UNIVERZA V LJUBLJANI
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Matija Novak

SET - Secure Electronic Transactions

SEMINARSKA NALOGA PRI PREDMETU
KRIPTOGRAFIJA IN TEORIJA KODIRANJA 2

Mentor: prof. dr. Aleksandar Jurišič

Ljubljana, 2011

Kazalo

1 Uvod

Izmenjava dobrin je v zgodovini človeštva vedno igrala zelo pomembno vlogo. Z razvojem je trgovanje postajalo čedalje bolj kompleksno, tako da si je bil človek primoran izmišljevati vse bolj abstraktne predstavitve vrednosti. Surovine je tako zamenjal denar, pojavili so se čeki in ostali vrednostni papirji. Ti tradicionalni načini oblike plačevanja pa imajo številne pomankljivosti - denar lahko ponaredimo, podpis na papirju prav tako, čeki so lahko brez kritja. Razvoj informacijskih in komunikacijskih tehnologij je prinesel internet in kmalu se je uveljavil izraz elektronski denar, ki je v poslovanje prinesel še dodatno fleksibilnost. Elektronski denar pa sam po sebi ne prinaša rešitev za probleme, za katerimi trpi poslovanje s klasičnimi oblikami plačila, vendar pa lahko varnost in integriteto finančnih transakcij zagotovimo z dobro zasnovanim sistemom. Sistem mora upoštevatii vse sodelujoče v transakciji: kupca, prodajalca in banko.

Electronic Transactions (SET) ni sistem plačevanja, pač pa skupek protokolov, ki zagotavljajo varnost finančnih transakcij preko interneta. Specifikacija je začela nastajati leta 1996 kot skupen projekt dveh tedaj največjih izdajateljev kreditnih kartic. Razlog za skupen pristop je bila zahteva bank po standardizaciji finančnih transakcij. Do tedaj sta namreč tako MasterCard (v sodelovanju z Netscape-om in IBM-om) kot Visa (s podporo Microsofta) razvila svoje sisteme (Secure Electronic Payment Protocol in Secure Transaction Technology), vendar sta bila le-ta med seboj nekompatibilna. Čeprav so glavni akterji na obeh straneh zagotavljali odprtokodnost, bi standardizacija zahtevala implementacijo zunaj obeh sistemov, kar pa ne pomeni nič drugega kot samo še en sistem, ki bi deloval nad obema (in morda še katerim drugim). Ker bi vse skupaj s to rešitvijo postalo samo še bolj kompleksno, se je veliko bolj smiselen zdel skupen pristop obeh podjetji, katerima so se pridružili še nektareri veliki igralci iz sveta informacijskih tehnologij (IBM, GTE, Microsoft, RSA, VeriSign, Netscape, ...). Prva verzija je ugledala luč sveta v prvi polovici leta 1997, že naslednje leto pa so bile lansirane prve storitve. Želja vseh, ki so sodelovali pri projektu, da bi SET postal de-facto standard za plačevanje s kreditnimi karticami, pa se kljub veličini sistema ni uresničila.

Kljub temu, da je bil SET zasnovan konec devedesetih let prejšnjega stoletja, le-ta še vedno velja za zgled sistemom, ki operirajo z občutljivimi finančnimi podatki. Dejstvo je, da so bili principi javne kriptografije znani že veliko pred tem, potrebna je bile le smiselna, predvsem pa učinkovita implementacija. Finančne transakcije seveda zahtevajo nekatere specifične lastnosti, tako da je SET predstavil tudi nekaj novosti v svetu kriptografije. Pri opisu

principov in delovanja protokolov v SET sistemu se bom zato osredutočil prav na kriptografske elemente, ki so v prvi vrsti omogočili varno implementacijo poslovnih zahtev.

2 Motivacija

2.1 Elektronsko poslovanje

Elektronsko poslovanje si lahko razlagamo na več nacinov, odvisno iz katere perspektive gledamo na sam proces poslovanja. Vseeno so vsem razlagam skupni elementi trgovanja storitev in produktov preko elektronskih sistemov, kot so računalniške mreže. Z razvojem interneta se je delež poslov, ki se izvršijo po elektronski poti, drastično povečal. Internet pa je poleg možnosti poceni in učinkovitega poslovanja prinsel nove načine zlonamernega okoriščanja, zato je bistveno, da je elektronsko poslovanje implementirano varno in korektno.

Da bi bili uporabniki elektronskih sistemov v odprtih mrežah varni pred vdori tretjih oseb, so se skupaj z elektronskim poslovanjem pojavile ideje o tako imenovanih e-commerce protokolih. Zaradi kompleksnosti so taki protokoli velikokrat vsebovali napake, zato so le steža konkurirali kriptografskim protokolom, ki so delovali na transportni plasti med dvema točkama v odprti računalniški mreži. Seveda taki protokoli nisto specializirani za procesiranje finančnih transakcij niti ne zagotavljajo nikakršnih poslovnih zahtev, tako da ideja o sufisticiranem sistemu za upravljanje finančnih transakcij med velikimi kooporacijami nikoli ni zamrla. Znanje, potrebno za implementacijo takega sistema, je bilo na voljo že veliko pred prvimi poskusi e-commerce protokolov, vprašljiva je bila le prijaznost sistema do uporabnika.

2.2 Kakšen sistem potrebujemo

V procesu finančne transakcije sodeluje več tipov entitet, vsaka izmed njih pa ima svoje specifične zahteve. Vsem skupna in hkrati tudi najpomembnejša zahteva pri načrtovanju primernega protokola oziroma sistema le-teh je zagotovo varnost. V splošnem lahko zahtevo po varnosti razdelimo na naslednje podzahteve:

- Zaupnost informacije o naročilu in informacije o plačilu: Imetniku kreditne kartice moramo zagotoviti, da so vse informacije varne pred zunanjim svetom in dosegljive le tistim, ki jih določena informacija dejansko zadeva. Tako naj bo informacija o naročilu vidna le trgovcu, informacija

o plačilu pa le banki, ki izvrši transakcijo. Z izpolnitvijo te zahteve se zmanjša možnost goljufije tako s strani zlonamernega prodajalca kot s strani tretje osebe. SET zagotavlja varnost s kriptiranjem vseh sporočil, ki se pošiljajo od ene entitete do druge.

- Integriteta podatkov: Podatki, ki jih imetnik kreditne kartice pošlje prodajalcu, vsebujejo informacijo o naročilu, osebne podatke in informacijo o plačilu. Če je katerakoli komponenta med postopkom spremenjena, transakcija ne more biti uspešno izvedena. Kakršnakoli možnost spreminjanja podatkov je potencialna priložnost za prevare in napake. Sistem mora torej zagotavljati, da se podatki na cilju ujemajo s podatki, ki so bili poslani s strani uporabnika sistema. Integriteta podatkov je v SET sistemu zagotovljena z digitalnim podpisovanjem, kar omogočajo principi javne kriptografije in uporaba zgoščevalnih algoritmov.

- Avtentikacija imetnika kreditne kartice: Sistem mora vsebovati učinkovit mehanizem, ki povezuje imetnika kreditne kartice z veljavnim bančnim računom. Tak mehanizem prepreči nekatere vrste prevar, hkrati pa potencialna učinkovitost tudi zmanjša ceno celotne transakcije.

- Avtentikacija prodajalca: Lastnik kreditne kartice mora imeti možnost identificirati prodajalca in pridobiti zagotovilo, da prodajalec lahko preko povezav s finančnimi institucijami sprejema finančne transakcije. Avtentikacija je v SET zagotovljena z digitalnimi podpisi in certifikati.

Za zagotovitev zgoraj naštetih zahtev je zaželjeno, da uporabimo že preverjene principe in postopke. Hkrati moramo v račun vzeti tudi že obstoječe principe, saj bo lahko le na ta način sistem standardiziran. Dodamo torej še naslednje zahteve:

- Za zagotovitev varnosti vsem vpletenih stranem uporabimo najboljše varnostne prakse, tehnike in specifikacije, ki so v danem trenutku na voljo. To vključuje varne kriptografske algoritme, protokole in infrastrukturo.

- Sistem ne sme biti odvisen od varnostnih mehanizmov in protokolv, ki delujejo na transportni plasti (od točke do točke), niti ne sme onemogočati uporabe le-teh. SET se sicer poslužuje svojih varnostnih mehanizmov, ki so neodvisni od varnostnih protokolov na transportni plasti. Uporaba le teh sicer ni nujna, je pa zaželjena kjer je to možno, saj dodaten varnostni ovoj lahko kvečjemu koristi.

- Sistem naj bo neodvisen od strojnih in programskih platform, kar omogoča maksimalno razpoložljivost sistema. SET deluje tako na osebnih računalnikih kot na platformah, na katerih delujejo sistemi ki operirajo s finančnimi transakcijami.

Za sistem, ki zadostuje vsem zgoraj naštetim zahtevam, lahko rečemo, da je varen za vse entitete, ki jih sistem zadeva. Poleg varnosti dobimo še povsem neodvisen sistem, ki bi bil primeren za zelo široko uporabo. Ko govorimo o finančnih transakcijah sta pa prav varnost in preprosta uporaba tisto, kar iščemo.

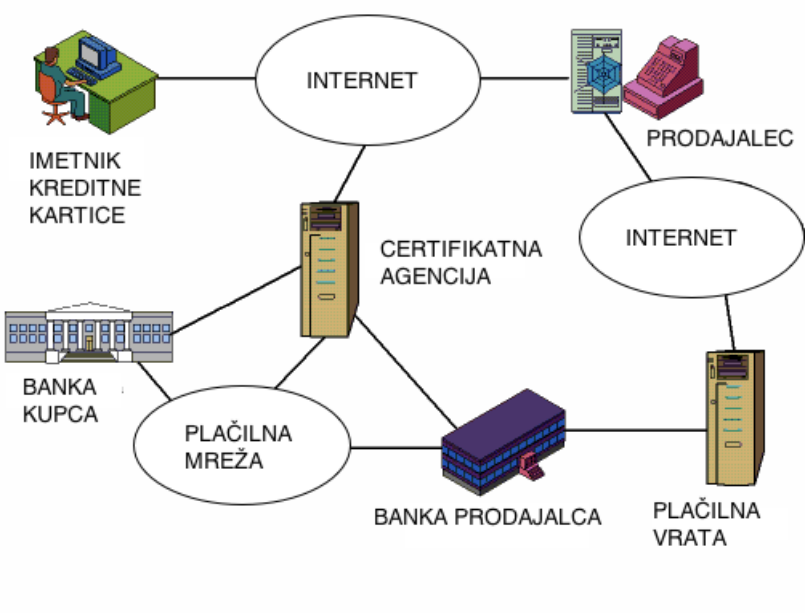
2.3 Zakaj SSL ni dovolj?

Pionirji poslovanja preko interneta se niso ukvarjali z učinkovitostjo poslovanja v smislu hitrosti, enostavnosti samega postopka in ekonomičnosti, pač pa predvsem s skrivanjem podatkov pred zunanjim svetom. Imetniki kreditnih kartic paso imeli zaradi nagle rasti in dostopnosti internate povsem utemeljene pomisleke glede pošiljanja številke kreditne kartice prodajalcu preko odprtih mrež.

SSL (Secure Socket Layer) je kriptografski protokol, ki zagotavlja varno komunikacijo preko interneta. SSL vzpostavi kriptirano povezavo med odejmalcem in strežnikom ter s tem zagotavlja varno komunikacijo, hkrati pa poskrbi še za integriteto poslanih podatkov ter avtentikacijo. Da to doseže, se poslužuje tehnik asimetrične in simetrične kriptografije. Tehnologija javnih ključev avtenticira entiteti na obeh straneh varne povezave in poskrbi za varno izmenjavo simetričnega ključa, s katerim je kriptirana poslana informacija.

Integriteta podatkov je zagotovljena z uporabo zgoščevalnih algoritmov, s pomočjo katerih lahko za poslane podatke izračunamo izvleček. Ta izvleček je še pred enkripcijo dodan podatkom in skupaj z njimi poslan naslovniku. Nasovnik na drugi strani za podatke izračuna svoj izvleček ter ga primerja s tistim, ki ga je dobil polega podatkov. Če med prenosom poslane podatke prestreže tretja oseba in le-te spremeni, bo naslovnik izračunal drugačen izvleček in s tem bo tudi vedel, da so bili podatki med prenosom spremenjeni.

