Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Kriptografija in računalniška varnost
Podiplomski magisterski študij

ELEKTRONSKI PLAČILNI SISTEMI
(ELECTRONIC PAYMENT SYSTEMS)

Kandidat: **Aleksander Pivk**

Mentor: **prof.dr. Aleksandar Jurišić**

Ljubljana, junij 2000

POVZETEK

Denar so v preteklosti izumili kot abstraktno merilo vrednosti. Zgodovina je prinašala nova in nova merila (od bankovcev do čekov in kreditnih kartic), višek pa dosegamo pri elektronskem plačevanju, ki omogoča poslovanje preko novega poslovnega medija interneta. Najprej so opisani osnovni koncepti kriptografije, ki se dandanes uporabljajo pri elektronskem poslovanju, v nadaljevanju pa se posvečam vprašanjem o varnosti, zanesljivosti, zaupnosti in integriteti, čemur sledi pregled plačilnih shem in sistemov. Nazadnje sta opisana še tehnološki vpogled in napoved za prihodnost, priloga pa nam podaja matematičen opis modernih kriptografskih mehanizmov.

1 UVOD

Prve oblike trgovanja v zgodovini so bile v menjavi blaga, kjer so menjavali blago glede na potrebe. Kasneje je trgovanje postajalo vse bolj zapleteno in pojavil se je denar kot plačilno sredstvo. Vendar se tu razvoj ni končal in imamo danes kar nekaj nadomestil, ki predstavljajo plačilna sredstva (boni, čeki, kreditne kartice, itd.), najnovejša nadomestila pa so sistemi za elektronsko plačevanje.

Tradicionalne načine plačevanja ogrožajo različni, dobro znani varnostni problemi: kraja plačilnih sredstev, ponarejanje podpisov, denarja, čekov..., medtem ko vseh pasti pri elektronskem plačevanju še ne poznamo. Digitalne dokumente lahko poljubno kopiramo, digitalni podpis lahko ustvari vsak, ki pozna prave ključe, tudi anonimnost je večkrat vprašljiv faktor. Potrebni bodo novi mehanizmi, ki bodo omogočali varne transakcije, da se bomo ljudje odločali za tako vrsto nakupov. V tem članku se osredotočam na pregled plačilnih sistemov, kjer je glavna iztočnica njihova varnost.

2 OSNOVNI KONCEPTI KRIPTOGRAFIJE

Najpomembnejša vloga elektronskih plačilnih sistemov je, da pošten kupec prepriča prevzemnika, naj sprejme legitimno plačilo in dodatno zagotoviti varovanje zasebnosti. Na drugi strani pa se mora prevzemnik znati ubraniti nepoštenih kupcev. Pri tem nam močno pomagajo kriptografske sheme, ki pa jih bom tukaj razdelil na dve glavni področji:

- Skupen ključ (simetrični algoritmi – DES; geslo/PIN)
- Javni digitalni podpis (asimetrični algoritmi – RSA in izvedenke)

2.1 Skupen ključ

Kupec in prevzemnik si delita zaupno informacijo, zato da lahko drugi prvemu pooblasti plačilo (simetrična avtentikacija). Opciji, ki se tu pojavljata sta uporaba ali gesla oziroma PIN kode ali skupnega DES ključa (izmenjano po varnem kanalu). Obe strani imata na voljo popolnoma enake zaupne informacije, kar pomeni, da je nemogoče zagotoviti zavračanje nepristnih sporočil (v primeru, da se kupec in prevzemnik ne strinjata okoli določenega plačila, ne moremo dokazati, kdo je odgovoren za kritje nastalih stroškov). Ta način plačevanja ni primeren takrat, ko mora kupec nositi breme, ki ga povzročijo goljufi (še posebej pri velikih zneskih). V primeru, ko izvajamo avtentikacijo v nepovezanih sistemih (primerno za plačevanje manjših vrednosti), ima prevzemnik pri sebi glavni ključ (master key), ki mu omogoča, da izpelje kupčev ključ iz njegove identitete. Sporočilo preverimo tako, da izračunamo razpršilno vrednost funkcije sporočila in zaupne informacije, ki jo imenujemo MAC (Message Authentication Code).

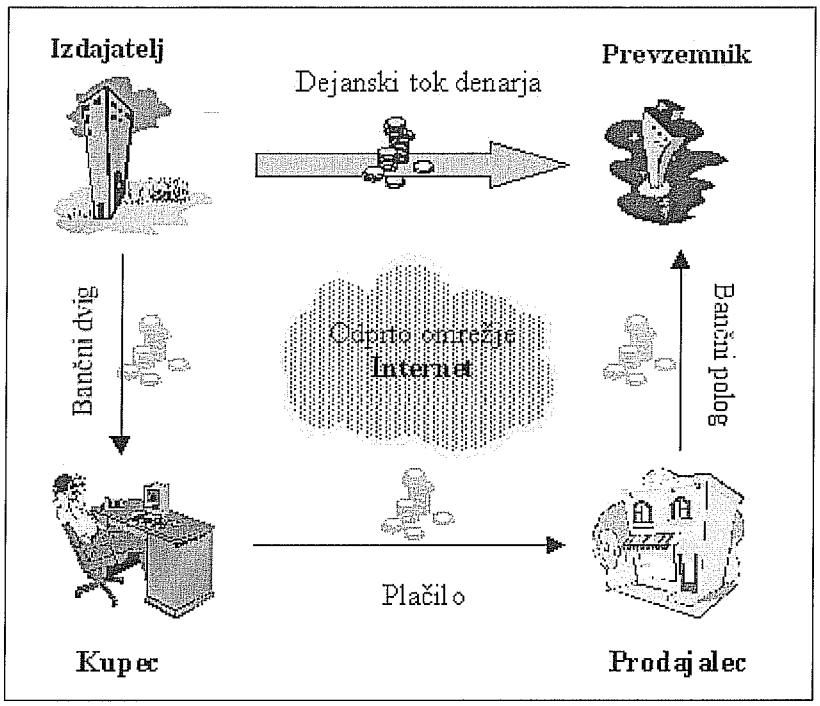
2.2 Javni digitalni podpis

Kupec in prodajalec imata vsak svoj par javni/zasebni ključ, ki jima ga izda ustanova za izdajanje digitalnih certifikatov. Javni ključ je bolje znan kot overitveni ključ, zasebni pa kot podpisovalni ključ. S tem parom vsak izkazuje svojo pristnost in odgovornost. Večina

