Elektroniset maksuvälineet

Teemu Rinta-aho

Helsinki 29. lokakuuta 1999

Sähköisen kaupankäynnin seminaari

HELSINGIN YLIOPISTO
Tietojenkäsittelytieteen laitos

Sisältö

1 Johdanto

Sähköisellä kaupankäynnillä tarkoitetaan tietoverkoissa käytävää kauppaa. Yritysten välillä sähköinen kaupankäynti on ollut jollain tasolla käytössä jo pitkään (EDI), mutta Internetin laajeneminen yksityishenkilöiden käyttöön, sekä sen vahva kaupallistuminen ovat tehneet myös suoran sähköisen kuluttajakaupan mahdolliseksi. Nykyään Internetistä voi ostaa lähes kaikkea mitä perinteisistä kaupoistakin, jopa ruokaa. Erityisen kiinnostavaa on digitaalisen informaation myyminen (lehdet, musiikki, elokuvat, jne.), sillä tällaisessa kaupassa tavara voidaan myös toimittaa asiakkaalle Internetin välityksellä. Asiakkaalle tavaran löytäminen ja myyjälle sen perille toimittaminen ovatkin monesti huomattavasti helpompia ongelmia ratkaistaviksi, kuin turvallisen ja käyttökelpoisen maksujärjestelmän luominen.

Nykyään useat eri yritykset sekä tutkimuslaitokset kehittävät omia ehdotelmiaan tulevaisuuden maksuvälineeksi. Toistaiseksi mikään ei ole saavuttanut suosituimmuusasemaa. Useat ostokset Internetissä tehdään yhä luottokortilla. Tämä vastaa luottokorttinumeron antamista myyjälle puhelimen välityksellä. Nykyiset selaimiin integroidut salausjärjestelmät mahdollistavat luottokorttinumeroiden turvallisen välittämisen.

Suomessa ovat yleisessä käytössä ns. Web-maksut, jolloin kauppiaan järjestelmä täyttää pankin maksulomakkeen automaattisesti. Asiakas kirjautuu pankin palveluun ja maksaa laskun. Kauppias saa tiedon maksusta välittömästi. Järjestelmän käyttäminen vaatii asiakkaalta tilin kauppiaan tukemassa pankkijärjestelmässä. Järjestelmää käytettäessä riskin kantaa asiakas.

Luottokorttia ja Web-maksua joustavamman sähköisen rahan kehittämiseksi tehdään tutkimustyötä monessa eri yrityksessä, niin kaupan kuin tietotekniikan alalla toimivissakin. Sähköinen raha on joustavampi ja nopeampi tapa suorittaa pieniä maksuja kuin luottokortti. Lisäksi sähköistä rahaa voidaan siirtää älykortin ja tietokoneessa olevan kukkaron välillä sekä suoraan Internetissä. Suurimpana ongelmana monessa esitetyssä järjestelmässä on kuitenkin että käytetyt rahat joudutaan tarkistamaan niitä käytettäessä pankista.

Tutkielman toisessa luvussa käsitellään nykyisiä maksujärjestelmiä, sekä niiden soveltuvuutta sähköiseen kaupankäyntiin. Kolmannessa luvussa esitellään uusi maksujärjestelmä SET (Secure Electronic Transactions) joka perustuu turvalliseen luottokorttinumeron välittämiseen Internetissä. Neljännessä luvussa käsitellään sähköisen rahan vaatimuksia, ongelmia sekä esitellään käytännön toteutus sähköisestä rahasta. Viimeisessä luvussa on kokoava arvio esitellyistä tekniikoista.

2 Maksujärjestelmät

Yritysten välisessä ja kuluttajakaupassa eri osapuolilla on erilaisia vaatimuksia maksujärjestelmälle. Monet jo kauan käytössä olleet järjestelmät eivät ole suoraan käyttökelpoisia sähköisessä kaupassa. Tavalliset Internetin kautta ostoksiaan tekevät asiakkaat tarvitsevat joustavan ja helppokäyttöisen maksuvälineen, kun taas yritysten välisessä kaupassa voidaan käyttää raskaampia, usein sopimuksiin perustuvia järjestelmiä. Yritysten välisten transaktioiden nopeutuminen on sinänsä toivottava ominaisuus, joka voisi toteutua käyttämällä soveltuvilta osin samoja uusia maksujärjestelmiä ja -välineitä, kuin kuluttajille tullaan tarjoamaan.

2.1 Nykyiset maksujärjestelmät

Nykyään käytettäviä maksujärjestelmiä yritysten välisessä kaupassa ovat [TIV]:

- jälkivaatimus,
- postiennakko,
- ennakkomaksu pankin kautta,
- asiakastili ja tilausmaksu,
- lasku,
- tili ja yrityksen myöntämä luotto,

- OVT-laskutus,
- self billing sekä
- luottokortti.