Čeprav protokol ni specializiran za finančne transakcije, pa ponuja rešitev za kar nekaj zahtev iz prejšnjega poglavja. Kar se tiče pošiljanja informacij o naročilu in plačilu do prodajalca, SSL v resnici velja za standard, saj so podatki varni pred zunanjimi osebami. Vendar pa SSL ne nudi nobenega mehanizma, ki bi kupca branil pred zlonamernim prodajalcem. S tem, ko ima prodajalec številko kreditne kartice, obstaja možnost, da jo zlorabi. Velja tudi obratno - prodajalec ni varen pred zlonamernim kupcem. Ker SSL deluje



Slika 1: SET entitete in povezave med njimi.

na transportni plasti od ene točke do druge, so na vsakem koncu potrebni še dodatni mehanizmi, ki bi finančno transakcijo dejansko izvedli. Prav omenjeni problemi so dovolj velik razlog za razvoj sistema, ki bi bil specializiran izključno za finančne transakcije preko interneta.

3 Entitete

Poglejmo si za začetek entitete, ki nastopajo v SET sistemu. Za razliko od direktnih transakcij, kjer se proces začne pri prodajalcu, v SET transakciji proces začne **imetnik kreditne kartice**. Imetnik kreditne kartice pri procesu sodeluje preko osebnega računalnika, ki je priklopljen na internet. Kreditna kartica je last **finančne institucije** oziroma banke, uporabnik pa jo pridobi z odprtjem računa pri le tej. S tem postane tudi avtoriziran uporabnik kartice, kar mu daje pooblastila za uporabo. Z izdajo kreditne kartice banka uporabniku med drugim zagotovi tudi varno plačevanje.

Prodajalec je oseba ali organizacija, ki ponuja storitve ali produkte. Ker govorimo o elektronski transakcijah, prodajalci svoje storitve tržijo na internetu ali pa celo preko elektronske pošte. Da lahko prodajalec sprejema kreditne

kartice svojih strank, mora imeti odprt račun pri finančni instituciji oziroma banki, ki lahko zagotavlja izvrševanje avtorizacije kreditnih kartic in plačil. Z avtorizacijo dobi prodajalec podatek o tem, ali je kartica veljavna oziroma aktivna, pa tudi če ima kritje za trenutno naročilo. Če je vse vredu, banka poskrbi tudi za nakazilo denarja iz računa kupca na prodajalčev račun. To stori preko plačilnega sistema med bankami, ki je neodvisen od SET sistema.

Med prodajalcem in banko so ponavadi **plačilna vrata**, ki za banko opravijo avtorizacijo in zajetje plačila. Na ta način lahko banka te naloge zaupata tudi kaki drugi finančni instituciji, ki podpira več znamk kreditnih kartic. Finančna vrata po potrebi tudi formatirajo SET sporočila v format, ki se ujemajo s prodajalčevim sistemom trgovanja. Ker integriteta podatkov velja med dvema sosednjima entitetama v SET sistemu, tako formatiranje nima vpliva na rezultat preverjanja integritete in je celo zaželjeno povsod tam, kjer pozitivno vpliva na učinkovitost celotnega sistema.

Za izdajo digitalnih potrdil lastnikom kartic, prodajalcem in plačilnim vratom poskrbi **certifikatna agencija**. Prav od certifikatne agencije in celotne infrastrukture grajene okoli ene oziroma več certifikatnih agencij je odvisen uspeh SET sistema. Glavna naloga agencije je sprejemanje registracijskih zahtev, obdelava le-teh in izdajanje digitalnih potrdil. Prav ta pa vsebujejo vso potrebno informacijo, s katero se lahko preveri veljavnost in izvor le tega, s tem pa tudi vzpostavi zaupanje v imetnika potrdila.

4 Kriptografski principi v SET

Kriptografija v splošnem poskrbi za kriptiranje in dekriptiraje informacij. V najbolj enostavnem primeru pošiljatelj na sporočilu izvede neko funkcijo, pošlje sporočilo naslovniku, ta pa originalno informacijo pridobi z inverzno funkcijo. S tem je bila informacija sktita pred zunanjim svetom. Seveda se v praksi uporabljajo bolj kompleksni pristopi, še posebaj velja to za občutljive informacije, kar finančne prav gotovo so. Bolj kompleksne sheme praviloma pomenijo tudi večjo varnost, zato specifikacije SET protokolov predvidevajo že preverjene pristope, zaradi specifičnosti nekaterih poslovnih zahtev pa vpeljejo tudi novosti.

4.1 Simetrična kriptografija

Simetrična kriptografija za kriptiranje in dekriptiranje uporablja en sam ključ, ki je znan naslovniku pošiljatelju, zunanjemu svetu pa mora ostati skrit. Simetrija sheme zahteva, da je transformacija kriptiranja inverzna transformaciji

dekriptiranja. Eden standardnov simtrične kriptografije je DES (Data Encription Standard), ki se uporablja tudi v SET sistemu. DES uporablja premikanje bitov v obe smeri, kar je časovno nezahtevna operacija in je zato celoten proces hiter, poleg tega se pa da premikanje bitov zelo učinkovito implementirati na strojnem nivoju. Kljub temu je DES sam po sebi neuporaben v sistemu, kjer so zaradi narave informacij potrebni bolj specifični prijemi. Povedali smo že, da sta eni ključnih zadev avtentikacija in integriteta podatkov, katerih en sam kriptografski algoritem, kot je DES, niti slučajno ne more zagotoviti. Dodatne težave nastopijo tudi pri distribuciji ključev, kar je v SET sistemu tudi ključno opravilo. Ker lahko le dve entiteti delita enak ključ in ker število entitet v SET sistemu zelo hitro narašca, tudi število potrebnih ključev raste eksponentno. Poleg tega je potrebno zaradi varnosti ključe menjati kar se da pogosto, kar samo še poslabša zahtevnost. Nastali problem s ključi lahko rešimo na veliko bolj eleganten način, to je z uporabo kombinacije principov simetrične kriptografije in principov asminetrične kriptografije. Rešitev, ki se poslužuje algoritmov DES in RSA (asimetrični principi), si bomo pogledali nekoliko kasneje v poglavju o digitalnih ovojnicah.

4.2 Asimetrična kriptografija in RSA-OAEP shema

V času nastajanja SET specifikacij so bili principi asimetrične kriptografije že davno znani in preverjeni. Začetki javne kriptografije, kakor tudi rečemo asimetričnim principom kriptografije, segajo v leto 1976, ko sta Diffie in Hellman predstavila prvo shemo, ki temelji na faktorizaciji velikih praštevil. Kriptiranje in dekriptiranje v tem primeru vključuje dva ključa, privatnega, ki je znan samo pripadajoči entiteti, in javni ključ, ki je objavljen javno in tako znan vsem entitetam v sistemu. Podatke, ki so kriptirani z javnim ključem, je moč dekriptirati samo z pripadajočim privatnik ključem. Poleg samega kriptiranje sta Diffie in Hellman predstavila učinkovit način izmenjave ključev, s katerim se lahko dve entiteti z javnima ključema dogovorita za skrivni ključ, ki se v trenutni seji uporabi pri prenosu podatkov. Če zadevo poenostavimo, lahko implementacijo dogovora o ključu razdelimo v dve fazi. V prvi fazi pošiljatelj pošlje sporočilo prejemniku, s katerim začne protokol dogovarjanja o ključu. Tako pošiljatelj kot prejemnik v prvi fazi neodvisno zaženete nek algoritem (v splošnem poljuben, seveda pa je zaželjeno da ustreza določenim zahtevam) ter si izmenjata rezultat. V drugi fazi oba vpletena ponovno neodvisno po algoritmu izračunata skupen ključ. Vsekakor nekaj, kar SET sistem nujno potrebuje, vendar tak način generiranja ključev ne pride v poštev. Zaradi količine potrebnih ključev bi sistem deloval prepočasi. Že omenjena rešitev, digitalna

ovojnica, pa vseeno potrebuje asimetrični princip. Potreben element se skriva v algoritmu RSA (Rivest, Shamir, Adleman). Ta se uporablja tako za kriptiranje kot za digitalno podpisovanje, kar v polni meri izkorišča tudi SET. Shema, ki je uporabljena v SET sistemu, se imenuje RSA-OAEP. Ta združuje RSA algoritem s kodirno shemo OAEP (Optimal asymmetric encryption padding), ki sta jo predstavila Mihir Bellarein in Phillip Rogaway leta 1994.

RSA

Varnost algoritma RSA temelji na faktorizaciji velikh števil. V podrobnsti ozdaja se v tem seminarju ne bomo spuščali, bomo pa predstavili shemo RSA operacij, saj bo na ta način bralec lažje doumel pomen kriptografskih elementov v SET sistemu. RSA uporablja par ključev, privatnega, ki je znan samo lastniku, ter javnega, ki je znan vsem. Sporočilo je vedno kriptirano z javnim ključem, dekriptirano pa s privatnim ključem. Par takih ključev generiramo na nasledji način:

1. Izberi dve različni veliki prašteili p in q. Števili morata biti zaradi varnostnih razlogov izbrani naključno.
2. Izračunaj število $n = pq$.
3. Izračunaj $\phi(n) = (p-1)(q-1)$ (Eulerjeva funkcija).
4. Izberi število e, ki je večje od 1 in manjše od $\phi(n)$ ter tuje s številom $\phi(n)$. Število e se skupaj s številom n uporablja kot javni ključ.
5. Izračunaj število $d = e^{-1} \pmod{\phi(n)}$, ki se uporablja kot privatni ključ. Pri izračunu števila d si največkar pomagamo z razširejnim Evklidovim algoritmom.

Ko imamo generiran par ključev, javni del pošljemo osebi, ki nam bo poslala kriptirano sporočilo. V večini sistemov, tudi v SET, je to rešeno z digitalnim certifikatom, v katerega je vključen tudi javni ključ. Pošiljatelj bo sedaj sporočilo, ki ga želi poslati"pretvoril v število m ter ga kriptiral na naslednji način:

1. Če velja $m < 0$ ali $m > n - 1$, m zavrni.
2. Izračunaj število $c = m^e \pmod{n}$.

Ko prejmemo kriptogram, le tega enostavno dekriptiramo s svojim privatnim ključem:

1. Če velja $c < 0$ ali $c > n - 1$, c zavrni
2. Izračunaj število $m = c^d \pmod{n}$

RSA ima lastnost, da je produkt dveh kriptogramov enak enkripciji produktu pripadajočih čistopisov ($m_1^e m_2^e \equiv (m_1 m_2 \pmod{n})$), kar omogoča napad z izbranim kriptogramom. Napadalec, ki želi dekriptirati kriptogram $c = m^e \pmod{n}$, lahko prosi imetnika privatnega ključa, da odkodira kriptogram $c' = cr^e \pmod{n}$ za poljubno vrednost r. Zaradi multiplikativne lastnosti je c' kar enkripcija števila $mr \pmod{n}$. V primeru, da je napadalec uspešen in pridobi število $mr \pmod{n}$, lahko izračuna čisopis m tako, da pomnoži mr z inverzom števila $r \pmod{n}$.

Še ena slabost čiste RSA sheme se skriva v dejsvu, da ne vključuje elementa naključnosti. Napadalec lahko izvede napad z izbranim čitopisom tako, da generirane čistopise, jih kodira z javnim ključem in primerja s kriptogramom, ki ga želi dekriptirati. V primeru, da mu uspe najti ustrezen čistopis, je lahko prepričan, da je ravno ta tisti, ki ga išče. Z drugimi besedami, RSA ni semantično varen. Pri semantično varnih kriptosistemih napadalec namreč ne more ločiti dveh kriptogramov pa čeprav pozna oba pripadajoča čistopisa.

Omenjene slabosti lahko odpravimo z uporabo randomiziranih "padding" shem. Le te v čistopise dopolnijo do neke izbrane dolžine, kar preprečuje, da bi čistopis padel v množico "nevarni" čistopisov. Ena takih shem je OAEP, ki se uporablja tudi v SET sistemu. Kot bomo videli kasneje, SET protokoli koristijo RSA algoritem pri pošiljanju naključno generiranih simetričnih ključev (digitalne ovojnice). Gledana s stališča besedila, so ključi kratki, kar pravzaprav pomeni "nevaren" čistopis. Če v RSA ključih uporabljamo še majhna števila, je nevarnost uspešnega napada še toliko večja.

OAEP (Optimal asymmetric encryption padding)

Namen razširitvenih shem je priprava sporočil pred kriptiranjem. V splošnem razširitev pomeni dodajanje naključnih podatkov sporočilu, tako da ta bo njegova dolžina zadostovala predpisanemu vhodu v kriptosistem. Seveda samo dodajanje naključnih podatkov ne zagotavlja, da napadalec ne bo mogel manipulirati s čistopisi in s tem razkrivati matematičnih lastnosti enkripcijske sheme. Shema OAEP se zato obnaša kot nekakšna oblika Feistlove mreže, ki preko naključnega generatorja procesira sporočilo, ki je potem kot vhod podan operaciji asimetričnemega kriptiranja. Z vpeljavo naključnosti v RSA se tudi njegova shema iz deterministične spremeni v verjetnostno. OAEP je v kombinaciji z RSA (v splošnem pa s katerokoli funkcijo, katere inverz je

težko izračunati) je semantično varen pred napadom z izbranim čistopisom. Lastnost, ki onemogoča dekriptiranje kateregakoli delčka čistopisa brez da bi poznal inverzno funkcijo enkripcijskega algorima RSA, preprečuje tudi parcialno dekriptiranje kriptograma (napad z izbranim kriptogramom).