- **Sprejemljivost** – plačilna infrastruktura mora biti dostopna vsakomur in široko sprejeta. V primeru, da dobiš plačilo v obliki digitalnega denarja, lahko z njim poljubno razpolagaš ali pa ga kje varno shraniš.
- **Učinkovitost** – stroški transakcij se morajo minimizirati. Finančne institucije zaračunavajo določene odstotke pri nakupih s kreditnimi karticami, kar pa je nesprejemljivo v primeru mikroplačil.
- **Uporabnost** – plačevanje mora biti tako preprosto kot v realnem svetu. Uporabniki morajo imeti možnost omejevanja izgube z določanjem zgornjega pragu vrednosti nakupa, preprosto mora biti nadziranje plačil, prav tako mora biti omogočena avtomatizacija plačil.
- **Varnost** – najpomembnejša vprašanje pri digitalnem plačevanju, ker omogoča podporo finančnim transakcijam preko interneta. Pasivnih in aktivnih prisluškovalcev se na omrežju ne manjka, zato so potrebne tehnološke rešitve kot so digitalni podpis, digitalni certifikat in drugi kriptografski mehanizmi.
- **Zanesljivost** – plačilni sistem naj bi bil odporen do napak. Plačilne transakcije morajo biti *atomske*, kar pomeni da so lahko ali sprejete ali zavrnjene, vmesno neznano ali nekonsistentno stanje pa ni mogoče. Noben plačnik ne bi sprejel možnosti, da se je denar izgubil nekje na internetu. Poseben primer tu predstavljajo zrušeni sistemi, vendar bomo mi privzeli, da obstajajo specifični sinhronizacijski postopki, ki rešujejo nekonsistentne situacije.

Poseben problem pa predstavlja še avtorizacija, ki se dandanes rešuje na 3 načine:

- **Zunanja avtorizacija** – stranka za overjanje (tipično banka) pošlje opozorilo kupcu, da naj potrdi ali zavrne svoje plačilo preko varnega zunanjega kanala (navadna pošta, telefonski klic). To je tipičen pristop pri poštnem ali telefonskem naročanju. Pri tem načinu lahko vsak, ki pozna podatke s tuje kreditne kartice, kupuje v njegovem imenu. Lastnik kartice mora redno pregledovati bančne izpise in se na napačne transakcije pritožiti. Po preteku določenega časa (90 dni), se na napačne transakcije ni več možno pritožiti.
- **Avtorizacija z geslom** - stranka za overjanje zahteva, da vsako sporočilo kupca vključuje vrednost razpršilne funkcije (MAC) izračunano iz sporočila in tajnega ključa, ki jih poznata samo omenjeni stranki. S tem dosežemo varnost proti zunanjim napadalcem, še vedno pa ne zagotavlja *ne-zavračanja pristnega sporočila*: iz sporočila se ne da določiti, ali je dvoumno sporočilo avtentificiral kupec ali nepošten bančni uslužbenec. Kratki ključi (4-6 številčni PIN) so zelo občutljivi na razne vrste napadov in zato sami ne morejo zagotavljati visoke stopnje varnosti. Dober način uporabe bi bil lahko kot kontrolni dostop do pametne kartice (e-denarnice), ki temelji na varnih kriptografskih mehanizmih.
- **Avtorizacija z digitalnim podpisom** - stranka za overjanje vedno zahteva digitalno podpisano sporočilo. Ta zagotavlja *ne-zavračanje pristnega sporočila*: samo lastnik zasebnega ključa lahko podpiše sporočilo (z javnim ključem pa lahko preverimo verodostojnost podpisanega sporočila). Reševanja razprav o avtentikaciji sporočil so tako dosti bolj poštena in enostavna.



Slika 1: Splošna denarna shema (plačaj vnaprej)

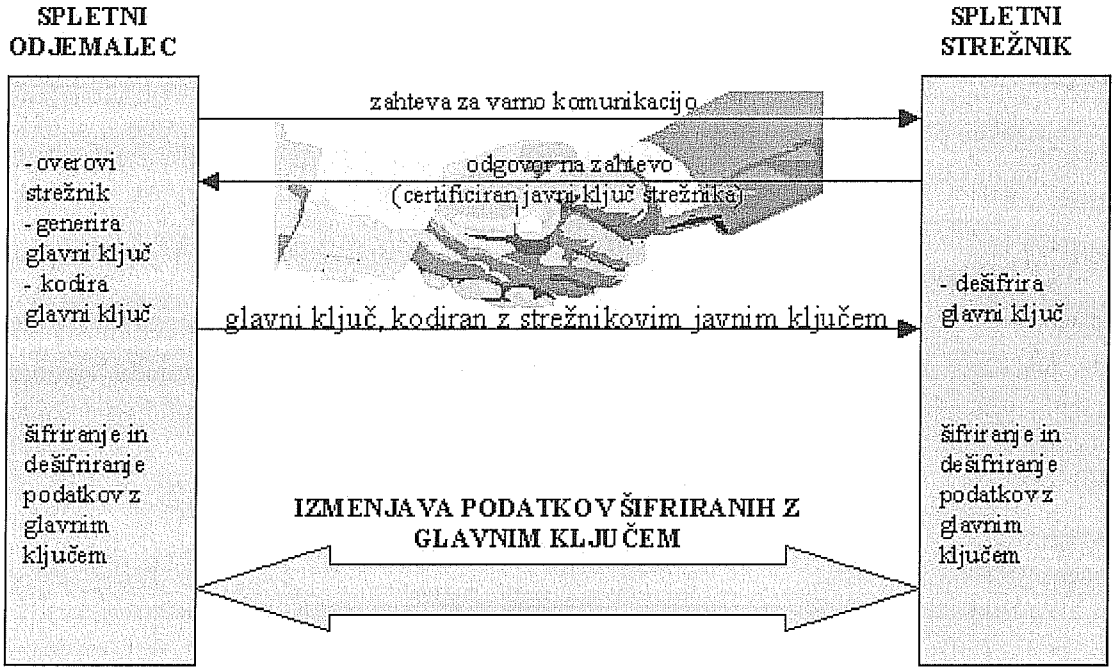
V ta razred spadajo elektronske denarnice, ki temeljijo na pametnih karticah, elektronski denar in potrjeni digitalni čeki. Najbolj poznane rešitve pa so: DigiCash eCash (zelo dober model – slepi podpis), NetCash (ni več v uporabi), CyberCoins (za nakupe do $10, ni več v uporabi), IBM Micro Payment (v pilotski fazi, zahteva posredovanje ponudnika dostopa do interneta), MilliCent (ne zagotavlja anonimnosti), Mondex (uporablja Value Tansfer Protocol, ki zagotavlja močno kriptografijo pri zaščiti prenosa denarja), GeldKarte (deluje le v Nemčiji, zelo nizki transakcijski stroški) in VisaCash (v prototipni fazi, uporabljena na OI v Atlanti).

