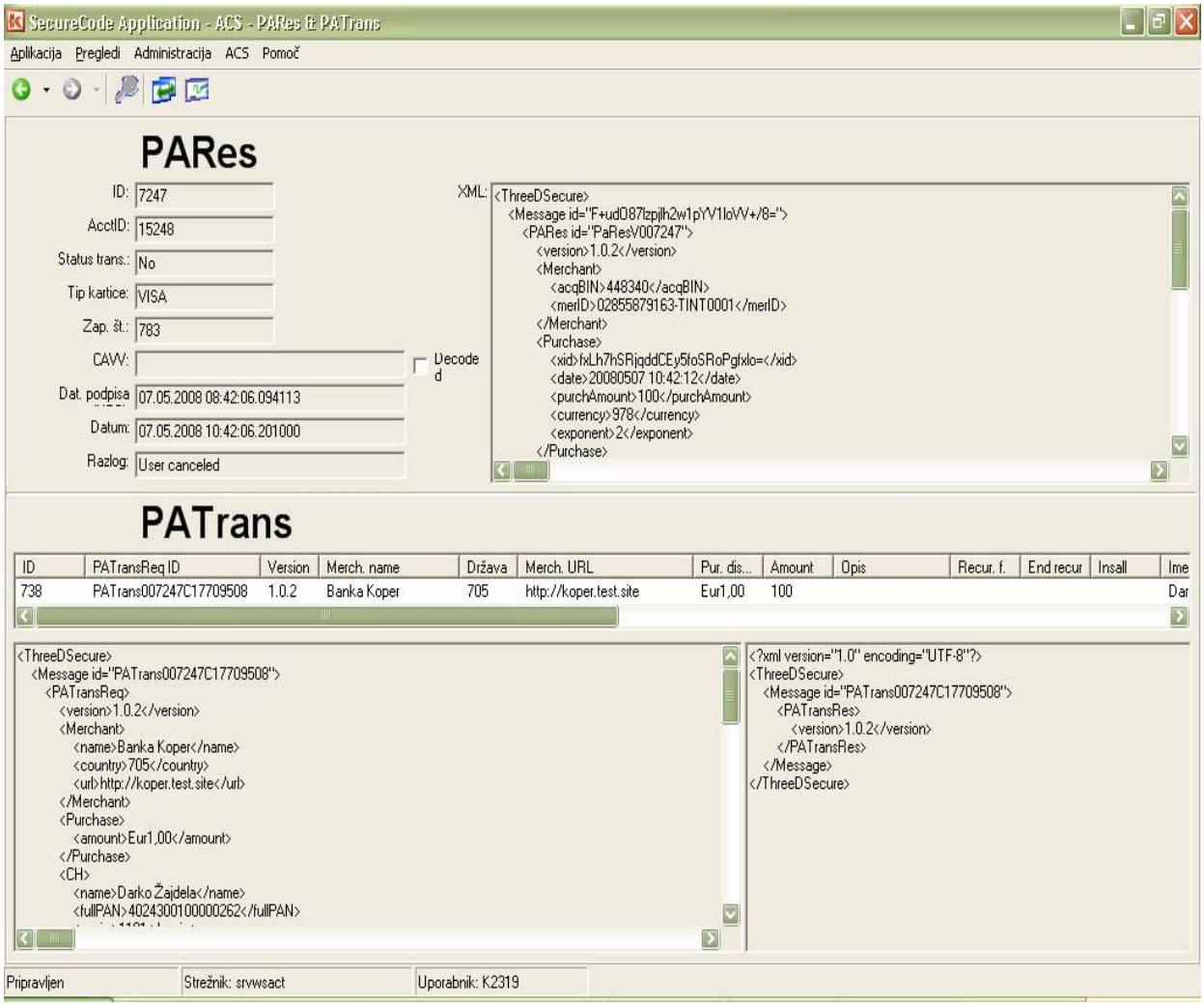
Servis digitalno podpisuje PARes sporočila. Ob zagonu servis prikliče metodo ACS spletnega servisa GetAllCerts, ki mu vrne podatke certifikatov. Za vsak certifikat naredi servis začetni dostop. Vsak nadaljnji dostop do certifikata pri digitalnem podpisovanju je tako znatno hitrejši. Privatni ključ digitalnega certifikata je shranjen v HSM napravi. Digitalni podpis dejansko naredi HSM naprava in ne ACS servis. Digitalno podpisovanje je v ločeni komponenti zaradi pohitritve podpisovanja.