OAEP shema potrebuje za svoje procesiranje zgoščevalno funkcijo H, ki je lahko poljubna, in funkcijo, ki generira masko. Ker OAEP operira z nizi, ki jih sestavljajo okteti (informacija sestavljena iz 8 bitov), RSA pa operira s števili, si najprej poglejmo konverzijo števil v nize oktetov in obratno. Na vhod podamo število x, na izhodu pa želimo niz dolžine l oktetov:

1. Če velja $x \geq 256^l$, zavrni vhod
2. Zapiši število x v unikatno l-mestno predstavitev nad bazo 256:

   $$x = x_{l-1}256^1 + \ldots + x_1256 + x_0$$

3. Vrni niz oktetov $X = X_1 \ldots X_l$, kjer je X_i oktet s stevilčno vrednostjo x_{l-i} za vsak $1 \leq i \leq l$

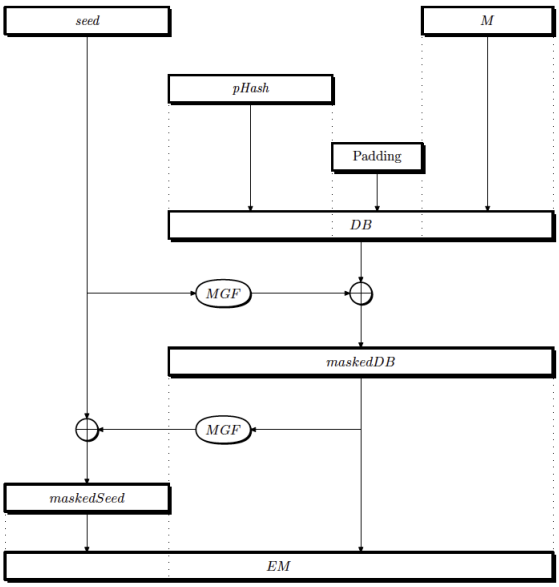
Konverzija niza oktetov v število je inverzna prejšnje operacije:

1. Naj bo $X = X_1 \ldots X_l$ niz oktetov in naj bo x_{l-i} stevilčna vrednost okteta X_i za $1 \leq i \leq l$
2. Vrni $x = x_{l-1}256^{l-1} + \ldots + x_1256 + x_0$

Sedaj si lahko pogledamo funkcijo, ki generira masko. Ta za vhod vzame niz oktetov spremenljive dolžine, željeno dolžino izhodenga niza (število oktetkov) ter naključno generiran niz oktetov, ki služi kot seme. Oba, tako vhodni kot izhodni niz, sta poljubne velikosti, praviloma pa sta zelo dolga. Generiranje maske je deterministična funkcija, torej je izhod popolnoma odvisen od vhoda, izhod pa je psevdonaključen, kar pomeni, da iz enega dela izhodnega niza ne moremo napovedati ostanek brez da bi poznali celotni vhodni niz. Koraki funkcije si sledjio takole:

1. Naj bo l število oktetov v maski in l_H število oktetov v nizu izhoda zgoščevalne funkcije H. Če velja $l > 2^{32}l_H$ vrni napako (maska predolga)
2. Naj bo T prazen niz oktetkov
3. Za vsak $i = 0...\lceil \frac{l}{l_H} \rceil$:

   Pretvori i v niz oktetov C dolžine 4 (uporabi funkcijo za pretvorbo števila v niz oktetov)



Slika 2: OAEP kodiranje: MGF - generator maske

Zlepi niz T z izvlečkom zlepka vhodnega semena Z in niza C: $T = T||H(Z||C)$

4. Vrni vodilnih l oktetov niza T

Zgoščevalna funkcija in funkcija, ki generira masko, sta v OAEP shemi parametrizirani, zato ju podamo na vhod kodiranja oziroma dekodiranja. Opcijsko lahko na vhod kodiranja podamo tudi kodirne parametre P (niz oktetov), ki pa jih lahko v tem trenutku brez izgube splošnosti izpustimo (niz parametrov bo prazen). Poglejmo si, kako OAEP kodirni algoritem procesira vhodno sporočilo M:

1. Naj bo l_H dolžina izhoda zgoščevalne funkcije v oktetih ($2^{61} - 1$ oktetov v primeru algoritma SHA-1). Če je dolžina parametrov P večja od l_H, zavrni P

2. Naj bo l_M dolžina sporočila M v oktetih in l_{EM} dolžina izhoda algoritma OAEP v oktetih. Če velja $l_M > l_{EM} - 2l_H - 1$, zavrni M (predolgo sporočilo)

3. Generiraj niz oktetov PS, sestavljen iz $l_{EM} - l_M - 2l_H - 1$ ničelnih oktetov

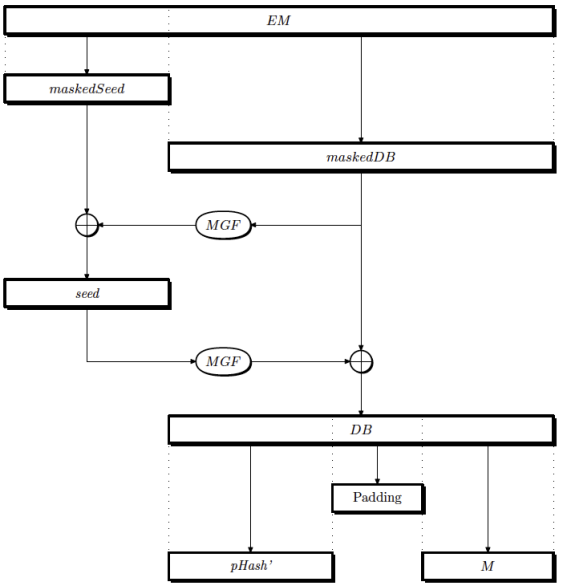
4. Izračunaj $h_P = H(P)$ kot niz oktetov dolžine l_H, kjer je H zgoščevalna funkcija, in generiraj zlepek $DB = h_P||PS||01||M$
5. Generiraj naključni niz oktetov s dolžine l_H, ki bo služil kot seme na vhodu funkcije za generiranje maske f_{gm}. S funkcijo f_{gm} generiraj masko m dolžine $l_{EM} - lH$
6. Izračunaj $m_{DB} = DB \oplus m$
7. S funkcijo f_{gm} izračunaj masko m' dolžine l_H, kot seme na vhodu funkcije uporabi m_{DB}
8. Izračunaj $m_s = s \oplus m'$
9. Vrni $EM = m_s||m_{DB}$

Shema OAEP kodiranja je prikazana na sliki Slika 2. Dekodiranje je inverzna operacija, na vhodu vzame kodirano sporočilo EM in opcijsko kodirne parametre P:

1. Naj bo l_H dolžina izhoda zgoščevalne funkcije v oktetih. Če je dolžina parametrov P večja od l_H, zavrni P
2. Naj bo l_{EM} dolžina kodiranega sporočila v oktetih. Če velja $l_{EM} < 2l_H - 1$, zavrni EM
3. Naj bo m_s prvih l_H oktetov vhoda EM in m_{DB} ostanek oketov (to je $l_{EM} - l_H$ oktetov)
4. S funkcijo za generiranje maske f_{gm} izračunaj m' dolžine l_H oktetov. Kot seme na vhodu vzami m_{DB}
5. Izračunaj $s = m_s \oplus m'$
6. S funkcijo f_{gm} izračunaj m dolžine $l_{EM} - l_H$ oktetov. Kot seme na vhodu vzami s
7. Izračunaj $DB = m_{DB} \oplus m$
8. Izračunaj $h_P = H(P)$kot niz oktetov dolžine l_H, kjer je H zgoščevalna funkcija, in razbij DB na sledeč način: $DB = h'_P||PS||01||M$

   Če oktet 01 ne obstaja (torej ne moremo ločiti PS in M), vrni napako

   Če h_P ni enak h'_P, vrni napako



Slika 3: OAEP dekodiranje: MGF - generator maske

9. Vrni M

Shema OAEP dekodiranja je prikazana na Sliki 3.

RSA-OAEP

Sedaj, ko poznamo algoritem RSA in OAEP shemo kodiranja, oboje združimo v algoritem RSA-OAEP. Poglejmo si operacijo enkripcije po korakih:

1. Sporočilo M pošlji preko operacije OAEP kodiranja (opcijsko na vhod podamo še kodirne parametre P), ki vrne kodirano sporočilo EM. Če operacija kodiranja vrne napako, vrni napako
2. Kodirano sporočilo EM pretvori v število m
3. Izračunaj $c = m^e \pmod{n}$, kjer je (n, e) javni ključ prejemnika
4. Število c pretvori v niz oktetov C dolžine k ter vrni C

Dekripcija je inverzna operacija, koraki pa si sledijo v naslednjem vrstnem redu:

1. Če prejeti kriptogram C ni dolg k oktetov, zavrni kriptogram C
2. Kodiran kriptogram C pretvori v število c
3. Izračunamo število $m = c^d \pmod{n}$
4. Število m pretvori v niz oktetov EM dolžine $k - 1$ oktetov
5. Niz oktetov EM pošlji preko operacije OAEP dekodiranja (opcijsko na vhod podamo še kodirne parametre P), ki vrne dekodirano sporočilo M. Če operacija dekodiranja vrne napako, vrni napako
6. Vrni niz oktetov M

Dokaz sematičn varnosti in s tem varnost pred adaprivnim napadom z izbranim kriptogramom bomo izpustili, saj presega vsebino tega seminarja. Si pa lahko bralec omenjeni dokaz pogleda v [6].

4.3 Zgoščevalne funkcije in digitalni podpisi

Zgoščevalna funkcija za podano sporočilo izračuna izvleček fiksne dolžine, za katerega je zaželjeno, da je unikaten, torej različen pri vsakem vhodnem sporočilu. Dolžina samega vhodnega sporočila je navzgor omejena, sicer pa je lahko poljubna. SET za zgoščevanje uporablja algoritem SHA-1 (Secure Hash Algorithm), ki na vhodu sprejme sporočila maksimalne dolžine $2^{64} - 1$ in vrača izvlečke dolžine 160 bitov. Če imamo privatni ključ, lahko z njim izvleček sporočila zakriptiramo in s tem dobimo digitalni podpis. V SET ssitemu se pri digitalnem podpisovanju uporablja RSA algoritem, ki smo ga opisali v prejšnjem poglavju.

Preko enkripcije izvlečka sporočila s privatnim ključem je ustvarjena povezava med imetnikom privatnega ključa in sporočilom. Pošiljatelj kriptiran izvleček skupaj z originalnim podpisom pošlje naslovniku, ta pa na drugi strani s pošiljateljevim javnim ključem dekriptira izvleček in ga primerja s svojim izvlečkom, ki ga z enakim zgoščevalnim algoritmom izračuna iz sporočila. Če se izvlečka ujemata, naslovnik ve, da je pošiljatelj zakriptiral izvleček sporočila s svojim privatnim ključem in da se sporočilo med pošiljanjem ni spremenilo.

Pomembno je vedeti, da sama prisotnost digitalnega podpisa ne pove nič o stanju sporočila, s katerim je povezan, oziroma, povedano drugače, deigitalni podpis ne avtenticira sporočila samega. Če pošiljatelj poslanega sporočila ne zakodira, omogoči preverjanje podpisa prav vsakemu, ki dobi v posest sporočilo

skupaj z digitalnim podpisom. Če pa pošiljatel sporočilo na nek način enkriptira, lahko podpis preverjajo točno določen naslovnik, to je tisti, ki zna sporočilo dekriptirani. Kako taka enkripcija poteka je stvar odločitve, izbiramo pa lahko med simetričnimi in asimetričnimi algoritmi. V SET protokolu se največ uporablja princip digitalne ovojnice, ki si ga bomo pogledali v naslednjem poglavju.