Lisäksi kansainvälisessä yritysten välisessä kaupassa on käytössä

- maksumääräys,
- ulkomaan shekki,
- kansainvälinen postisiirto,
- remburssi ja
- perittävä.

Kotimaan kuluttajakaupassa käytettävät maksutavat ovat:

- käteinen,
- jälkivaatimus,
- Web-maksut,
- postiennakko,
- asiakastili ja tilausmaksu,
- maksukortit ja luottokortit sekä
- luotot, joita ovat
  - lasku sekä
  - tili tai myyjän luotto.

Kansainvälisen kuluttajakaupan maksutapoja ovat:

- luottokortti,
- postiennakko,
- asiakastili ja tilausmaksu,
- shekki,
- maksumääräys,
- postisiirto sekä
- lasku.

Maksutavoista OVT, eli organisaatioiden välinen tiedonsiirto, tarkoittaa laskun toimittamista automaattisesti tietojärjestelmästä toiseen, sekä mahdollisesti sen automaattista maksamista. Self billing taas tarkoittaa, että laskua ei lähetetä ollenkaan, vaan asiakas tietää sovitun hinnan ja maksaa sen omatoimisesti. Web-maksut tarkoittavat pankkien tarjoamia www-maksutositteita jonka web-kauppa täyttää asiakkaan hyväksyntää sekä välitöntä maksua varten.

Maksutapoja on monia, mutta niistä mikään ei sovellu kovin hyvin tuotteiden, jotka voidaan välittää Internetin välityksellä, maksamiseen. Tällaisia tuotteita voivat tulevaisuudessa olla mm. digitaalisessa muodossa oleva kuva ja ääni sekä muu informaatio, kuten hakupalvelut.

2.2 Elektroniset maksujärjestelmät

Elektronisen maksujärjestelmän täytyy olla turvallinen, luotettava, skaalautuva ja tehokas, sekä sen täytyy olla integroitavissa olemassaoleviin Internet-sovelluksiin sekä talouden rakenteisiin [Pan96].

Elektroninen maksaminen on toteutumassa kolmen toisiaan täydentävän ratkaisun muodossa [TIV]:

- **tilivelan siirto**, jossa yleensä käytetään luottokorttia ja jota käytetään suurissa ostoissa,
- **tilirahan siirto**, jossa maksutapahtuma kohdistuu muualla sijaitsevaan tiliin ja jota käytetään keskisuurissa ostoissa sekä
- **sähköinen käteinen**, jota käytetään pienissä maksuissa ja joka voi olla:
  - **korttirahaa** eli sähköinen raha on toimikortilla tai
  - **verkkorahaa** eli ohjelmistopohjaisesti toteutettua.

Näistä ensimmäinen, tilivelan siirto, on tällä hetkellä yleisimmin käytössä. Uusi SET-standardi mahdollistaa turvalliset luottokorttimaksut ja tulee varmasti pitämään tämän maksujärjestelmän markkinaosuuden suurena jatkossakin.

Tilirahan siirtoa tai Web-maksuja käytetään Suomessa paljon. Tämä on varsin kätevä järjestelmä, jos asiakkaalla on tili kauppiaan tukemassa pankissa. Heikkoutena on kuitenkin sopimattomuus kansainväliseen kuluttajakauppaan sekä pieniin maksuihin. Elektroninen shekki on teknisesti käytännössä samankaltainen ratkaisu, mutta shekit ovat enää käytössä kuluttajakaupassa lähinnä yhdysvalloissa, joten kansainvälistä maksujärjestelmää elektronisista shekeistä tuskin tulee.

Sähköinen käteinen on konsepteista uusin ja teknisesti mielenkiintoisin. Seteleiden ja kolikoiden korvaaminen bittijonoilla nopeuttaa ja tekee kaupankäyntiä joustavammaksi. Samaa rahaa voi käyttää missä vain, joko Internetissä tai älykortin avulla vaikkapa ravintolassa. Lisäksi sähköinen raha ei paina mitään, ei kulu, eikä vie juurikaan tilaa. Ongelmana on kuitenkin rahan käytön vaatima tarkistus, ja sitä kautta järjestelmän skaalautumattomuus ja raskaus Internet-käytössä.

Internetissä sähköisen rahan käyttö perustuu rahan tarkistamiseen sitä vastaanotettaessa rahan luoneelta instituutiolta. Jos rahaa halutaan käyttää Internetin ulkopuolella, täytyy käyttää ns. “luotettavaa laitteistoa” (trusted hardware), eli älykorttia joka toimii itsenäisesti ja jonka toiminnan oikeellisuuteen käyttäjä ei pääse vaikuttamaan. Tällainen älykortti suorittaa haluttuja maksutoimintoja, mutta esimerkiksi

kortilla olevaa rahaa ei voi kopioida, sillä siirrettäessä rahaa kortti itse huolehtii rahan poistamisesta muististaan. Tällöin rahaa ei tarvitse tarkistaa, jos myyjä luottaa asiakkaan korttiin.