4.2 Plačaj na mestu

Deluje na principu debetnih kartic, ki se od kreditnih kartic razlikujejo v tem, da na sprednji strani nimajo odtisnjenih nobenih podatkov. Plačevanje zahteva napravo, ki bere magnetni zapis, poznati moramo pa še PIN, ki služi kot avtorizacija. Pri tem načinu se kupcu trga denar z bančnega računa neposredno ob nakupu. Dobra lastnost tega je, da se zmanjšajo možnosti za goljufanje, slabost pa, da je veliko težje vrniti kupljeno blago, ker je transakcija že opravljena. Ta sistem bo zelo težko globalno zaživel, ker ni dovolj standardov, ki bi podpirali neposredno trganje s tujega bančnega računa, lahko pa živi na lokalnem nivoju. Znana predstavnika sta BankNet in FSTC Electronic Check.

4.3 Plačaj kasneje

Najbolj razširjena in uveljavljena shema za plačevanje, ki jo vsi poznamo kot kreditna kartica. Prednosti tega sistema so, da je sprejet globalno, da je neodvisen od valute in da omogoča vračanje kupljenega blaga znotraj časovnega okvira. Za varno plačevanje s kreditnimi karticami sta bila sprejeta dva standarda (SSL in SET), ki sta opisana v naslednjem poglavju. Najbolj poznane rešitve s kreditnimi karticami so: WireCard (Java applet šifrira podatke z uporabo RSA in BlowFish algoritma, dolžina ključa je 2048 bitov), CyberCash (deluje



Slika 3: Shematičen prikaz varnostnega protokola SSL

V prvi fazi odjemalec pošlje strežniku zahtevo za varno komunikacijo. Ta se predstavi s svojim certifikatom in javnim ključem. Odjemalec nato ustvari glavni ključ, ga šifrira s strežnikovim javnim ključem ter vrne strežniku. Le-ta dešifrira glavni ključ ter potrdi svojo identiteto tako, da pošlje odjemalcu naključno sporočilo šifrirano z glavnim ključem. Pri opcijski fazi (overovljanje odjemalca) pošlje strežnik naključno sporočilo odjemalcu, ki se na sporočilo podpiše ter vse skupaj s svojim certifikatom vrne strežniku. Opis delovanja nam prikazuje slika 3.

5.2 *i*KP (*i*-Keyed Protocol)

Protokol so razvili pri podjetju IBM Research v začetku leta 1995 in je predhodnik standarda SET. Vsi protokoli *i*KP (i = 1..3) temeljijo na javni kriptografiji, med seboj pa se razlikujejo v številu udeležencev (max. 3), ki imajo v lasti par javni/zasebni ključ in se lahko digitalno podpisujejo.

Najpreprostejši je protokol *1KP*, ki zahteva, da ima le prevzemnik digitalni certifikat in ustrezne ključe, medtem ko imata kupec in prodajalec le njegov javni ključ. Avtorizacija plačevanja je realizirana s številko kreditne kartice in pripadajočo PIN številko, ki se primerno šifrirana in opremljena z ostalimi podatki o nakupu pošlje do prevzemnika. *1KP* ne podpira ne-zavračanja sporočil poslanih od kupcev ali prodajalcev.

Pri naslednjem protokolu *2KP* ima poleg prevzemnika digitalni certifikat in ustrezne ključe še prodajalec. Dobra lastnost te vrste je, da kupec lahko vedno preveri verodostojnost prodajalca, brez posredovanja drugih strank. Avtorizacija plačevanja poteka isto kot pri *1KP*. *2KP* podpira ne-zavračanje sporočil poslanih od prodajalcev.

5.4 E-cash

Razvilo ga je podjetje DigiCash, ki se ukvarja z anonimnim elektronski denarjem. Ta sistem zagotavlja visoko stopnjo anonimnosti in nesledljivosti. Temelji na kriptografskem konceptu slepega podpisa, ki je podrobneje opisan v prilogi.

Pri dvigu kovancev, je treba najprej pripraviti »prazne kovance« (naključne serijske številke), te skriti v ovojnico in poslati banki v potrditev. Ko banka odobri prenos denarja z bančnega računa v digitalno obliko, kovance podpiše preko ovojnice (serijska številka vsakega kovanca ostane banki skrita) in jih vrne kupcu. Kupec odpre ovojnico z javnim ključem banke in veljavne e-kovance shrani na trdi disk ali pametno kartico. Plačilo se izvede tako, da prodajalec prejete kovance pošlje banki, ta shrani serijske številke v svoji bazi in vrne prodajalcu ustrezno avtorizacijo. Na ta način banka prepreči večkratno potrošnjo istega kovanca. Kovance, ki jih banka sprejme ne more prepoznati, prepozna lahko le podpis, s katerim je podpisala digitalno ovojnico. Dobra lastnost tega sistema je, da lahko z njimi plačujemo tudi drugim uporabnikom.

5.5 μ-*i*KP (*i*-Keyed Protocol)

Mikroplačila so plačila majhnih vrednosti, ki morajo biti opravljena hitro, transakcijski stroški pa morajo biti minimalni. Shema je primerna le pri ponavljajočih plačilih, ker so nastavitveni stroški dokaj visoki, transakcijski pa nizki. Ta protokol temelji na varnih enosmernih razpršilnih funkcijah (funkcija f je enosmerna, če je težko poiskati vrednost x, za znano vrednost $y=f(x)$). Kupec si mora izbrati osnovno vrednost x, nadaljnje vrednosti pa se računajo po rekurzivni formuli:

1. $A^0(x)=x$
2. $A^{i+1}=f(A^i(x))$

Vrednosti od $A^0,\ldots, A^{n-1}$, znane kot *kuponi*, omogočajo, da lahko kupec opravi n mikroplačil fiksne vrednosti v natanko enemu prodajalcu na naslednji način. Prvič, kupec pošlje A^n in v do prodajalca na varen način. Ta si prek svoje banke zagotovi, da se A^n nanaša na verigo, ki jo bo kupec kasneje uporabil za plačevanje. Mikroplačila potem izvajamo tako, da po vrsti prodajalcu razkrivamo vrednosti A^{n-1}, A^{n-2}, ... , A^0. Poravnava se izvrši tedaj, ko prodajalec svoji banki predstavi delno verigo $A^i .. A^j$ $(0\leq i\leq j\leq n)$ in zahteva znesek $v*(j-i)$.