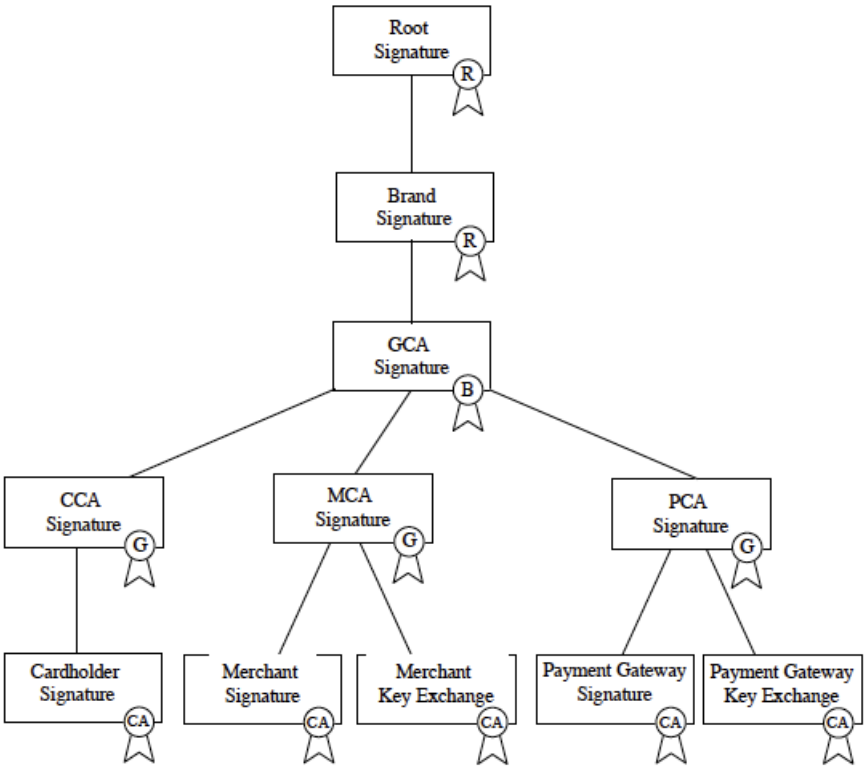
4.4 Digitalne ovojnice

V simetričnih kriptosistemih se morata pošiljatelj in prejemnik najprej dogovorito za ključ, ki bo veljal v času seje. Seveda obstaja tu tveganje, da bo ta ključ pristal v napačnih rokah, zato ga je treba pred zunanjim svetom skriti, poleg tega pa je priporočljivo, da se ključ menja karseda pogosto. Simetrična kriptografija v kombinaciji z asmietrično kriptografijo ponuja rešitev imenovano digitalna ovojnica. Digitalna ovojnica sestoji iz sporočila, ki je kriptiran z naključno generiranim simetričnim ključem, in samega ključa, ki je kriptiran z naslovnikovim javnim ključem preko RSA-OAEP algoritma, ki smo ga opisali v poglavju 4.2. Zadnje omogoča, da lahko simetrični ključ odpre samo naslovnik. S tem ključem nazadnje naslovnik dekriptira še sporočilo.

Digitalna ovojnica je pravzaprav alternativa za protokole, ki skrbijo za dogovor in izmenjavo ključev. Osnovo za take protokole sta postavila že Diffie in Hellman, vendar pa v SET sistemu, kjer je število uporabnikov zelo veliko in izmenjevanje sporočil zelo pogosto (s tem tudi menjanje ključev), taki protokoli ne pridejo v poštev. Poleg tega so operacije simetrične kriptografije hitrejše od operacij asimetrične kriptografije, tako da z dobrim simetričnim algoritmom in dovolj dolgim ključem lahko dosežemo podoben učinek, kot če bi sporočila kriptirali po principih javne kriptografije. Omenili smo že, da SET specifikacije kot simetrični kriptografski algoritem predvideva DES (tako je tudi v implementaciji sistema), vendar je v splošnem lahko uporabljen katerikoli simetrični kriptosistem.

4.5 Digitalni certifikati

Pare javnih in privatnih ključev v splošnem lahko generira kdorkoli, kar pa posledično pripelje do pomislekov glede zaupanja. Kako smo lahko prepričani, da javni ključ zares pripada določeni osebi? Ali obstaja mehanizem, ki preprečuje lažne upodobitve in s tem prevare? V resnici taki mehanizmi in varovalke, ki bi preprečevale upodabljanje druge osebe, niti v najbolj dodelanih računalniških sistemih niso implementirani brez vpeljave tretje, zaupanja vredne entitete,



Slika 4: Hierarhija zaupanja. Prikaz nivojev je zgolj ilustrativen, saj so lahko certifikati, ki jih izdajajo certifikatne agencije posameznih entitet, direktno povezani s certifikati, ki jih izdajajo certifikatne agencije znamk kreditnih kartic. Možne so tudi druge direktne povezave.

ki lahko poveže javni ključ z unikatno identificirano entiteto. Mehanizem, ki ustvari tako povezavo, se imenuje digitalni certifikat. Digitalni certifikat je nekakšen žeton, sestavljen iz serije znakov, ki ga uporabimo kot vhod v kriptografskih procesih. Za izdajanje certifikatov je zadolžena certifikatna agencija, ki s tem, ko izda certifikat, prevzame tudi nekatere odgovornosti zanj.

Vsi sodelujoči v SET sistemu se morajo že na začetku odločiti o tem, komu zaupajo in komu ne, kar seveda vpliva na vse nadaljne medsebojne odnose v SET sistemu. Določena entiteta lahko zaupa banki, plačilnim vratom ali znamki kreditne kartice. Kako točno bo ta entiteta posredovala imetniku kreditne kartice (ali pa prodajalcu) certifikat je odvisno od politike, ki jo ima določena institucija, zato na tem mestu SET specifikacije dopuščajo nekaj ma-

neverskega prostora. S tem, ko entiteta na neki točki sprejme digitalno potrdilo druge entitete, indicira zaupanje do le-te. Le ta pa se je s tem, ko je pridobila certifikat, zavezala kot zaupanja vredna entiteta.

SET certifikati se preverjajo preko tako imenovane hierarhije zaupanja (Slika 4). Vsak certifikat je povezan s certifikatom za podpisovanje entitete, ki ga je izdala, pri tem pa tudi digitalno podpisala. Kot primer si poglejmo digitalni certifikat imetnika kreditne kartice, ki ga je podpisala njegova banka (lahko tudi znamka kreditne kartice na zahtevo banke). Certifikat banke je povezan s certifikatom znamke kreditne kartice, ta pa s korenskim certifikatom. Javni ključ za pospisovanje korenskega certifikata je znan vsem entitetam v SET sistemu (oziroma njihovim programskim opremam, ki tudi hrani vse certifikate) in mu vsi brezpogojno zaupajo. Koliko nivojev ima hierarhija certifikatnih agencij, ki izdajajo certifikate, ni določeno s SET specifikacijami.

Sama distribucija certifikatov je kompleksen proces in presega obseg te seminarske naloge, zato se na tem mestu ne bomo spuščali v podroben opis le te. Omenimo samo to, da SET specifikacije predvidevajo standard X.509, ki specificira celotno infrastrukturo za distribucijo certifikatov.

4.6 Kriptiranje in dekriptiranje v SET

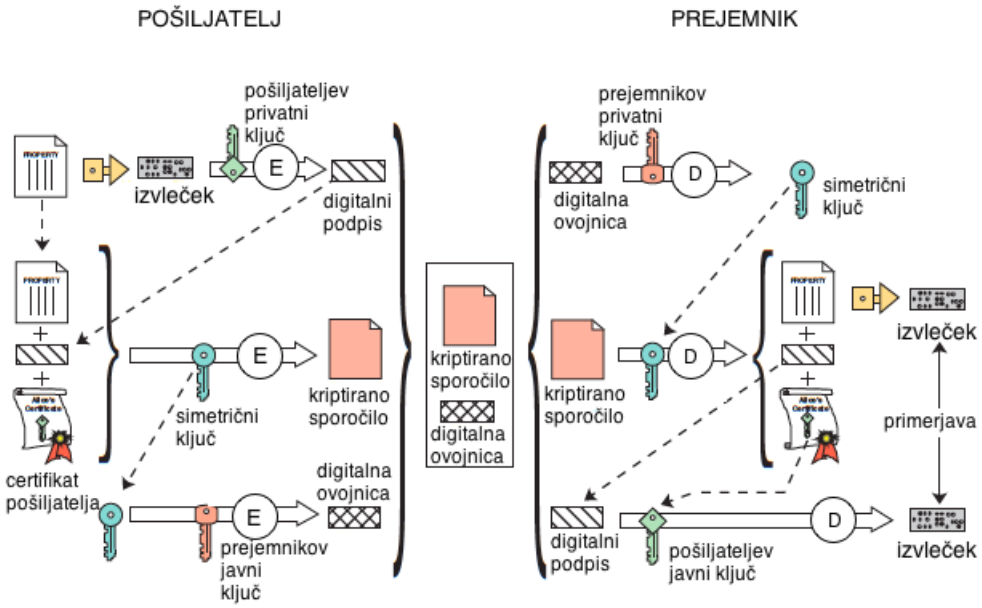
Omenili smo že, da za avtentikacijo in integriteto sporočil v SET sistemu poskrbijo kriptografski principi simetrične in asimetrične kriptografije. Slika 5 prikazuje tipični operaciji kriptiranja in dekriptiranja sporočil, ki se pretakajo preko SET protokolov. Seveda nekateri protokoli zahtevajo drugačen način avtentikacije (dvojno podpisovanje si bomo pogledali v poglavju 4.7), vendar je v osnovi ideja pri vseh enaka.

Proces enkripcije

1. Pošiljatelj pošlje sporočilo preko zgoščevalnega algoritma H. Rezultat je izvleček MD, ki se bo kasneje uporabil pri preverjanju entigritete sporočila.

2. Pošiljatelj kriptira izvleček MD svojim privatnim ključem K_{ss}, s čimer ustvari digitalni podpis.

3. Pošiljatelj naključno generira nov simetrični ključ K, s katerim preko DES algoritma kriptira sporočilo, svoj digitalni podpis in kopijo svojega certifikata, ki poleg ostale informacije vsebuje tudi pošiljateljev javni ključ K_{sp}.



Slika 5: Primer tipičnega kriptiranja v SET protokolih

4. Da bo lahko prejemnik prebral sporočilo, potrebuje tudi kopijo simetričnega ključa K. Pošiljatelj simetrični ključ zasčiti tako, da ga z javnim ključem prejemnika K_rp preko RSA algoritma enkriptira v digitalno ovojnico. Kopijo ključa K_rp ima pošiljateljs shranjeno v digitalnem certifikatu prejemnika.

5. Pošiljatelj pošlje prejemniku kriptirano sporočilo, digitalni podpis, svoj digitalni certifikat (ta vsebuje kopijo pošiljateljevega javnega ključa K_{sp}) in digitalno ovojnico, ki vsebuje simetrični ključ K.

Proces dekripcije

1. Prejemnik prejme kriptirano sporočilo, digitalni podpis prodajalca, digitalni certifikat prodajalca ter digitalno ovojnico s simetričnim ključem.

2. Prejemnik s svojim privatnim ključem K_rp dekriptira ovojnico ter s tem pridobi kopijo simetričnega kljuca K.

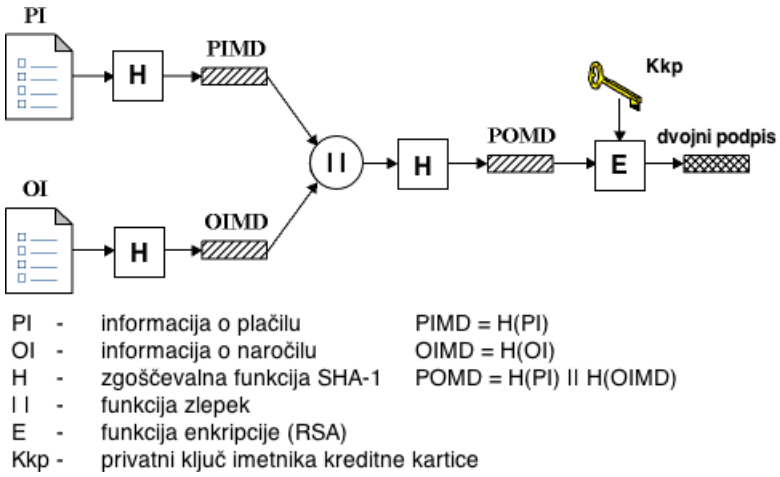
3. Prejemnik s simetričnim ključem K preko DES algoritma dekriptira sporočilo, podpis in certifikat pošiljatelja. S slednjim pridobi tudi kopijo javnega ključa pošiljatelja K_{sp}.

4. Prejemnik pošlje sporočilo preko zgoščevalnega algoritma H ter tako pridobi nov izvleček MD'. Dobljeni digitalni podpis dekriptira s pošiljateljevim javnim ključem ključem K_{sp} ter dobljeni izvleček MD primerja z izvlečkom MD'. Če sta enaka, je lahko prejemnik prepričan, da je bilo sporočilo podpisano s privatnim ključem pošiljatelja K_{ss} in da se sporočilo med tranzitom ni spreminjalo. V nasprotnem primeru prejemnik zavrne sporočilo.