Servis poleg digitalnega podpisovanja pošilja PATransReq sporočila na zgodovinski strežnik. ACS servis prikliče metodo ACS spletnega servisa GetAllUnSentPATransReq na vnaprej nastavljen interval in vsa prejeta sporočila pošlje na zgodovinski strežnik. Če zgodovinski strežnik uspešno prejme in obdela sporočilo, odgovori s PATransRes sporočilom, ki ga ACS servis le odda spletnem servisu v obdelavo (priklic metode PATransResProcess).

**ACS odjemalec**

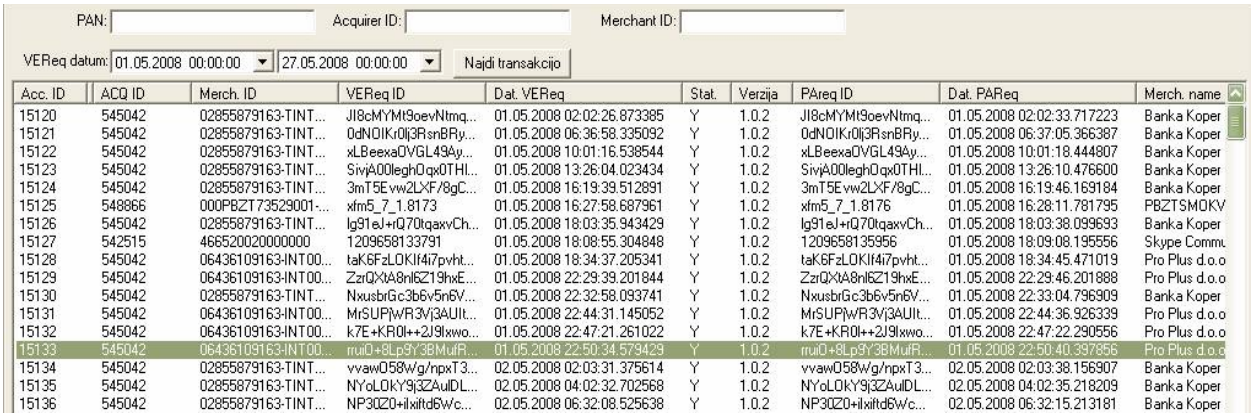
ACS odjemalec je namizna aplikacija, ki za prikaz podatkov uporablja metode odjemalca ACS spletnega servisa. Komponenta omogoča iskanje podatkov kartice, iskanje transakcije, iskanje napak in administracijo sistema (ročna deblokacija kartice, nastavitev delovanja, URL naslovi komponent, itd.). Preko uporabniškega vmesnika je možno natančno pregledati posamezna XML sporočila (Slika 24, Slika 25), status sporočila ter razlog napake obdelave sporočila. Uporabniški vmesnik ima tudi možnost izvajanja statistike uporabe ACS, kar služi za obračun stroškov uporabe ACS do partnerjev podjetja.

***Slika 24: Prikaz ACS odjemalca – podroben pregled sporočil***




*Vir: Interna gradiva podjetja, 2007.*

***Slika 25: Prikaz ACS odjemalca – pregled transakcij***




*Vir: Interna gradiva podjetja, 2007.*

**SCA servis**

SCA servis je neodvisna komponenta našega podjetja, ki služi upravljanju s ključi, shranjenimi v HSM napravi. ACS spletni servis uporablja SCA servis za izdelavo CAVV podatka, za overjanje CVC kode in enkratnega gesla, ki ju imetnik kartice vpiše v okno za overjanje. Avtorizacijski strežnik s pomočjo SCA servisa preveri podatek CAVV. SCA servis je torej naša izdajateljeva komponenta za overitev 3-D Secure podatkov v avtorizaciji transakcije.

### 4.4.3 Podatkovni model

Delovanje sistema je odvisno od tega, kako je oblikovana in kako se uporablja podatkovna baza. Bazo podatkov lahko pojmujemo kot enega osnovnih življenjskih virov sistema, ki mora biti oblikovana tako, da:

- omogoča hiter dostop do podatkov;
- vsebuje točne podatke brez preobilja podatkov oziroma odvečnih podvajanj;
- omogoča učinkovito delo;
- je prilagodljiva;
- zagotavlja varnost.