Myös useat nykyiset järjestelmät voidaan yksinkertaistaa: erilliset bussikortit, kopiokortit, puhelinkortit ja muut vastaavat ovat tarpeettomia tällaisen universaalin älykortin tultua käyttöön.

Älykortit tuovat maksamiseen myös monia uusia ulottuvuuksia. Tulevaisuudessa älykortin voi esimerkiksi laittaa matkapuhelimeen, ja siirtää rahaa toisella puhelimella olevaan älykorttiin, ja näin siirtää rahaa henkilöltä toiselle. GSM:n sekä muiden digitaalisten matkapuhelinjärjestelmien turvallisuusominaisuudet, sekä SIM (Subscriber Identity Module) -pohjaisuus ovat luonteva alusta maksu- ja talouspalveluiden toteuttamiselle. SIM-kortti sisältää tunnistetiedot puhelinliittymän omistajasta ja salausavaimen, joten lisäsovellusten ei tarvitse enää kantaa huolta tietoturvasta. Jo nyt SIM-korteille voidaan ladata muitakin kuin puhelimen toimintaan tarvittavia lisäohjelmistoja. Nämä STK-standardin (SIM ToolKit) mukaiset ohjelmat voivat käyttää hyväkseen olemassaolevaa salatut yhteydet mahdollistavaa puhelinverkkoa keskinäiseen kommunikointiin [Bir99].

Kaikkien sovellusten ei kuitenkaan tarvitse sijaita samalla SIM-kortilla, vaan tulevaisuudessa matkapuhelimissa tulee olemaan toinenkin korttipaikka muita älykortteja varten. Näin SIM-kortilla sijaitseva STK-sovellus (esimerkiksi pankkipalvelu) voi vaikkapa käyttää puhelimen toisessa korttipaikassa sijaitsevalla älykortilla olevaa rahaa laskun maksamiseen. Merita aloittaa pilottiprojektin jossa voidaan käyttää WAP-pohjaista (Wireless Application Protocol) palvelua laskun maksamiseen Visan älykortilla GSM-puhelimen välityksellä [Bir99].

Älykorttien turvallisuus perustuu ns. “luotettavaan laitteistoon” (trusted hardware). Universaalin monitoimi-älykortin käyttöönottoa ovat kuitenkin hidastaneet monet ongelmat. Eräässä projektissa havaittuja käytännön ongelmia ovat mm. seuraavat [AB96].

- **Kustannukset**. Laitteisto älykorttien käyttämiseen pitäisi asentaa ennen älykortteja, ja tämä on yritykselle kalliimpaa kuin normaalin rahan vastaanottaminen.
- **Standardien puuttuminen**. Kansainvälisten standardien puuttuessa yritykset eivät uskalla lähteä toteuttamaan älykorttiprojekteja.
- **Kontrollivastuu**. Sekä pankit, yritykset että valtio haluaisivat kaikki kontrolloida älykortteja.
- **Korttioperaattoriin luottaminen**. Miten yritykset voivat luottaa transaktioiden oikeellisuuteen.

Lisäksi kilpajuoksu turvallisten mikroprosessorien valmistajien ja rikollisten välillä jatkuu, kuten virusten ja virustorjuntaohjelmistojen kirjoittajienkin välillä. Viimeisimmätkään älykorttijärjestelmät eivät ole murtovarmoja [AK96].

3 Maksujärjestelmäesimerkki: SET

Kuva 1: Virallinen SET-logo

3.1 Yleistä

Secure Electronic Transactions (SET) on avoin, toimittajasta riippumaton standardi joka perustuu tilivelan siirtoon. Sen kehittämisessä ovat olleet mukana mm. VISA, Mastercard, Microsoft, IBM, Netscape ja American Express.

SET:in tavoitteet ovat [VM97]:

- maksutapahtumassa tarvittavien tietojen turvallinen välittäminen,
- taata siirretyn tiedon eheys,
- autentikoida käyttäjä kortin omistajaksi,
- autentikoida myyjä,
- käyttää parhaita nykyisin tunnettuja turvallisuuskäytäntöjä,
- taata protokolla, joka ei riipu kommunikointiväylän turvallisuusmekanismeista eikä estä niiden käyttöä sekä
- luoda mahdollisuudet yhteistoimintaan ja rohkaista eri ohjelmistoyrityksiä siihen.