4.7 Dvojni podpis

Dvojni podpis je pomembna inovacija razvijalcev SET specifikacij. Namen dvojnega podpisa je enak standardnemu podpisu, torej zagotoviti avtentikacijo in integriteto podatkov. Za razliko od standardnega digitalnega podpisa dvojni podpis poveže dve sporočili, kateri sta namenjeni dvema različnima naslovnikoma. V primeru SET sistema želi kupec poslati informacijo o naročilu, ki je namenjena prodajalcu, in informacijo o plačilu, ki je namenjena banki oziroma kaki drugi finančni instituciji, ki bo izvršila transakcijo (na primer plačilna vrata). Obe sporočili sta zapakirani v en paket, ki bo od kupca najprej potoval do prodajalca, od prodajalca pa naprej do banke. Prodajalce ne zanima informacija o plačilu, niti kupcu ni v interesu, da jo ta vidi, saj vključuje tudi številko kreditne kartice. Podobno banke ne zanima kaj je kupec naročil pri prodajalcu, saj le ta za procesiranje svojih funkcij te informacije ne potrebuje. Vseeno pa mora med obema informacijama obstajati povezava, s katero lahko kupec dokaže, da je bilo plačilo namenjeno za točno določeno naročilo.

Imetnik kreditne kartice generira dvojni podpis na sledeč način: Za informacijo o naročilu in informacijo o plačilu z zgoščevalnim algoritmom SHA-1 izračuna izvlečka ter ju zlepi. Dobljeni zlepek potem še enkrat pošlje preko zgoščevalnega algoritma, končni izvleček pa zakriptira s svojim privatnim ključem. Da bo lahko prejemnik na drugi strani dvojni podpis preveril, mu mora pošiljatelj (v našem primeru imetnik kreditna kartice) poleg dvojnega podpisa poslati tudi izvleček sporočila, ki mu ni namenjen. Prodajalec bo tako prejel dvojni podpis, informacijo o naročilu ter izvleček informacije o plačilu, plačilna vrata pa bodo prejela dvojni podpis, informacijo o plačilu in izvleček informacije o naročilu. Dvojni podpis preverimo podobno kot navaden podpis, le da upoštevamo, da je sestavljen iz dveh delov. Prejemnik bo za sporočilo, ki mu je namenjeno direktno, izračunal izvleček, ga zlepil s posredovanim izvlečkom sporočila, ki ga ne zadeva, ter dobljeno primerjal z dekriptiranim dvojnim podpisom. Shema generiranje dvojnega podpisa je prikazana na sliki 6. Kako generiranje in pre-



Slika 6: Konstrukcija dvojnega podpisa

verjanje podpisa izgleda v praksi pa si bomo pogledali v naslednjem primeru.

Naj bo H zgoščevalni algoritem SHA-1, E funkcija kodiranja v RSA in KR_C privatni ključ kupca. Naj bo $OI = 315a46e5\ 1283f7c6\ 47000000(16)$ informacija o naročilu in $PI = 1325f475\ 68000000(16)$ informacija o plačilu. Ker SHA-1 algoritem procesira bloke velikosti 512 bitov razdeljene v 32 bitne besede, moramo obe informaciji dopolniti do velikosti bloka. Algoritem SHA-1 zahteva, da zadnih 64 bitov predstavlja velikost originalnega sporočila in da je prvi bit v dopolnitvi do velikosti bloka enak 1. Informaciji po dopolnitvi sedaj izgledata takole:

315a46e5	1283f7c6	47800000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000048

1325f475	68800000	00000000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000000
00000000	00000000	00000000	00000028

Naj bo h_O izvleček paketka z informacijo o naročilu in h_P izvleček paketka z infomracijo o plačilu. Algoritem SHA-1 vrne naslednja izvlečka velikosti 160 bitov:

$$h_O = H(OI) = c4511d95\ 4556f627\ fa491c85\ a5a8cf0c\ 6af4f62c$$
$$h_P = H(PI) = 6e94de9c\ ab3cb005\ 35d792ca\ 05aac971\ 76a17d65$$

Dobljena izvlečka zlepimo skupaj ($h_O||h_P$) in dopolnimo do velikosti 512 bitov tako, kot od nas zahteva SHA-1 algoritem:

c4511d95	4556f627	fa491c85	a5a8cf0c
6af4f62c	6e94de9c	ab3cb005	35d792ca
05aac971	76a17d65	80000000	00000000
00000000	00000000	00000000	00000140

Ko zlepek pošljemo preko zgoščevalnega algoritma SHA-1, dobimo:

$$h = H(h_O||h_P) = ee3e9a3d\ ba2dda59\ c6631a58\ 1c7cdd9e\ 1bec3e99(16) =$$
$$1360134484714001519823723727533031546268859285377(10)$$

Sedaj potrebujemo privatni ključ, s katerim bo kupec zakodiral izračunani izvleček. Par privatnega in javnega kluča generiarmo po metodi, ki smo jo opisali v prejšnjem poglavju. Najprej si izberemo dve veliki praštevili p in q in izračunamo produkt $n = pq$. Naj bo $p = 47$ in $q = 73$, torej je $n = 3431$ in $\phi(n) = (p-1)(q-1) = 3312$. Recimo da si kupec izbere javni ključ $e_c = 79$, iz česar sledi, da je pripadajoči privatni ključ $d_c \equiv 2767 \pmod{3312}$. Privatni ključ smo izračunali s pomočjo rezširjenega Evklidovega algoritma, kar nam omogoča naslednja zveza:

$$d_c \equiv e_c^{-1} \pmod{\phi(n)} \equiv 79^{-1} \pmod{3312}$$

V procesu dvojnega podpisovanja sta vlogi privatnega in javnega ključa obrnjeni, saj se privatni ključ uporablja za kriptiranje oziroma podpisovanje, javni ključ pa za dekriptiranje oziroma verifikacijo podpisa. Da zakriptiramo končni izvleček h, bomo le tega najprej razbili na numerične bloke enekih dimenzij ter zakriptirali enega po enega. Naj bo h_i en tak blok dolžine 3, oziroma, da bo bolj pregledno, zapišemo h kot:

136	013	448	471	400	151
982	372	372	753	303	154
626	885	928	537	7	

Kriptirajmo sedaj prvi blok:

$$h_i^{d_c} \equiv 136^{2767} \equiv 3304 \pmod{3431}$$

Enako naredimo za vse ostale bloke. Zakriptirane bloke ponovno zlepimo, kar nam prinese dvojni podpis DS:

3044	0180	0168	2013	3308	1361
3420	0395	0395	1740	0977	0227
0604	0082	0900	0363	0103	

Sedaj želi prodajalec preveriti ta podpis. Za to ima na na voljo pošiljateljev javni ključ $e_c \equiv 97 \pmod{3312}$, informacijo o naročilu OI in izvleček informacije o plačilu $H(PI)$. Iz informacije o naročilu OI bo z zgoščevalnim algoritmom izračunal izvleček $H(OI)$, ga zlepil skupaj z izvlečkom informacije o plačilu $H(PI)$ ter iz dobljenega povno izračunal izvleček:

$$h_M = H(H(OI)||H(PI) = \\ 136013448471400151982372372753303154626885928537 7(10)$$

Dobljeni izvleček bo primerjal z izvlečkom, ki ga dobi, ko s pošiljateljivim javnim ključem dekriptira dvojni podpis.

Enako kot prodajalec dvojni podpis preveri tudi banka, le da ima ta na voljo pošiljateljev javni ključ $e_c \equiv 97 \pmod{3312}$, informacijo o plačilu PI in izvleček informacije o naročilu $H(OI)$. S tem, ko je verifikacija uspela tako na strani prodajalca kot na strani banke, je kupec ustvaril povezavo med naročilom in plačilom, ki jo lahko tudi dokaže.

5 Plačilni procesi in transakcije v SET

Celoto SET sistema sestavlja več podsistemov oziroma protokolov, vsak od njih pokrije del celotnega procesa elektronskega plačevanja s plačilnimi karticami. Glavni procesi sistema SET so registracija imetnika kreditne kartice, registracija prodajalca, zahteva nakupa, avtorizacija plačila in zajetje plačila. Na tem mestu smo sistem nekoliko posplošili in izpustili nekatere procese, kot so povpraševanje po nakupu, protokol za upravljanje z napakami, povratne protokole in še nekatere, saj ti ne nastopajo direktno v procesu same finančne transakcije. Njihov namen je prevsem vzdrževanje konsistentnosti celotnega sistema.

5.1 Registracija imetnika kreditne kartice

Prodajalec bo zavrnil kakršenkoli poskus zahteve po začetku SET transakcije, če kupec ne bo imel veljavnega digitalnega potrdila. To pomeni, da se mora imetnik kreditne kartice najprej registrirati pri certifikatni agenciji ter seveda pridobiti par privatenega in javnega ključa.

Certifikat imetnika kreditne kartice ima funkcijo elektronske predstavitve številke kreditne kartice. Ker je digitalno podpisan s strani finančne institucije, kjer ima imetnik kartice odprt račun, ne more biti spremenjen ali pa celo generirani s strani kake tretje entitete. Sam certifikat ne vsebuje številke kreditne kartice in datum poteka le te, pač pa le informacije o računu in skrivno vrednost, ki jo pozna le programska oprema imetnika kartice in je zakodirana z enosmernim zgoščevalnim algoritmom. Če bi bila skrivna vrednost skupaj s številko računa in datumom poteka znana, bi bila povezava med certifikatom in kartico zlahka dokazljiva, vendar v tem primeru tudi razvidna iz certifikata. Ker pa certifikat ne vsebuje številke kreditne kartice in datuma poteka, povezavo med certifikatom in kartico preverijo plačilna vrata. Registracija se začne z začetno zahtevo imetnika kreditna kartice (Slika 7), sledi prevzem registracijskega obrazca (Slika 8) in na koncu še prevzem certifikata. Sledi opis posameznih podprocesov po korakih.

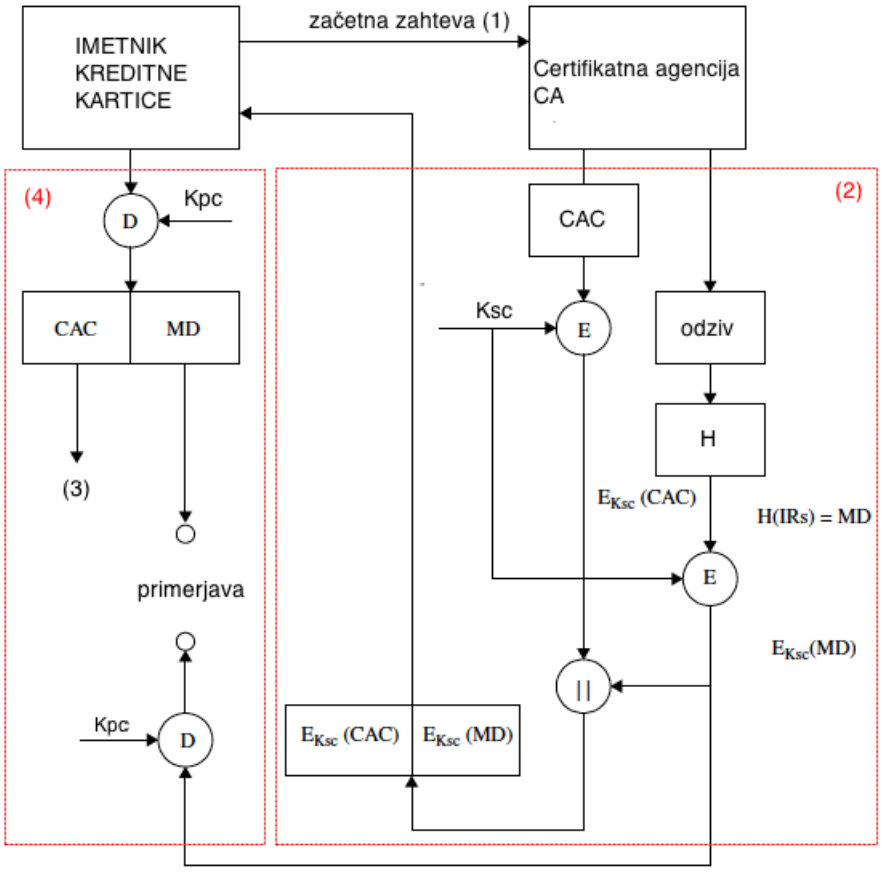
Začetna zahteva in odziv certifikatne agencije

1. Imetnik kreditne kartice pošlje certifikatni agenciji začetno zahtevo.
2. Certifikatna agencija prejme začetno zahtevo, generira odgovor, izračuna njegov izvleček ter ga zakriptira s svojim privatnim ključem (ga digitalno podpiše). Odgovor skupaj s svojimi digitalnimi certifikati pošlje imetniku kreditne kartice.
3. Imetnik kreditne kartice preko hierarhije zaupanja preveri prejete certifikate (rekurzivno do korenske agencije, ki ji brezpogojno zaupa).
4. Programska oprema, nameščena na računalniku imetnika kreditne kartice, preveri podpis certifikatne agencija tako, da ga najprej dekriptira z javnim ključem agencije (pridobi ga s certifikatom) in rezultat primerja z izvlečkom, ki ga iz odziva izračuna z enakim zgoščevalnim algoritmom, kot ga je uporabila certifikatna agencija.