Znana predstavnika v tej skupini sta NetBill in NetCheque, ki temeljita na Kerberos tehnologiji skupnih ključev. Pri naši opredelitvi spadata v čekovno shemo. Uporaba tehnologije skupnih ključev je opravičljiva zaradi zahteve po procesiranju množice mikroplačil v majhnem času, vendar je bilo objavljeno, da se bosta sistema oprla na tehnologijo javnih ključev.

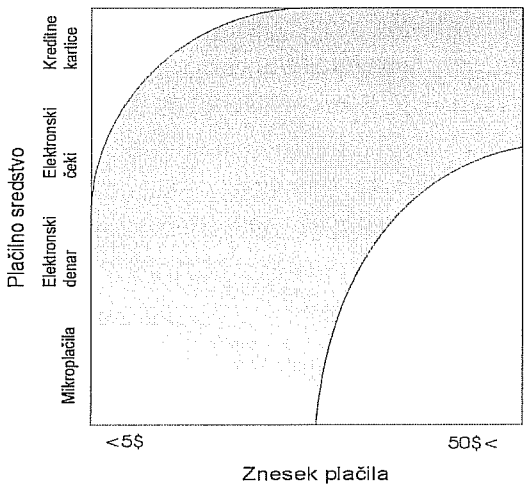
6.2 Varno strojna oprema

Večina nepovezanih sistemov zahteva pri svojem delovanju posebno napravo na strani kupca, ki preprečuje ponarejanje, da se zagotovijo varnostne zahteve bank. Prav tako pa mora biti v interesu kupca, da ima pri sebi napravo, ki varno operira z zasebnimi ključi in opravlja finančne transakcije. Na začetku je to lahko pametna kartica, ki pa naj bi sčasoma postala pametna naprava z varnim dostopom do majhne tipkovnica in zaslona. Temu lahko rečemo tudi *elektronska denarnica.* Brez takšne naprave, so kupčevi zasebni ključi in posredno njegov denar, dostopni vsakomur, ki lahko dostopi do njegovega računalnika. To pa je v današnjem več-uporabniškem okolju nesprejemljivo. Seveda pa je ogrožen tudi eno-uporabniški računalnik, do katerega se lahko posredno ali neposredno dostopa. Na primer, podtaknjen virus nam lahko pri vnosu ukrade PIN kode in zaščitna gesla, nato pa neposredno prosi pametno kartico, naj sprovede plačilo na nek tuj račun. Pomeni, da za pravo varnost, potrebujemo tudi zanesljive vhodno/izhodne kanale med uporabnikom in pametno kartico.

6.3. Stroški, varnost, hitrost

Plačilne sheme, ki omogočajo plačevanje velikih zneskov, so zgrajene tako, da zagotavljajo veliko varnost elektronskih transakcij. To se odraža na velikem začetnem kapitalskem vložku ter vzdrževanju le-teh, kar pomeni, da so predrage za plačevanje majhnih zneskov. Za plačevanje različno velikih zneskov se zato uporabljajo različne plačilne sheme, ker te predstavljajo kompromis med stroški, varnostjo in hitrostjo.

Graf 1 predstavlja, katera plačila so najbolj primerna za plačevanje zneskov glede na njihovo višino. Za majhne zneske je priporočljivo uporabiti mikroplačila in elektronski denar, za plačevanje večjih zneskov pa sta priporočljivejša elektronski ček in kreditne kartice.



Graf 1: Plačilne sheme glede na znesek plačila

http://www.zurich.ibm.com/Technology/Security/publications/1999/BGHHKSTHW99.ps.gz

[10] A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[11] J.-P. Boly, A. Bosselaers, R. Cramer, R. Michelsen, S. Mjoslnes, F. Muller, T. Pedersen, B. Pfitzmann, P. Rooij, B. Schoenmakers, M. Schunter, L. Vallee and M. Waidner, The ESPIRIT Project CAFE – High Security Digital Payment Systems, ESORICS '94, LNCS 875, Springer-Verlag, Berlin 1994, pp.217-230, http://www.semper.org/sirene/publ/BBCM1_94CafeEsorics.ps.gz

[12] Mastercard, SET Specification, http://www.mastercard.com/shoponline/set/index.html

[13] DigiCash e-Cash, http://www.digicash.com

[14] First Virtual, http://www.fv.com

[15] CyberCash, http://www.cybercash.com

[16] FSTC Electronic Check, http://www.echeck.org

[17] Millicent, http://www.millicent.digital.com

[18] Netscape, SSL Protocol, http://home.netscape.com/eng/ssl3/ssl-toc.html

[19] NetBill, The NetBill Electronic Commerce Project, 1995, http://www.ini.cmu.edu/netbill/home.html

[20] Mondex, http://www.mondex.com

[21] SEMPER, http://www.semper.org

[22] NetCheque, http://nii-server.isi.edu/info/NetCheque/

[23] IBM's Internet Keyed Payment (iKP) System: http://www.zurich.ibm.com:80/Technology/Security/extern/ecommerce/iKP.html

[24] Semper's links list: http://www.semper.org/sirene/pointers_complete.html

[25] R.J. Anderson, Why Cryptosystems Fail, Communications of the ACM 37/11 (1994) pp.32-40.

Generiranje ključa

Vsaka oseba mora kreirati javni ključ in pripadajoči zasebni ključ:

1. Izberi praševilo q, da $2^{159}<q<2^{160}$ (velikost q je 160 bitov, velikost p vsaj 768 bitov).
2. Izberi t, da $0 \le t \le 8$, in izberi praštevilo p, kjer $2^{511+64t}<p<2^{512+64t}$ in $q \mid (p-1)$.
3. Izberi generator α iz enolične ciklične grupe reda q v Z_p^*
   a) Izberi element $g \in Z_p^*$ in izračunaj $\alpha = g^{(p-1)/q} \bmod p$ (ponavljaj dokler $\alpha = 1$)
4. Izberi naključno število a, tako da velja $1 \le a \le q-1$
5. Izračunaj $y = \alpha^a \bmod p$
6. Javni ključ sestavljajo (p, q, α, y), zasebni ključ pa je a.

Generiranje podpisa in verifikacija

A podpiše sporočilo m poljubne dolžine. B lahko preveri podpis z uporabo A-jevega javnega ključa.