**Tabele 3-D Secure podatkovnega modela**

**1) ACS_CONFIG**

ACS_CONFIG je tabela za shranjevanje različnih nastavitev, kot so na primer teksti vseh spletnih oken, serijska številka certifikata za dostop do zgodovinskega strežnika, naslov zgodovinskega strežnika, itd.

**2) ACS_REJECTED**

ACS_REJECTED tabela se uporablja za shranjevanje zavrnjenih sporočil VEReq ali PAReq.

**3) ACS_ENROLL_TYPE**

ACS_ENROLL_TYPE je šifrant nastavitve tipa prijave v sistem. Poznamo dva tipa prijave:

- 1 – ročna prijava, ko se mora imetnik sam prijaviti v program preko ACS spletne strani;
- 2 – avtomatična prijava vseh kartic (odločitev vodstva je bila, da so vse Maestro kartice avtomatično prijavljene v program).

**4) ACS_AUTHPAGE**

ACS_AUTHPAGE je tabela nastavitve okna za overjanje. V tej tabeli je zapisana pot do logotipa MasterCard SecureCode in Verified By Visa programa.

### 5) ACS_BIN

ACS_BIN tabela se uporablja za nastavitev lastnosti rangov kartic. Preko tabele določimo katero overitveno okno se bo prikazalo imetniku kartice (ACS URL v VERes sporočilu), koliko krat lahko imetnik zgreši geslo, kateri ključ se uporablja za podpisovanje PARes, itd.

### 6) ACS_PARTNER

ACS_PARTNER je šifrant partnerjev našega podjetja, ki uporabljajo 3-D Secure sistem. V šifrantu nastavljamo podatke partnerja, ki se prikažejo na overitvenem oknu (na primer logotip partnerja).

### 7) ACS_GREETING

ACS_GREETING tabela je namenjena nastavljanju privzetega pozdravnega sporočila po partnerju v primeru avtomatične vključitve kartice v program.

### 8) ACS_TRANSACTION

ACS_TRANSACTION je tabela, v katero shranimo vse podatke sporočil VEReq in VERes.

### 9) ACS_PARES

V tabeli ACS_PARES se shranijo vsi podatki sporočila PARes, če je ta bil uspešno obdelan, ne glede na rezultat overjanja imetnika.

### 10) ACS_PARES_INVALID

Tabela ACS_PARES_INVALID vsebuje vsa neuspela sporočila PARes (zaradi napake obdelave PAReq sporočila).

### 11) ACS_PATRANS

Tabela se uporablja za pošiljanje sporočila PATransReq na zgodovinski strežnik.

## 4.5 Implementacija sistema

V četrti fazi življenjskega cikla razvoja sistema se izvede razvoj aplikacije oziroma programske opreme, njena namestitev in vrednotenje.

Razvoj 3-D Secure izdajateljevih komponent je potekal v dveh fazah. Prva faza je bila izgradnja ogrodja sistema, v kateri smo izdelali osnovne funkcije obdelave VEReq, PAReq, digitalno podpisovanje, preverjanje imetnika kartice. Druga faza izgradnje je potekala med samo overitvijo sistema. Preko 164 testov, ki jih je moral ACS opraviti, smo ugotovili pomanjkljivosti prve faze razvoja in te tudi odpravili. Po uspešni overitvi smo prejeli potrdilo za uporabo sistema v produkciji. Naročili smo vse potrebne produkcijske certifikate, nastavili smo produkcijske parametre aplikacije ter aplikacijo postavili v življenje.

# 5 ZAKLJUČEK

Cilj magistrskega dela je bil dosežen, saj sem kot vodja razvoja na projektu omogočil podporo 3-D Secure tehnologiji. Razviti sistem bomo v nadaljevanju poskušali posodobiti z večjezičnostjo, saj bomo v prihodnosti vključili tudi partnerje iz drugih držav.

V sistemu so v času pisanja magistrskega dela vključene vse Maestro kartice in nekaj sto MasterCard in Visa kartic. V nadaljevanju bomo tako kot smo to storili za vse Maestro kartice avtomatično vključili tudi vse MasterCard in Visa kartice. Na ta način si bomo kot izdajatelj kartic zagotovili največjo možno varnost opravljanja internetnih plačil s kartico.