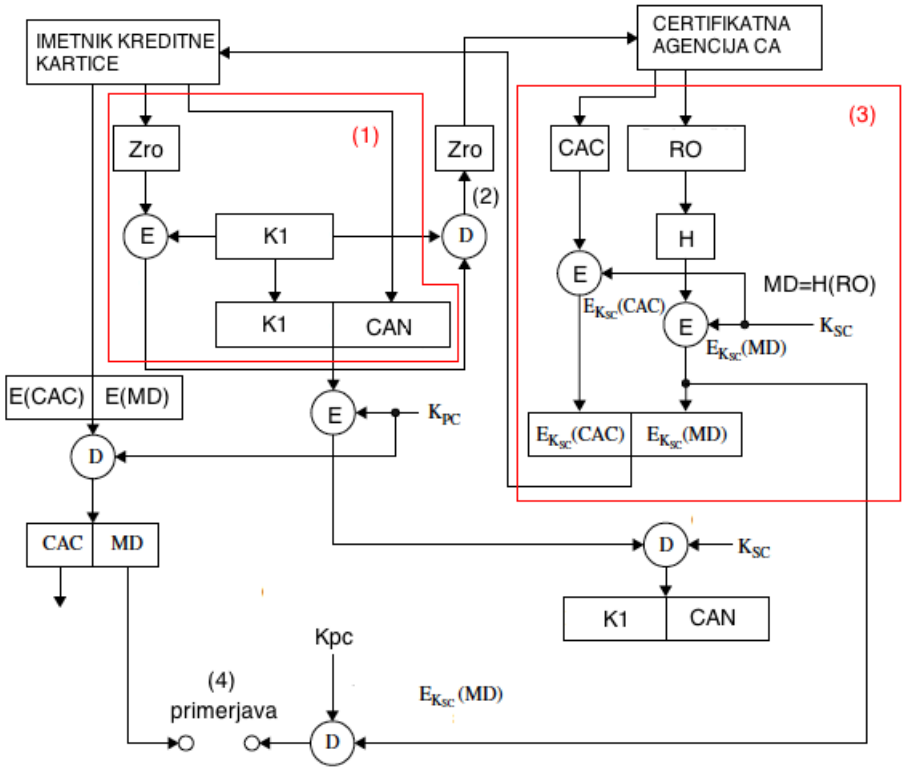
Certifikati agencije, ki jih imetnik kreditne kartice pridobi z odzivom, so s programsko opremo shranjeni na računalnik imetnika kreditne kartice, saj se potrebni še v kasnejših korakih registracije. Sledi zahteva in prevzem registracijskega obrazca.

Prevzem registracijskega obrazca

1. Imetnik kreditne kartice generira zahtevo za registracijski obrazec in jo preko DES algoritma zakriptirana z naključno generiranim simetričnim



Slika 7: Registracija imetnika kreditne kartice - začetna zahteva: E - operacija kriptiranja, D - operacija dekriptiranja, H - zgoščevalna funkcija, CAC - certifikat agencije, K_{sc} - privatni ključ certifikatene agencije, K_{pc} - javni ključ certifikatne agencije



Slika 8: Registracija imetnika kreditne kartice - prevzem obrazca: E - operacija kriptiranja, D - operacija dekriptiranja, H - zgoščevalna funkcija SHA-1, Z_{ro} - zahteva za registracijski obrazec, RO - registracijski obrazec, CAC - certifikat agencije, K_{sc} - privatni ključ certifikatene agencije, K_{pc} - javni ključ certifikatne agencije, K_1 - simetrični ključ za DES

ključem K_1. Ta ključ je skupaj s številko računa imetnika kreditne kartice zakriptiran z javnim ključem certifikatne agencije. Generirana digitalna ovojnica je skupaj s kriptirano zahtevo poslana certifikatni agenciji.

2. Certifikatna agencija s svojim privatnim ključem dekriptira številko računa in simetrični ključ K_1, s katerim dekriptira še zahtevo.

3. Certifikatna agencija preveri zahtevo ter pripravi obrazec, generira izvleček ter ga zakriptira s svojim privatnim ključem (obrazec digitalno podpiše). Obrazec skupaj s podpisom in svojim certifikatom pošlje imetniku kreditne kartice.

4. Imetnik kreditne kartice preko hierarhije zaupanja preveri certifikat agencije in njen podpis.

Na tem mestu ima imetnik kreditne kartice v posesti registracijski obrazec, ki ga izpolni s potrebnimi podatki. Ti so ponavadi odvisni od finančnih institucij, saj morajo le te preko njih identificirati osebo, ki je poslala zahtevo za certifikat, kot veljavnega imetnika kreditne kartice. Programska oprema na strani imetnika kartice generira še par javnega in privatnega ključa, čemur sledi naslednji korak - prevzem certifikata.

Prevzem certifikata

1. Imetnik kreditne kartice generira zahtevo za certifikat, ki vsebuje izpolnjen registracijski obrazec.

2. Imetni kreditne kartice ustvari novo sporočilo, ki vsebuje zahtevo, generiran javni ključ imetnika in na novo generiran simetrični ključ K_2. Vse skupaj digitalno podpiše z uporabo zgoščevalnega algoritma in svojim privatnim ključem. Celotno sporočilo nazadnje kriptira z na novo generiranim simetričnim ključem K_3. Ta ključ je skupaj s številko računa imetnika kartice kriptiran z javnim ključem certifikatne agencije.

3. Imetnik kartice kriptirano sporočilo, ki vsebuje zahtevo z izpolnjenim obrazcem, simetrični ključ K_2 in podpis imetnika kartice, skupaj z digitalno ovojnico, ki vsebuje simetrični ključ K_3, pošlje certifikatni agenciji.

4. Certifikatna agencija s svojim privatnim ključem dekriptira infomracijo o računu imetnika kreditne kartice, simetrični kljuc K_3, s katerim dekriptira še zahtevo, ter javni ključ imetnika kreditne kartice.

5. Certifikatna agencija preveri podpis imetnika kreditne kartice tako, da ga dekriptira z javnim ključem imetnika kartice ter dobljeni izvleček primerja s izvlečkom, ki ga z istim zgoščevalnim algoritmom izračuna sama.

6. Certifikatna agencija preveri zahtevo, za kar ima na voljo informacijo o računu in izpolnjen registracijski obrazec. Proces preverjanja zahteve, ki poteka med certifikatno agencijo in finančno institucijo, ni predpisan s SET specifikacijami.

7. Če je z zahtevo vse vredu, certifikatna agencija generira certifikat, ki ga vključi v odgovor na zahtevo. Le tega s svojim privatnim ključem digitalno podpiše. Odgovor zakriptira s simetričnim ključem K_2, ki je bil vključen v zahtevo imetnika kreditne karice. Odgovor je poslan imetniku kreditne kartice.

8. Imetnik kartice preveri certifikat ter dekriptira odgovor z uporabo simetričnega ključa K_2, ki ga ima shranjenega programska oprema.

9. Imetnik kartice preveri podpis certifikatne agencije ter shrani certifikat in informacijo iz odgovora za nadaljno uporabo v SET sistemu.

5.2 Registracija prodajalca

Zaradi enakih razlogov, kot mora to storiti imetnik kreditne kartice, se mora pri certifikatni agenciji registrirati tudi prodajalec. V tem primeru je registracijski postopek nekoliko drugačen kot pri registraciji imetnika kreditne kartice, začene in konča pa se na enak način - z zahtevo po registracijskem obrazcu in prevzemom certifikata.

Zahteva registracijskega obrazca

1. Prodajalec certifikatni agenciji pošlje zahtevek po registracijskem obrazcu.

2. Certifikatna agencija identificira obrazec, ki ustreza zahtevi, ga digitalno podpiše ter skupaj s svojimi digitalnimi certifikati pošlje prodajalcu.

3. Prodajlec s pomočjo programske opreme preko hierarhije zaupanja preveri certifikate agencije ter digitalni podpis.

Prodajalec ima sedaj v posesti ustrezen registracijski obrazec, zato ga izpolni z ustreznimi podatki. Za potrebe kriptiranja in podpisovanja prodajalec s pomočjo prograske opreme generira še dva para asimetričnih ključev. En par

bo namenjen kriptiranju (izmenjevanje ključev), drugi pa podpisovanju. Sledi kreiranje sporočila z zahtevo za prevzem certifikata.

Zahteva in prevzem certifikata

1. Prodajalec kreira zahtevo za prevzem certifikata, ki poleg izpolnjenega obrazca vsebuje tudi oba generirana javna ključa, ter zahtevo digitalno podpiše. Celotan zahteva je kriptirana še z naključno gneriranim simetričnim ključem K_1. Na koncu je simetrični ključ skupaj s podatki o računu prodajalca zakriptiran še z javnim ključem agencije (ustvarjena je digitalna ovojnica), vse skupaj pa poslano agenciji.

2. Certifikatna agencija s svojim privatnim klučem dekriptira digitalno ovojnico ter s pridobljenim simetričnim ključem K_1 odkriptira sporočilo.

3. Certifikatna agencija preveri podpis prodajalca (za to ima na voljo prodajalčev javni ključ za pospisovanje).

4. Certifikatna agencija preko povezav z finančnimi institucijami, ki so neodvisne od SET sistema, preveri registracijske podatke, generira digitalne certifikate ter jih podpiše.

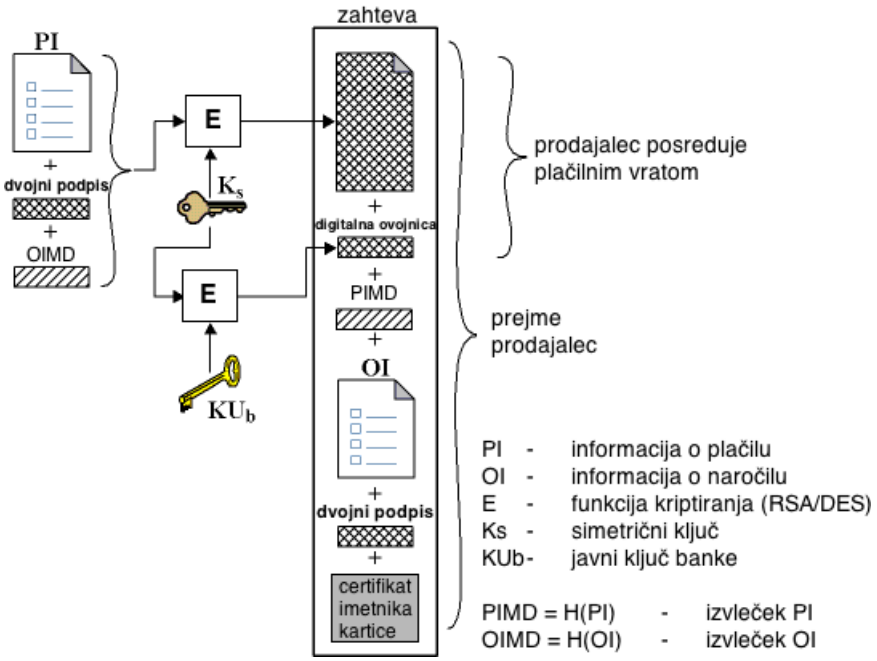
5. Generirani certifikati so zapakirani v odziv, ta pa je kriptiran z novim naključno generiranim simetričnim ključem K_2. Ta je kriptiran še z javnim ključem prodajalca ter v generirani digitalni ovojnici priložen odzivu odziv. Na koncu certifikatna agencija vse skupaj pošlje prodajalcu.

6. Prodajalec dekriptira ovojnico, s pridobljenim simetričnim ključem K_2 dekriptira odziv, ki vsebuje prodajalčeve certifikate. Le te s pomočjo programske opreme preveri (preko hierarhije zaupanja) ter shrani ta nadaljno uporabo.

Podobno, kot velja za validacijo registracijskih podatkov pri imetnikih kartic, tudi v tem primeru le ta ni določena s SET specifikacijami. Gotovo je le, da je potrebna povezava med certifikatno agencijo in banko oziroma posrednikom, ki pozna vse potrebne informacije o prodajalcu. Protokoli, ki delujejo na tej povezavi, morajo za varnost poskrbeti sami.