Generiranje ključa (A naredi naslednje):

1. Izbere naključno število k, da $0 < k < q$
2. Izračuna $r = (\alpha^k \bmod p) \bmod q$
3. Izračuna $k^{-1} \bmod q$
4. Izračuna $s = k^{-1}\{h(m) + ar\} \bmod q$
5. Par (r,s) predstavlja ključ osebe A

Verifikacija ključa (B mora naredi naslednje):

1. Pridobi avtentičen javni ključ (p, q, α, y)
2. Preveri, da 0 < r < q in 0 < s < q, drugače zavrne podpis
3. Izračunaj $w = s^{-1} \bmod q$ in $h(m)$
4. Izračunaj $u_1 = w \cdot h(m) \bmod q$ in $u_2 = rw \bmod q$
5. Izračunaj $v = (\alpha^{u_1} y^{u_2} \bmod p) \bmod q$
6. Sprejmi podpis le v primeru, da $v = r$.

9.3 SHA-1 (The Secure Hash Algorithm)

Algoritem temelji na MD4 (Message Digest) in ga je predlagal ameriški inštitut za standarde in tehnologijo (NIST). Lastnosti algoritma so:

- Razpršena vrednost je 160-bitna, algoritem pa uporablja 5 32-bitnih verižnih spremenljivk
- Funkcija stiskanja je sestavljena iz 4 faz, MD4 postopkovne funkcije f, g in h pa uporablja takole: f v prvi fazi, g v tretji, h pa v drugi in četrti. Vsaka faza ima 20 korakov.
- Znotraj stiskalne funkcije se vsak 16-besedni blok razširi v 80-besednega. Zadnjih 64 besed je XOR z 4 besedami prejšnje pozicije razširjenega bloka (prikazuje spodnja formula). Teh 80 besed je nato posamezno vhod vsem fazam.

  $$X[j] = (X[j-3] \oplus X[j-8] \oplus X[j-14] \oplus X[j-16]) \leftarrow 1, \text{ kjer je } 16 \le j \le 79$$

- Algoritem uporablja 4-neničelne konstante

Algoritem MD4 je bil razvit posebej za implementacijo programov na 32-bitnih računalnikih. Pri delu z nizi besed uporablja princip *big-endian*. Kot izhod dobimo 160-bitno razpršeno

PRILOGA 2: Specifikacija protokola SET za varno plačevanje

Udeleženci plačilne sheme SET so naslednji:

- *Kupec* (Cardholder): izvajalec nakupa, ki plačuje s plačilno kartico.
- *Izdajatelj* (Issuer): finančna ustanova, ki izdaja plačilne kartice kupcem.
- *Prodajalec* (Merchant): ponuja blago ali storitve v zameno za plačilo.
- *Prevzemnik* (Acquirer): finančna ustanova, ki odpira bančne račune prodajalcem, izvaja avtorizacijo in prenos plačil.
- *Plačilni posrednik* (Payment Gateway): naprava, ki jo upravlja prevzemnik, ki procesira plačilna sporočila prodajalcev.
- *Ustanova za izdajanje in overovitev certifikatov* (UIOC): pooblaščena stranka, ki legitimnim prosilcem izdaja certifikate, po potrebi pa jih tudi overja.

SET opredeljuje sedem glavnih poslovnih zahtev:

1. Zagotavlja zaupnost informacij o plačilu o naročilu.
2. Zagotavlja neokrnjenost razposlanih podatkov.
3. Zagotavlja overovitev kupca, da je ta upravičen uporabnik bančnega računa.
4. Zagotavlja overovitev prodajalca, da ta lahko sprejema plačila s plačilnimi karticami preko prevzemne finančne ustanove.
5. Jamči uporabo najbolj zanesljivih sistemov in tehnik za zagotavljanje varnosti vključenih strank v transakcije e-poslovanja.
6. Kreira protokol, ki ni odvisen od prenosa varnostnih mehanizmov niti ne preprečuje njihove uporabe.
7. Pospešuje in spodbuja interoperabilnost med dobavitelji mrežne, strojne in programske opreme.

Proces elektronskega nakupovanja lahko razdelimo na naslednje stopnje:

1. Kupec išče želene izdelke na različne načine:
    - s pomočjo brskalnika si na spletu ogleduje spletne kataloge prodajalcev
    - ogleduje si katalog prodajalca na CD-ROM-u
    - ogleduje si papirno izdajo kataloga
2. Kupec si izbere izdelke, ki bi jih želel kupiti.
3. Kupcu je predstavljena naročilnica, ki vsebuje izbrane izdelke, njihove cene in skupno ceno, iz katere so razvidni stroški pošiljanja in davčne pristojbine.V določenih primerih, je mogoče tudi pogajanje za ceno izdelkov.
4. Kupec si izbere način plačila. V našem primeru nas zanima samo plačevanje s kartico.
5. Kupec pošlje prodajalcu izpolnjeno naročilo skupaj z navodili za plačilo.
6. Prodajalec zahteva avtorizacijo od kupčeve finančne ustanove.
7. Prodajalec pošlje kupcu potrdilo o naročilu.
8. Prodajalec dostavi na najbolj primeren način kupljeno blago kupcu.
9. Prodajalec zahteva plačilo od kupčeve finančne ustanove.

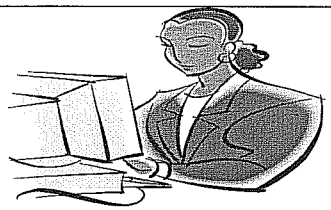
Čeprav smo te stopnje našteli v določenem zaporedju, to ne pomeni, da se vedno tako tudi razvrstijo. Možno so določena odstopanja, v katera se tukaj ne bomo spuščali. V našem primeru se bomo predvsem osredotočili na faze 5, 6, 7 in 9, ko se kupec dejansko odloči za nakup s plačilno kartico.

Protokol SET definira vrsto transakcijskih protokolov, ki uporabljajo kriptografske koncepte za izvajanje varnih transakcij elektronskega poslovanja. Tu se bomo osredotočili na faze 5, 6, 7 in 9, ki jih opisujejo naslednje faze:

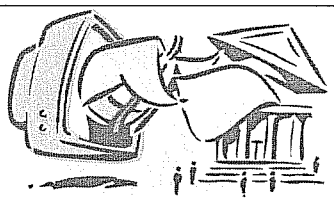
a) Registracija kupca pri UIOC
b) Registracija prodajalca pri UIOC
c) Zahteva za nakup
d) Avtorizacija plačila
e) Zajem plačila

Vse te faze so podrobneje opisane v nadaljevanju. Pri podrobnem opisu transakcij lahko opazimo tudi debelejše označen tekst, ki označuje, da tisti korak zahteva sodelovanje uporabnika (vnos). Vsi ostali koraki pa predstavljajo popolnoma avtomatiziran proces, ki v najslabšem primeru vključujejo le minimalno pomoč uporabnika (pritisk na gumb, potrditev sporočila, ipd.)