Razvoj informacijskega sistema brez razumevanja problematike in cilja sistema ni možen, zato sem v magistrskem delu začel z uvrstitvijo elektronskih plačilnih sistemov v elektronsko poslovanje. Ugotovil sem, da imajo elektronski plačilni sistemi velik pomen, za nadaljnji razvoj elektronskega poslovanja. V elektronskem poslovanju se je pojavilo že veliko uspešnih in manj uspešnih oblik elektronskega plačevanja. Zakaj so nekateri sistemi ‘propadli’ ter zakaj prihajajo v uporabo podobni sistemi, sem ugotovil preko analize zahtev elektronskih plačilnih sistemov. Ugotovil sem, da ne obstaja najboljši elektronski plačilni sistem. Nekateri so primerni za določeno obliko elektronskega plačevanja, kot na primer PayPal-ov za poslovanje med posamezniki, drugi za mikroplačila, itd.

3-D Secure sistem je bil izdelan kot naslednik dveh bolj znanih elektronskih plačilnih sistemov SET in 3D-SET. Ugotovil sem razliko med sistemi ter zakaj naj bi 3-D Secure doživel večji uspeh od obeh predhodnikov. Končni uspeh 3-D Secure sistema je odvisen od sprejemanja uporabnikov. Dejavnike zaupanja uporabnikov sem zapisal v drugem poglavju magistrskega dela. V zadnjem poglavju sem obravnaval metodologijo, ki smo jo uporabili za razvoj 3-D Secure sistema. Opisal sem naš pristop z uporabo metodologije življenjskega cikla. Z raziskavo zakaj se elektronski plačilni sistemi nenehno razvijajo sem ugotovil, da je 3-D Secure sistem le eden od sistemov na poti do najboljšega elektronskega plačilnega sistema.

# LITERATURA IN VIRI


[1] Abrazhevich, D. (2004). *Electronic Payment Systems, A User-Centered Perspective and Interaction Design*. Eindhoven: Technische Universiteit.

[2] Activa. (2007). *Pametna kartica*. Najdeno 25. februarja 2008 na spletnem naslovu http://www.activa.si

[3] Avison, D. & Fitzgerald, G. (1996). *Information Systems Development - Methodologies, Techniques and Tools*. (2nd ed.) London: McGraw-Hill.

[4] Attridge, J. (2002). *An Overview of Hardware Security Modules*. B.k.: Sans Institute.

[5] Böhle, K. (2001). *Potential of Server-based Internet Payment Systems*. B.k.: European Institute for prospective technological Studies.

[6] Bračun, F. (2003). *Model dejavnikov zaupanja v plačevanje prek interneta*. Najdeno 25. februarja 2008 na spletnem naslovu http://ecenter.fov.uni-mb.si/Raziskovanje/Raziskave/e-placevanje.htm

[7] Centeno, C. (2002). *Securing Internet Payments – The potential of Public Key Cryptography*. b.k.: Institute for Prospective Technological Studies.

[8] Collin, B. (1998). *What happens if your partner turns against you?*. B.k.: Computer Security Institute.

[9] EPC. (2007). *SEPA online payment*. B.k.: European Payment Council.

[10] ECB. (2002). *E-payments in europe – the euro perspective*. B.k.. European Central Bank.

[11] *EuroPki organizacija*. Najdeno 25. februarja 2008 na spletnem naslovu http://www.europki.org.

[12] GPayments. (2001). *Authentication, the missing element in online payment security*. Warriewood.

[13] Gradišar, M. & Resinovič, G. (2001). *Informatika v poslovnem okolju*. Ljubljana: Ekonomska fakulteta.

[14] Hassler, V. (2001). *Security Fundamentals for E-Commerce*. Massachusetts: Artech House.

[15] Hendry, M. (1997). *Smart Card Security and Applications*. London: Artech House.

[16] Interna gradiva podjetja. (2007). *Dokumentacija ACS*.

[17] Jarupunphol, P. & Mitchell, C. J. (2003). *Measuring 3-D Secure and 3D Set against ecommerce end-user requirements*: London, University of London.

[18] Jerman Blažič, B. (2001). *Elektronsko poslovanje na internetu.* Ljubljana: Gospodarski vestnik.

[19] Kalakota, R. & Whinston, A. (1997). *Electronic commerce: a manager's guide*. B.k.: Addison Wesley.