5.3 Zahteva nakupa

Zahteva nakupa pride na vrsto po tem, ko imetnik kreditne kartice na spletni strani že izbere željene artikle ter način plačila s kreditno kartico. Jasno je,



Slika 9: Zahteva nakupa

da mora biti sama izkušnja nakupovanja neodvisna od načina plačila, tako da lahko prodajalec implementira poljuben način "nakupovalnega vozička", kjer pa mora upoštevati željo kupca po zasebnosti in varnosti. Da pa lahko kupec sploh pošilja SET sporočila, mora najprej pridobiti kopijo digitalnega certifikata plačilnih vrat. Celoten proces samega nakupa začne imetnik kreditne kartice s tem, ko pošlje prodajalcu začetno zahtevo. Le ta odgovori z začetnim odzivom, ki vključuje tudi potrebna certifikate. Sledi dejanska zahteva nakupa, postopek pa se zaključi z odzivom prodajalca na le to.

Začetna zahteva in odziv

Imetnik kreditne kartice z začetno zahtevo pridobi certifikat prodajalca ter certifikat plačilnih vrat. Če v procesu plačevanja v vlogi posrednika sodeluje še kakšna druga SET entiteta, se v odziv vključi tudi certifikat le tega, tako da ga lahko preveri tudi imetnik kartice. Prvi koraki v zahtvi nakupa si sledijo v naslednjem vrstnem redu:

1. Imetnik kreditne kartice pošlje prodajalcu začetno zahtevo.
2. Prodajalce sprejme začetno zahtevo, generira odziv, vanj vključi unikatno identifikacijsko številko transakcije, ter ga digitalno podpiše. Skupaj z generiranim odzivom imetniku kartice odpošlje še vse potrebne certifikate. V večini primerov sta to certifikat prodajalca ter certifikat plačilnih vrat, preko katerega prodajalec opravlja avtorizacije in zajetja plačil.
3. Imetnik kreditne kartice s pomočjo programske opreme preko hierarhije zaupanja preveri vse prejete certifikate ter jih shrani za poznejšo uporabo. Sledi še verifikacija digitalnega podpisa po ustaljenem postopku.

Zahteva nakupa

Imetnik kreditne kartice zahtevo nakupa generira s pomočjo programske opreme, ki jo mora predhodno naložiti na osebni računalnik in je predpogoj za uporabo SET sistema. Vsebinski del zahteve sestavljata informacija o naročilu OI, ki je pridobljena v fazi spletnega izbiranja, in informacija o plačilu PI, ki je na tej stopnji že določena. Obema informacija je dodana še identifikacijska številka transakcije, ki jo je določi prodajalec. Preko te številke bodo plačilna vrata pri avtorizaciji plačila povezala informacijo o naročilu in informacijo o plačilu. Sledi podrobnejši opis konstrukcije zahteve po korakih (Slika 9):

1. Imetnik kreditne kartice izračuna izvleček informacije o naročilu OI in izvleček informacija o plačilu PI, dobljena izvlečka zlepi ter ponovno

pošlje preko zgoščevalnega algoritma SHA-1. Končni izvleček kriptira s svojim privatnim ključem, s čimer generira dvojni podpis, ki je skupaj z izvlečkom informacije o plačilu dodan zahtevi nakupa.

2. Imetnik kreditne kartice naključno generira simetrični ključ K_1 in z njim preko DES algoritma zakriptira informacijo o plačilu PI, dvojni podpis ter izvleček informacije o naročilu OI. Ključ K_1 je nazadnje skupaj s podatki o računu imetnika kartice zakriptiran z javnim ključem plačilnih vrat (ustvarjena je digitalna ovojnica, ki jo lahko odprejo samo plačilna vrata).

3. Zahteva nakupa, ki sestoji iz informacije o naročilu OI, dvojnega podpisa, digitalnega certifikata imetnika akrtice, izvlečka informacije o plačilu PI ter digitalne ovojnice s pripadajočim kriptiranim paketom, namenjenim plačilnim vratom, je sedaj poslana prodajalcu.

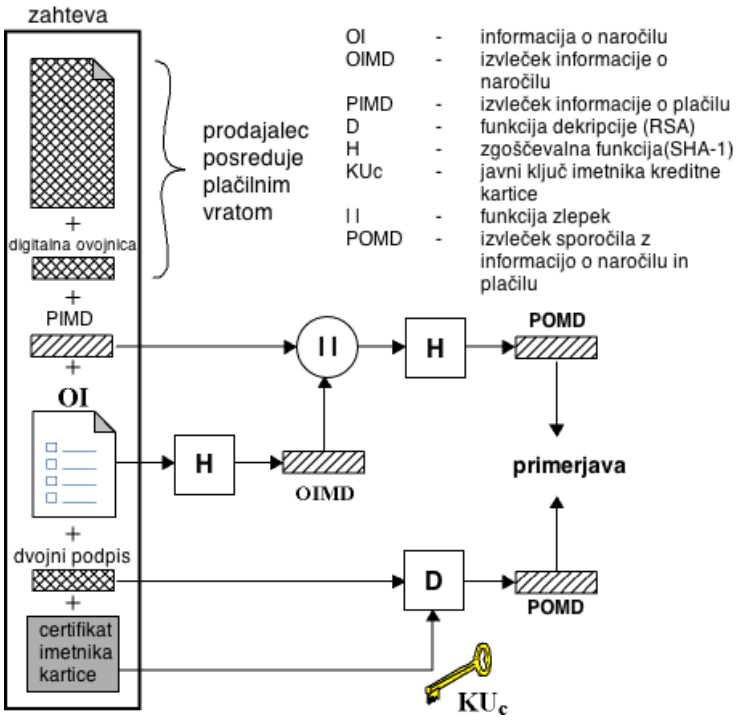
4. Prodajalec s pomočjo programske opreme preveri certifikat imetnika kartice ter dvojni podpis tako, da ga dekriptira z javnim ključem imetnika kartice, dobljeno pa primerja z zlepkom na novo izračunanega izvlečka informacije o naročilu OI in prejetega izvlečka informacije o plačilu PI (Slika 10).

Prodajalec ima sedaj na razpolago vse potrebne podatke, ki jih potrebuje za obdelavo zahteve. Procedure, s katerimi prodajalec obdela informacijo o naročilu OI, se SET specifikacijami niso specificirane, je pa točno definirana avtorizacija plačila, ki jo bomo podrobneje razdelali v naslednjem poglavju. Trenutno je dovolj le informacija, ali je avtorizacija plačila uspela, saj bo glede na to informacijo prodajalec generiral odziv. Če avtorizacija uspe, lahko poleg odziva prodajalec začne tudi postopke poslovne narave, kot so pakiranje in odprema plačanega blaga.

Odziv na zahtevo nakupa

1. Prodajalec s pomočjo programske opreme generira odziv, ki vključuje certifikat prodajalca, ter ga digitalno podpiše. Generiran odziv pošlje imetniku kreditne kartice.

2. Imetnik kartice s programsko opremo preveri certifikat prodajalca preko hierarhije zaupanja ter podpis prodajalca. Programska oprema poskrbi tudi za to, da se prejeti odziv varno shrani na računalniku imetnika kreditne kartice.



Slika 10: Verifikacija zahteve nakupa

5.4 Avtorizacija plačila

Prodajalec je imetnika kartice v smislu zaupanja že preveril preko njegovega digitalnega certifikata, sedaj pa mora preveriti še veljavnost informacije o plačilu ter ali ima plačilna kartica sploh dovolj kritja za naročeno blago. Te podatke lahko prodajalcu posredujejo plačilna vrata (ali kaka druga finančna institucija), zato prodajalec generira zahtevo za avtorizacijo plačila ter jo posreduje plačilnim vratom. V avtorizacijsko zahtevo je vključen tudi kriptiran paket, ki vsebuje informacijo o plačilu, dvojni podpis ter izvleček informacije o naročilu. Ta paket je vzet iz zahteve naročila, ki jo je generiral imetnik kreditne kartice (Slika 9). Da plačilna vrata lahko odprejo ta paket, potrebujejo simetrični ključ, s katerim je paket kriptiran. Digitalna ovojnica, ki je zaprta z javnim ključem plačilnih vrat in vsebuje potreben simetrični ključ, je tudi vključena v zahtevo nakupa, tako da je skupaj s kriptiranim paketom tudi vključena v zahtevo za avtorizacijo plačila. Plačilna vrata imajo na ta način vso potrebno informacijo za avtorizacijo, ki se izvrši preko poslovnih procedur. Le te so neodvisne od SET sistema, tako da je implementacija le teh stvar posamezne institucije. Glede na rezultat avtorizacije je potem generiran odziv, ki je kot odgovor poslan prodajalcu, ta pa glede na avtorizacijo generira odgovor na kupčevo zahtevo plačila.

Zahteva avtorizacije plačila

1. Prodajalec generira zahtevo za avtorizacijo plačila ter vanjo vključi s simetričnim ključem kriptirano informacijo o plačilu skupaj z dvojnim podpisom in izvlečkom informacije o naročilu. Certifikat imetnika kartice in digitalna ovojnica, ki vsebuje simetrični ključ, sta prav tako dodani zahtevi.

2. Prodajalec z uporabo zgoščevalnega algoritma SHA-1 in svojega privatenga ključa zahtevo digitalno podpiše.

3. Prodajalec s pomočjo programske opreme generira nov naključen simetrični ključ K in celotno zahtevo zakriptira preko DES algoritma. Generiran ključ je z javnim ključem plačilnih vrat zaprt v digitalno ovojnico ter priložen zahtevi. Prodajalec vse skupaj s svojim certifikatom pošlje plačilnim vratom.

4. Plačilna vrata preko hierarhije zaupanja preverijo certifikate prodajalca.

5. Plačilna vrata s svojim privatnim ključem odkriptirajo digitalno ovojnico, s čimer pridobijo simetrični ključ, s tem pa odprejo celotno zahtevo za avtorizacijo plačila.

6. Plačilna vrata preverijo digitalni podpis prodajalca in preko hierarhije certifikatnih agencij še digitalni certifikat imetnika kartice.

7. Plačilna vrata odprejo digitalno ovojnico in s tem pridobijo simetrični ključ K, s katerim je imetnik kreditne kartice zakriptiral informacijo o plačilu, izvleček informacije o naročilu ter dvojni podpis.

8. Plačilna vrata s pomočjo javnega ključa imetnika kartice in izvlečka informacije o naročilu preverijo dvojni podpis.

9. Plačilna vrata preverijo konsistentnost med informacijo o plačilu in zahtevo o avtorizaciji, ki jo nazadnje preko finančnih mrež posreduje finančni instituciji, kjer ima imetnik kartice odprt račun.

Odziv avtorizacije plačila

1. Plačilna vrata generirajo odziv na zahtevo avtorizacije plačila ter ga digitalno podpišejo.

2. Generiran odziv je preko DES algoritma kriptiran z naključno generiranim simetričnim ključem, ta pa je z javnim ključem prodajalca zaprt v digitalno ovojnico.

3. Plačilna vrata s pomočjo programske opreme generirajo žeton, ki ga bo prodajalec uporabil v postopku zajetja plačila. Žeton je kriptiran preko DES algoritma z uporabo novega naključno generiranega simetričnega ključa, ki je prav tako zaprt v digitalno ovojnico.

4. Odziv je skupaj z žetonom in digitalnim certifikatom plačilnih vrat poslan prodajalcu.

5. Prodajalec preko hierarhije certifikatnih agencij preveri certifikat plačilnih vrat. S svojim privatim ključem odpre digitalno ovojnico in s tem pridobi simetrični ključ, s katerim je kriptiran odziv. Sedaj preveri še digitalni podpis plačilnih vrat.

6. Prodajalec žeton zajetja s pomočjo programske opreme skupaj z digitalno ovojnico, ki vsebuje ključ, s katerim je zakriptiran žeton, shrani za postopek zajetja plačila.

5.5 Zajem plačila

Ko je postopek nakupa končan, želi prodajalec za opravljeno storitev oziroma prodano blago plačilo. SET na tem mestu predvideva dve možnosti: več posameznih zajeti plačil preko dneva, kar pomeni zajetje ob vsakem nakupu, ali pa en sam paket zajetij preko celotnega dneva. Gre za poslovno odločitev prodajalca in ne izključuje kombinacije obeh možnosti, torej več manjših paketov zajetij preko celotnega dneva. V vsakem primeru postopek začne prodajalec z zahtevo po zajetju, končajo pa plačilna vrata z odzivom na zahtevo.