A) REGISTRACIJA KUPCA PRI USTANOVI ZA IZDAJANJE IN OVERITEV CERTIFIKATOV



KUPEC



UIOC

1. Kupec pošlje začetno zahtevo za registracijo.

začetna zahteva →

2. Sprejme začetno zahtevo kupca.

3. Generira odgovor, ki ga šifrira s svojim javnim ključem in digitalno podpiše s pomočjo izračuna razpršene vrednosti (MD4).

← odgovor + certifikati

4. UIOC pošlje kupcu odgovor skupaj s svojimi certifikati.

5. Kupec prejme odgovor in verificira certifikate do korena drevesa zaupnih entitet.

6. Kupec preveri podpis, tako da odgovor dešifrira z javnim ključem UIOC in rezultat primerja z novo generirano razpršeno vrednostjo odgovora.

7. **Kupec vnese številko svojega računa.**

8. Kreira se zahteva za registracijski obrazec.

9. Sporočilo se šifrira z naključno generiranim simetričnim ključem (#1). Ta ključ se skupaj s številko računa šifrira z javnim ključem UIOC

10. Kupec pošlje šifrirano zahtevo za registracijski obrazec do UIOC.

zahteva za registracijski obrazec →

11. Dešifrira simetrični ključ (#1) in kupčevo številko računa s svojim zasebnim ključem, s pomočjo simetričnega ključa pa nato dešifrira še zahtevo za registracijski obrazec.

12. Razbere primeren registracijski obrazec in ga digitalno podpiše s pomočjo razpršene vrednosti obrazca, šifrira pa ga s svojim zaupnim ključem.

← registracijski obrazec

13. Pošlje registracijski obrazec in certifikat.

14. Prejme registracijski obrazec, certifikate verificira do korena drevesa zaupnih entitet.

15. Overovitev podpisa obrazca se izvede z dešifriranjem z javnim ključem UIOC in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

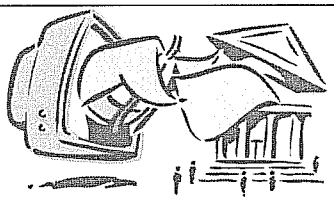
16. Kupec kreira par ključev (javni/zasebni).

17. **Kupec izpolni registracijski obrazec.**

18. Kupec kreira zahtevo za certifikat, kamor vključi podatke z registracijskega obrazca.

19. Kupec kreira sporočilo z zahtevo, javnim ključem in novo generiranim simetričnim ključem (#2); digitalni podpis se izvede s pomočjo vrednosti razpršene funkcije zahteve, šifriranje pa s kupčevim zasebnim ključem.

KUPEC



UIOC

20. Sporočilo se šifrira z naključno generiranim simetričnim ključem (#3). Ta ključ se skupaj s podatki o bančnem računu, šifrira z javnim ključem UIOC.

21. Pošlje šifrirano sporočilo z zahtevo za certifikat.

zahteva za certifikat →

22. Z zasebnim ključem se iz sporočila dešifrirajo simetrični ključ (#3) in podatki o bančnem računu; zahteva za certifikat pa se nato dešifrira s simetričnim ključem (#3).

23. Overovitev kupčevega podpisa zahteve se izvede z dešifriranjem z javnim ključem kupca in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

24. Overitev zahteve za certifikat se izvede s pomočjo podatkov o bančnem računu in informacij iz registracijskega obrazca.

25. Kreira se certifikat kupca, digitalno podpisan z zasebnim ključem UIOC.

26. UIOC generira odgovor s certifikatom, ki se digitalno podpiše s pomočjo vrednosti razpršene funkcije odgovora, šifrira pa z zasebnim ključem.

27. Šifriranje odgovora s certifikatom se izvede s simetričnim ključem (#2) iz kupčeve zahteve za certifikat.

← odgovor s certifikatom

28. Pošlje odgovor kupcu.

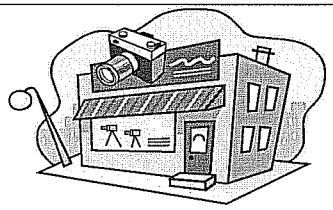
29. Prejme odgovor, certifikat se verificira do korena drevesa zaupnih entitet.

30. Kupec dešifrira odgovor s pomočjo simetričnega ključa (#2) – korak 19.

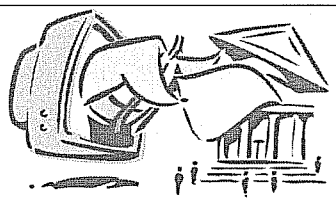
31. Overovitev podpisa odgovora se izvede z dešifriranjem z javnim ključem UIOC in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

32. Kupec shrani certifikat in informacije iz odgovora za nadaljnje potrebe e-trgovanja.

B) REGISTRACIJA PRODAJALCA PRI USTANOVI ZA IZDAJANJE IN OVERITEV CERTIFIKATOV



PRODAJALEC



UIOC

1. Prodajalec pošlje začetno zahtevo za registracijo.

začetna zahteva →

2. Sprejme začetno zahtevo prodajalca.

3. Razbere primeren registracijski obrazec in ga digitalno podpiše s pomočjo razpršene vrednosti obrazca, šifrira pa ga s svojim zaupnim ključem.

← registracijski obrazec

4. Pošlje registracijski obrazec in certifikat.

5. Prejme registracijski obrazec, certifikate verificira do korena drevesa zaupnih entitet.

6. Overovitev podpisa obrazca se izvede z dešifriranjem z javnim ključem UIOC in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

7. Prodajalec kreira 2 para ključev (javni/zasebni). En par služi za šifriranje, drugi za digitalno podpisovanje.

8. **Prodajalec izpolni registracijski obrazec.**

9. Prodajalec kreira zahtevo za certifikat.

10. Prodajalec kreira sporočilo z zahtevo in obema javnima ključema; digitalni podpis se izvede s pomočjo vrednosti razpršene funkcije zahteve, šifriranje pa z zasebnim ključem.

11. Sporočilo se šifrira z naključno generiranim simetričnim ključem (#1). Ta ključ se skupaj s podatki o bančnem računu, šifrira z javnim ključem UIOC.