[20] Laudon, K. & Traver, C. (2002). *E-commerce: business, technology, society*. London: Addison Wesley.
[21] MasterCard Int. (2004). *3-D Secure Member Enrollment and Implementation guide*. B.k.
[22] MasterCard Int. (2005a). *3-D Secure - Cardholder interface requirements*. B.k.
[23] MasterCard Int. (2005b). *SecureCode ACS Security Requirements*. B.k.
[24] Nyshadham, A. E. & Ugbaja M. (2006). *Study of Ecommerce Risk Perceptions among B2C Consumers: A Two Country Study*. Bled: Nova Southeastern University.
[25] O'Mahony, D., Peirce, M. & Tewari, H. (2001). *Electronice Payment Systems for E-Commerce.* (2nd ed.) London: Artech House.
[26] Oppliger, R. (2003). *Security Technologies for the World Wide Web.* (2nd ed.) London: Artech House.
[27] Pipan, M. (2002). *Diplomsko del, Elektronski plačilni sistemi na internetu*. Ljubljana: Ekonomska fakulteta.
[28] Puhrerfellner, M. (2000). *An implementation of the Millicent micro-payment protocol and its application in a pay-per-view business model*. Dunaj: Technical University.
[29] Robinson, P. (2001). *Understanding Digital Certificates and Secure Sockets Layer (SSL)*. B.k.: Entrust Inc.
[30] *SEPA Slovenija.* (2008). Najdeno 25. februarja 2008 na spletnem naslovu http://www.sepa.si.
[31] Shelly, G. B., Cashman, T. J. & Rosenblatt, H. J. (2001). *Systems Analysis and Design.* (4th ed.) Cambridge: Thomas Publishing.
[32] Skrt R. (2002). *Varno nakupovanje v spletnih trgovinah*. Najdeno 25. februarja 2008 na spletnem naslov http://www.nasvet.com/varnost-nakupovanje/.
[33] Stephen, T. A. (2000). *SSL & TLS Essentials Securing the Web*. B.k.: John Willey & Sons.
[34] Šepetavc P. (2007). *PayPal – varen način spletnega plačevanja*. Najdeno 25. februarja 2008 na spletnem naslov http://www.mladina.si/tednik/200752/clanek/nar--nove_tehnologije-peter_sepetavc/.
[35] Fischer, M. (2002). *Towards a Generalized Payment Model for Internet Services*. Dunaj: Technical University.
[36] Visa Int. (2004a). *3-D Secure Functional Requirements, Access Control Server*. B.k.
[37] Visa Int. (2004b). *3-D Secure Protocol Specifications, Core Functions*. B.k.
[38] Visa Int. (2001a). *3-D Secure Functional Specifications., Chip Card Authentication*. B.k.
[39] Visa Int. (2001b). *3-D Secure Service Specifications, Authentication History Service*. B.k.
[40] Visa Int. (2001c). *3-D Secure Implementation Guide*. B.k.
[41] Visa Int. (2001d). *3-D Secure Security Requirements, Enrollment and Access Control Servers*. B.k.
[42] Visa Int. (2006a). *Verified by Visa Introduction*. B.k.

[43] Visa Int. (2006b) *Verified by Visa System Overview External version 1.0.2*. B.k.
[44] Wayner, P. (1997) *Digital Cash: Commerce on the Net*. B.k.: Academic Press.
[45] Wikipedia. (2008a). *Http.* Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/HTTP.
[46] Wikipedia. (2008b). *Firewall*. Najdeno 25. februarja 2008 na spletnem naslovu http://en.wikipedia.org/wiki/Firewall_(networking).
[47] Wikipedia. (2008c). *Spletni brskalnik*. Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/Brskalnik.
[48] Wikipedia. (2008d). *Web servis*. Najdeno 25. februarja 2008 na spletnem naslovu http://en.wikipedia.org/wiki/Web_service.
[49] Wikipedia. (2008e). *TCP/IP*. Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/TCP
[50] Wikipedia. (2008f). *Zahteva za mnenja*. Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/Zahteva_po_razlagi.
[51] Wikipedia. (2008g). *JavaScript*. Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/JavaScript.
[52] Wikipedia. (2008h). *XML*. Najdeno 25. februarja 2008 na spletnem naslovu http://sl.wikipedia.org/wiki/XML.
[53] ZBS (Združenje bank Slovenije). (2007). *Online plačila – nacionalna obravnava*, Ljubljana.