Zahteva zajetja plačila

1. Prodajalec s programsko opremo generira zahtevo za zajetje plačila, poleg vključi svoj digitalni certifikat ter zahtevo digitalno podpiše.

2. Prodajalec naključno generira simetrični ključ ter preko DES algoritma zahtevo zakriptira, generiran ključ pa z javnim ključem plačilnih vrat zapre v digitalno ovojnico.

3. Prodajalec kriptirano zahtevo skupaj z digitalno ovojnico, žetonom in pripadajočo ovojnico, ki ju je dobil z odzivom na zahtevo avtorizacije plačila, pošlje plačilnim vratom.

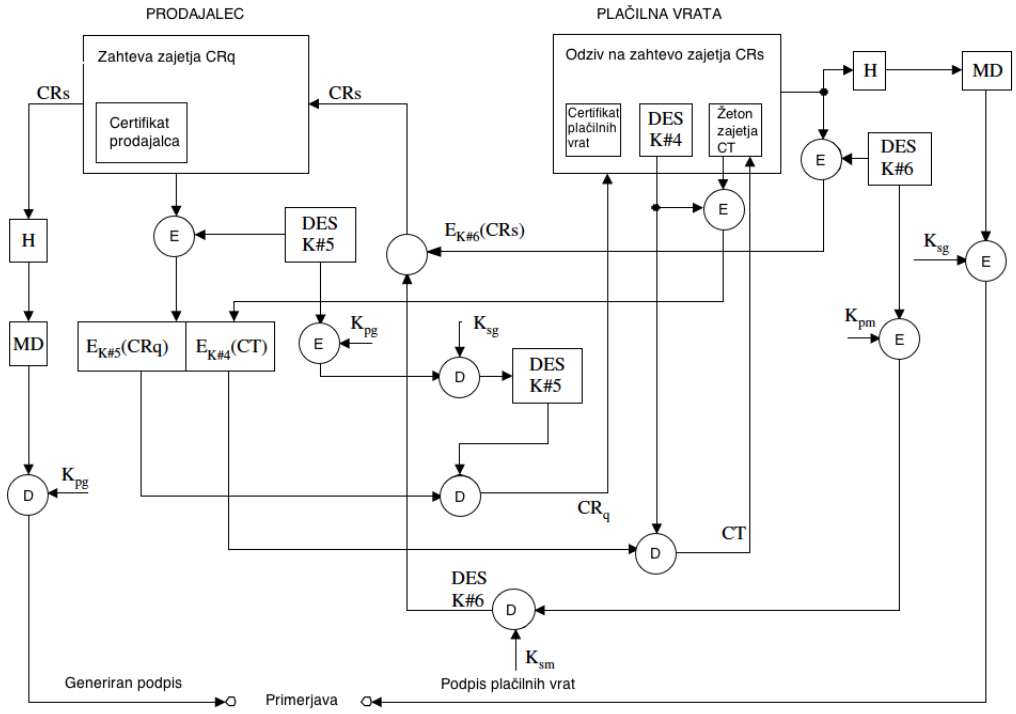
4. Plačila vrata najprej preko hierarhije zaupanja preveri certifikat prodajalca, potem odprejo digitalno ovojnico in s pridobljenim simetričnim ključem dekriptirajo zahtevo. Sledi preverjanje digitalnega podpisa.

5. Enako kot zahtevo plačilna vrata dekriptirajo še žeton zajetja plačila (zahtevi je priložena tudi digitalna ovojnica s simetirčnim ključem, s katerim je kriptiran žeton)

6. Plačilna vrata preverijo konsistentnost med žetonom in zahtevo, le to pa na koncu preko finančne mreže (neodvisna od SET sistema) pošlje finančni instituciji, kjer ima prodajalec odprt račun.

Odziv na zahtevo zajetja plačila

1. Plačilna vrata generirajo odziv, kamor vključijo tudi deigitalni certifikat za podpisovanje, vse skupaj pa digitalno podpišejo s svojim privatnim ključem in uporabo zgoščevalnega algoritma SHA-1.



Slika 11: Zajetje plačila: K_{pm} - javni ključ prodajalca, K_{pg} - javni ključ plačilnih vrat, K_{sg} - privatni ključ plačilnih vrat

2. Plačilna vrata naključno generirajo nov simetrični ključ in z njim preko DES algoritma zakriptirajo zahtevo. Generiran simetrični ključ je s javnim ključem prodajalca zaprt v digitalno ovojnico.

3. Odziv je skupaj z digitalno ovojnico in certifikatom plačilnih vrat poslan prodajalcu.

4. Prodajalec najprej preko hierarhije zaupanja preveri certifikat plačilnih vrat, potem pa s svojim privatnim ključem odpre digitalno ovojnico ter s pridobljenim simetričnim ključem dekriptira odziv. Sledi še preverjanje podpisa, s čimer je proces končan.

Shema zajetja plačila je prikazana na Sliki 11.

6 Pomankljivosti in možne izboljšave SET sistema

Kar se tiče elektornskega poslovanja, SET še vedno velja za zgled vsem modelom, ki jim je prioriteta varnost. Kljub dejstvu, da se transakcije izvršujejo preko odprtega omrežja, so prodajalci in kupci varni pred zunanjimi vdori. Prodajalec je zaščiten pred zlonamernimi kupci, ta pa ima zagotovilo, da številka njegove kartice ne bo vidna niti prodajalcu. Poleg medsebojnega zaupanja med prodajalci in kupci je pomembna tudi nizka cena transakcije, kar prinese tudi nižje stroške poslovanja tako za ene kot tudi za druge. Implementirana programska oprema naj bi uporabo sistema poenostavila, tako da je na prvi pogled SET sistem popoln v vseh pogledih. Na žalost pa se tu skriva nekaj pomanklivosti.

Kriptiranje in dekriptiranje v SET sistemu poteka preko RSA in DES algoritma. Zaradi nenehnega razvoja v računalništvu je DES kaj hitro postal lahka tarča napadov. Prvi odzivi na vse hitrejše napade z grobo silo so bili daljši ključi, ki pa so seveda bolj prehodna rešitev. Diferencialna in linearna kriptoanaliza sta skupaj z vse večjo računalniško močjo omogočila še hitrejše napade na DES, zato je bilo povečevanje dolžine ključev nesmiselno. Kljub temu, da SET specifikacije za simetrično kriptiranje predvidevajo DES algoritem, ni nikakršnih ovir, da se le ta zamenja za boljši rešitev, kot sta na primer trojni DES ali pa AES (Advenced Encription Standard), ki sta močnejša algoritma. Na tem mestu bi bil seveda potreben poseg v programsko opremo, ki skrbi za večino operacij kriptiranja pri uporabi SET sistema. Nasploh bi kakršnakoli sprememba izboljšave pomenila novo verzijo programske opreme, kar pa vsakdanjemu uporabniku ne zagotavlja enostavnega ravnanja s sistemom. Seveda za podobnim problemom trpijo vsi sistemi, ki uporabljajo enake simetrične kriptosisteme, kar pa je slaba tolažba za vse uporabnike SET sistema. Po drugi strani pa je ravno zaradi programske opreme možna implementacija podpore PIN kodam, seveda pa bi bile spremembe potrebne pri vseh entitetah.

Omenili smo že, da je SET ogromen in zelo kompleksen sistem, kar posledično izhaja iz kompleksnosti posameznih protokolov. V tipični SET transakciji se izvede več operacij kriptiranja (asimetričnega in simetričnega), digitalnega podpisovanja, preverjanj podpisov ter certifikatov, vse našteto pa procesira programska oprema, s čimer so varnostni mehanizmi pred uporabnikom skriti. Kljub temu, da SET na račun transparentnosti, evidenc in drugih prednosti, ki jih nudi, zmanjša ceno poslovanja, je celoten sistem ravno zaradi obvezne programske opreme (na strani kupca, prodajalca in finančnih inštitucij) in njenega vzdrževanja zelo drag. Tudi upravljanja s certifikati in

celotna infrastruktura, ki stoji za tem, je draga za vzpostavitev in sportno vzdrževanje, kar stroške samo še poveča. Seveda bi kakršnokoli cenitev sistema pomenilo krčanje varnostnih mehanizmov, ravno ti pa so največja odlika SET sistema. Podobno velja za hitrost posamezne transakcije - kakršna koli pohitritev na račun kakega kriptiranja ali preverjanja manj bi pomenila manjšo varnost, s tem pa smisel celotne ideje o kompletnem sistemu.

SET specifikacije pokrijejo večji del celotnega postopka plačevanje s kreditno kartico preko interneta. Plačilna infrastruktura med bankami je neodvisna in preizkušena, tako da tu ni bilo smisla spreminjati principov. Prav tako SET specifikacije ne pokrivajo procesov, kjer ni nevarnosti finančnih prevar, to so predvsem "nakupovalni vozički, ki ne operirajo s finančnimi inštrumenti, in interno poslovanje, ki se spreminja od prodajalca do prodajalca. Vsem pa je skupno hranjenje nekaterih pomembnih podatkov, kot so recimo žetoni zajetja, na lokalnih sistemih. Kljub temu, da za to poskrbi programska oprema, bi kraja teh podatkov pomenila potencialno škodo tako za prodajalce kot tudi za vse, ki so sodelovali v poslih z dotičnim prodajalcem (velja za tako za kupce kot za banke). SET specifikacije ne predvidevajo nikakršnih zahtev za shranjevanje in uničenje tovrstnih podatkov po končanem poslovnem procesu. Na uhajanje le teh pa specificirani varnostni mehanizmi nimajo vpliva.

Še ena zadeva, ki je SET razvijalci niso upoštevali, pa bi vseeno sodila v kontekst kompletnega sistema, je časovno žigosanje. Čas je pomemba informacija, še posebaj če govorimo o transakcijah in podpisovanju dokumentov (kar je na nek način tudi namen SET sistema). Seveda s časovnim žigošanjem pride tudi problem preprečevanja ponaverbe časovnega žiga, bi pa pametno implementirana rešitev preprečila marsikatero tožbo zaradi opravičenih ali neopravičenih zavrnitev transakcij.

7 Zaključek

SET se zaradi pomankljivosti, ki so opisane v poglavju 6, in zaradi globalne popularnosti, predvsem pa enostavnosti SSL protokola, ni uveljavil kot "de-facto" standard za plačevanje s kreditnimi karticami preko interneta, kot je bilo zamišljeno od samega začetka. SSL po drugi strani nikoli ni bil mišljen za podporo elektronskih finančnih transakcij, je pa postal standard za varovanje transakcij nasploh. Tega so se zavedali tudi pri Mastercardu in Visi, ki so po neuspehu SET sistema spet sedli za mizo, tokrat vsak za svojo. Visa je tako razvila koncept 3-D Secure, ki ga trži pod imenom Verified by Visa. Koncept je z nekaj razlikami prevzel tudi Mastercard in ga lansiral pod imenom Master-

card SecureCode. 3-D Secure doda dodaten korak avtentikacije pri spletnem plačevanju (ponavadi je uporabnik preusmerjen na spletno stran izdajatelja kartice, kjer opravi dodaten korak avtentikacije). Koncept temelji na pošiljanju XML dokumentov med tremi domenami: prodajalcem s svojo banko, banko, ki je izdala kartico, in infrastrukturo, ki jo ponuja znamka kreditne kartice. Pošiljanje je varovano s SSL protokolom, ki omogoča avtentikacijo vseh odjemalcev priključenih na sistem, predvsem pa zagotavlja hitrost, enostavnost in neodvisnost od programske opreme (uprabnik potrebuje samo spletni brskalnik). Seveda Verified by Visa in Mastercard SecureCode nista edina načina varnega spletnega plačevanja. Na voljo je še veliko sistemov, večini pa je skupna dvo ali več faktorska avtentikacija. Prvi faktor je ponavadi vrednost, ki si jo uporabnik lahko zapomni in se ne spreminja, druga pa psevdo-naključna vrednost, ki jo ponavadi generira generator psevdo-naključnih vrednosti. Tu ponovno pride na svoj račun kriptografija, vendar si ta tema zasluži samostojen seminar.

Slike

Literatura

[1] *SET Secure Electronic Transaction Specification, Book 1: Business Description*, 1997.

[2] *SET Secure Electronic Transaction Specification, Book 2: ProgrammerŐs Guide*, 1997.

[3] *SET Secure Electronic Transaction Specification, Book 3: Formal Protocol Definition*, 1997.

[4] L. Loeb, *Secure Electronic Transactions - Introduction and Technical Reference*, 1998

[5] RSA Laboratories, *RSAES-OAEP Encryption Scheme - Algorithm specification and supporting documentation*, 2000.

[6] E. Fujisaki, T. Okamoto, D. Pointcheval in J. Stern *RSA-OAEP is Secure under the RSA Assumption*, 2000. Dostopno na: http://eprint.iacr.org/.