12. Pošlje šifrirano sporočilo z zahtevo za certifikat.

zahteva za certifikat →

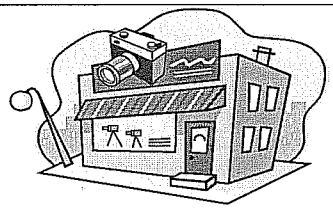
13. Z zasebnim ključem se iz sporočila dešifrirajo simetrični ključ (#1) in podatki o bančnem računu; zahteva za certifikat pa se dešifrira s simetričnim ključem (#1).

14. Overovitev prodajalčevega podpisa zahteve se izvede z dešifriranjem z javnim ključem prodajalca in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

15. UIOC potrdi zahtevo za certifikat glede na podatke o prodajalcu.

16. Kreirajo se certifikati prodajalca, digitalno podpisani z zasebnim ključem UIOC.

17. UIOC generira odgovor s certifikatom, ki se digitalno podpiše s pomočjo vrednosti razpršene funkcije odgovora, šifrira pa z zasebnim ključem.



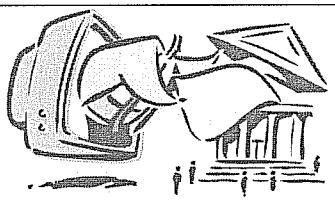
PRODAJALEC

19. Prejme odgovor, certifikat se verificira do korena drevesa zaupnih entitet.

20. Overovitev podpisa odgovora se izvede z dešifriranjem z javnim ključem UIOC in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

21. Prodajalec shrani certifikat in informacije iz odgovora za nadaljnje potrebe e-trgovanja.

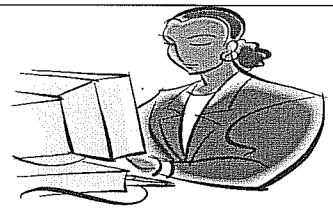
odgovor s certifikatom



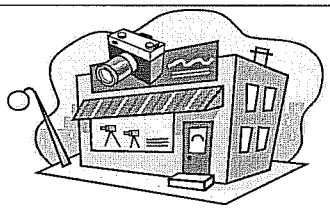
UIOC

18. Pošlje odgovor prodajalcu.

C) ZAHTEVA ZA NAKUP



KUPEC



PRODAJALEC

1. **Kupec nakupuje.**
2. Kupec pošlje začetno zahtevo za nakup.

začetna zahteva →

3. Sprejme začetno zahtevo kupca.
4. Kreira odgovor in ga digitalno podpiše s pomočjo razpršene vrednosti odgovora, šifrira pa ga s svojim zaupnim ključem.

← odgovor + certifikati

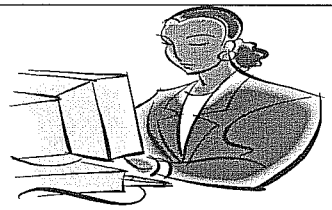
5. Pošlje kupcu odgovor skupaj s svojim certifikatom in certifikatom plačilnega posrednika.
6. Prejme odgovor, certifikate verificira do korena drevesa zaupnih entitet.
7. Overovitev podpisa prodajalca se izvede z dešifriranjem z javnim ključem prodajalca in primerjavo rezultata z novo generirano razpršeno vrednostjo odgovora.
8. Kupec kreira in izpolni naročilo. (ON)
9. **Kupec izpolni obrazec za plačilo. (OP)**
10. Dualni digitalni podpis nad ON in OP se izvede z razbitjem zlepka razprešenih vrednosti ON in OP, dualno razbitje pa se šifrira s zasebnim ključem.
11. Obrazec OP se šifrira z naključno generiranim simetričnim ključem (#1). Ta ključ se skupaj s podatki o bančnem računu kupca, šifrira z javnim ključem plačilnega posrednika.
12. Pošlje obrazec ON in šifriran obrazec OP do prodajalca.

obrazca ON in OP →

13. Prejme obrazca, certifikate verificira do korena drevesa zaupnih entitet.
14. Overitev kupčevega dualnega podpisa obrazca ON se izvede z dešifriranjem s kupčevim javnim ključem in primerjavo rezultata z novo generirano razpršeno vrednostjo zlepka razpršenih vrednosti obrazcev ON in OP.
15. **Prodajalec preda zahtevo (skupaj z obrazcem OP) plačilnemu posredniku za avtorizacijo.**
16. Generira odgovor o nakupu (vključuje tudi njegov certifikat), odgovor digitalno podpiše s pomočjo vrednosti razpršene funkcije, šifrira pa z zasebnim ključem.
17. Pošlje odgovor o nakupu.

← odgovor o nakupu

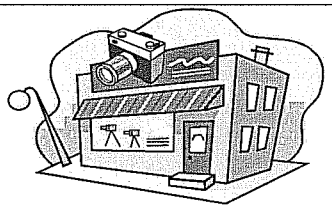
18. **Če je transakcija odobrena, prodajalec izpolni naročilo (npr. pošlje blago)**
19. Prejme odgovor, certifikat se verificira do korena drevesa zaupnih entitet.



KUPEC

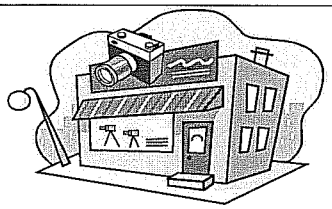
20. Overovitev podpisa odgovora se izvede z dešifriranjem z javnim ključem prodajalca in primerjavo rezultata z novo generirano razpršeno vrednostjo le-tega.

21. Kupec shrani odgovor o nakupu.



PRODAJALEC

D) AVTORIZACIJA PLAČILA



PRODAJALEC

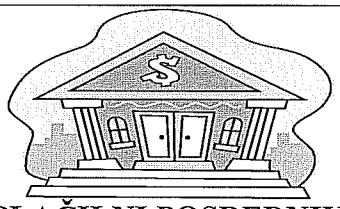
1. Kreira zahtevo za avtorizacijo.

2. Prodajalec digitalno podpiše zahtevo s pomočjo njene razpršene vrednosti, šifrira pa jo s svojim zaupnim ključem.

3. Zahteva se šifrira z naključno generiranim simetričnim ključem (#2). Ta ključ se šifrira z javnim ključem plačilnega posrednika.

4. Pošlje šifrirano zahtevo za avtorizacijo in šifriran obrazec OP kupčeve zahteve za nakup.

zahteva za avtorizacijo in obrazec OP →



PLAČILNI POSREDNIK

5. Certifikate prodajalca verificira do korena drevesa zaupnih entitet.

6. Z zasebnim ključem se dešifrira simetrični ključ (#2), s katerim pa se dešifrira zahtevo.

7. Overovitev podpisa prodajalca se izvede z dešifriranjem z javnim ključem prodajalca in primerjavo rezultata z novo generirano razpršeno vrednostjo zahteve.

8. Certifikat kupca verificira do korena drevesa zaupnih entitet.

9. Z zasebnim ključem se dešifrirajo simetrični ključ (#1) in kupčeve informacije o bančnem računu. S simetričnim ključem (#1) se dešifrira obrazec OP.

10. Overitev kupčevega dualnega podpisa obrazca OP se izvede z dešifriranjem s kupčevim javnim ključem in primerjavo rezultata z novo generirano razpršeno vrednostjo zlepka razpršenih vrednosti obrazcev ON in OP.

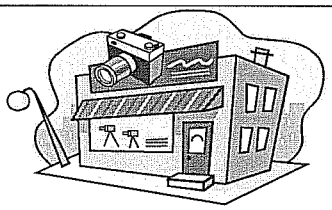
11. Zagotovljena je konsistentnost med prodajalčevo zahtevo za avtorizacijo in kupčevim obrazcem OP.

12. Pošlje se zahteva za avtorizacijo preko finančnega omrežja do kupčeve finančne ustanove.

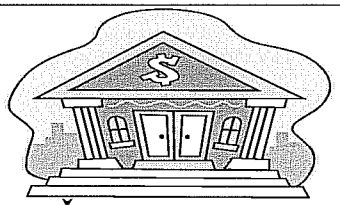
13. Generira sporočilo (odgovor avtorizacije), ki ga digitalno podpiše s pomočjo vrednosti razpršene funkcije sporočila, šifrira pa z zasebnim ključem.

14. Sporočilo (odgovor avtorizacije) se šifrira z novim, naključno generiranim simetričnim ključem (#3). Ta ključ se potem šifrira z javnim ključem prodajalca.

15.Kreira žeton zajetja, ki ga digitalno podpiše s pomočjo vrednosti razpršene funkcije žetona, šifrira pa z zasebnim ključem.



PRODAJALEC



PLAČILNI POSREDNIK

16. Žeton zajetja se šifrira z novim, naključno generiranim simetričnim ključem (#4). Ta ključ in kupčeve informacije o bančnem računu se skupaj šifrirajo z javni ključem plačilnega posrednika.

17. Pošlje prodajalcu šifriran odgovor o avtorizaciji.

odgovor o avtorizaciji

18. Prejme odgovor, certifikate verificira do korena drevesa zaupnih entitet.

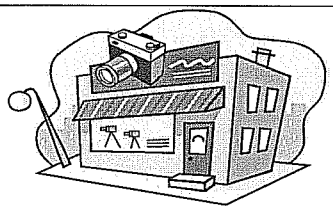
19. Z zasebnim ključem se dešifrira simetrični ključ (#3), s katerim pa se dešifrira odgovor.

20. Overovitev podpisa plačilnega posrednika se izvede z dešifriranjem z javnim ključem posrednika in primerjavo rezultata z novo generirano razpršeno vrednostjo odgovora.

21. Shranita se šifrirana žeton zajetja in ovojnica za kasnejše procesiranje.

22. **Prodajalec zaključi procesiranje nakupne zahteve.**

E) ZAJEM PLAČILA



PRODAJALEC

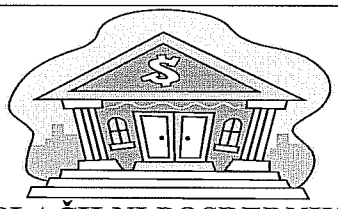
1. Kreira zahtevo za zajem.

2. V zahtevo vključi svoje certifikate, katero digitalno podpiše s pomočjo njene razpršene vrednosti, šifrira pa jo s svojim zaupnim ključem.

3. Zahteva se šifrira z naključno generiranim simetričnim ključem (#5). Ta ključ se šifrira z javnim ključem plačilnega posrednika.

4. Pošlje šifrirano zahtevo za zajem in šifriran žeton zajetja (shranjen pri odgovori o avtorizaciji) do posrednika.

zahteva za avtorizacijo in žeton zajetja →



PLAČILNI POSREDNIK

5. Certifikate prodajalca verificira do korena drevesa zaupnih entitet.

6. Z zasebnim ključem se dešifrira simetrični ključ (#5), s katerim pa se dešifrira zahtevo.

7. Overovitev podpisa prodajalca se izvede z dešifriranjem z javnim ključem prodajalca in primerjavo rezultata z novo generirano razpršeno vrednostjo zahteve.

8. Z zasebnim ključem se dešifrira simetrični ključ (#4), s katerim pa se dešifrira žeton.

9. Zagotovljena je konsistentnost med prodajalčevo zahtevo za zajem in žetonom.

10. Pošlje se zahteva za zajem preko finančnega omrežja do kupčeve finančne ustanove.

11. Generira sporočilo (odgovor zajema), ki vključuje certifikat posrednika in ga posrednik digitalno podpiše s pomočjo vrednosti razpršene funkcije sporočila, šifrira pa z zasebnim ključem.

12. Sporočilo (odgovor zajema) se šifrira z novim, naključno generiranim simetričnim ključem (#6). Ta ključ se potem šifrira z javnim ključem prodajalca.

13. Pošlje prodajalcu šifriran odgovor o zajemu.

← odgovor o zajemu

14. Prejme odgovor, certifikate verificira do korena drevesa zaupnih entitet.

15. Z zasebnim ključem se dešifrira simetrični ključ (#6), s katerim pa se dešifrira odgovor.

16. Overovitev podpisa plačilnega posrednika se izvede z dešifriranjem z javnim ključem posrednika in primerjavo rezultata z novo generirano razpršeno vrednostjo odgovora.

VIRI

[1] Set Secure Electronic Transaction LLC: The SET Standard Book 1 Business Description, SETCO, 1999, http://www.normos.org/en/setco.html
[2] Set Secure Electronic Transaction LLC: The SET Standard Book 2 Programmer's Guide, SETCO, 1999, http://www.normos.org/en/setco.html
[3] Set Secure Electronic Transaction LLC: The SET Standard Book 3 Formal Protocol Definitions, SETCO, 1999, http://www.normos.org/en/setco.html
[4] Set Secure Electronic Transaction LLC: SET Glossary, SETCO, 1999, http://www.normos.org/en/setco.html