3.2 Toteutus

SET:in toteutus perustuu vahvojen salaustekniikoiden käyttöön, käytössä on mm. kahden digitaalisen allekirjoituksen tekniikka. Lainsäädäntö vaihtelee monissa maissa salauksen suhteen. Kuitenkin monien maiden lainsäädännössä sallitaan salauksen käyttö talouteen liittyvissä transaktioissa, jotka ovat hyvin määriteltyjä ja kiinteämittaisiin viesteihin perustuvia, eikä salausta voida helposti käyttää muihin tarkoituksiin.

SET:in käyttö perustuu erityiseen ohjelmistoon, joka tallettaa käyttäjän tiedot, digitaaliset avaimet, kuitit jne. käyttäjän tietokoneelle. Tämä ohjelmisto kommunikoi sekä luottokorttiyhtiön, että myyjän ohjelmistojen kanssa. Luottokorttiyhtiöltä hankitaan ensiksi oma digitaalinen avain, jota käytetään salaukseen sekä digitaalisiin allekirjoituksiin. Tämä avain liittyy aina omistajan luottokorttiin.

3.3 Toiminta

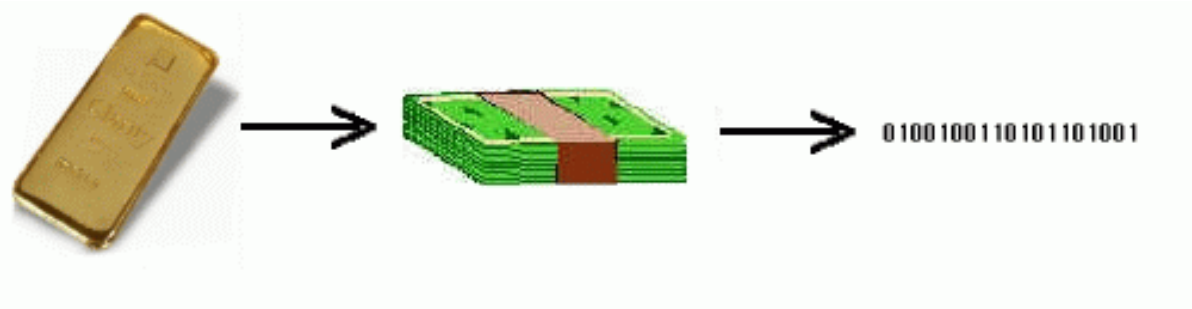
Kun asiakas haluaa suorittaa maksun, autentikoi ohjelmisto myyjän myyjältä saadun sertifikaatin perusteella ja asikas saa varmistuksen myyjästä. Tämän jälkeen asiakas

käyttää myyjän julkista avainta salattuun tiedonsiirtoon myyjän ja itsensä välillä. Asiakas lähettää tilaustiedot sekä luottokortin numeron ja maksun summan myyjälle. Tilaustiedot ovat myyjän luettavissa, mutta laskutustiedot ovat salattuna luottokorttiyhtiön avaimella, eivätkä näin ollen ole myyjän luettavissa. Myyjä välittää laskutustiedot eteenpäin, ja saa luottokorttiyhtiöltä vahvistuksen laskutuksesta. Tämän jälkeen myyjä lähettää vahvistuksen tilauksesta asiakkaalle. Kaikki lähetetyt viestit ovat digitaalisesti allekirjoitettuja, ja esimerkiksi tilausvahvistus tallettuu asiakkaan ohjelmistoon sähköisenä kuittina. Tällaista kuittia ei voi väärentää, eikä myyjä voi esimerkiksi myöhemmin kiistää lähettäneensä allekirjoittamaansa tilausvahvistusta. Myyjä ei missään vaiheessa näe asiakkaan luottokorttitietoja, mutta varmistuu asiakkaan henkilöllisyydestä asiakkaan lähettämän digitaalisen allekirjoituksen perusteella.

Järjestelmän edut perinteiseen luottokorttimaksuun ovat selkeät: ei luottokorttinumeroa, eikä muita tärkeitä tietoja välitetä missään vaiheessa salaamattomana, myyjä ei saa asiakkaan luottokorttinumeroa, mutta sekä myyjä että asiakas voivat autentikoida toisensa. Kaikki monimutkainen logiikka voidaan toteuttaa ohjelmistoilla, ja asiakkaalle näytetään vain välttämättömät tiedot. Ohjelmisto voi toimia taustalla, www-selaimen kanssa yhteistyössä, ja asiakkaan tarvitsee vain vastata tiettyihin järjestelmän varmistuskyselyihin.

Järjestelmä on jo käytössä useissa Internet-kaupoissa niin Suomessa kuin ulkomaillakin. Luottokunnan www-sivuilta on ladattavissa asiakasohjelma, ja Visan omistajat voivat hakea samasta paikasta oman salausavaimensa. Sivuilla on myös testikauppa, jossa järjestelmää voi kokeilla turvallisesti.Asiakasohjelmisto on toistaiseksi saatavilla vain Windows-käyttöjärjestelmiin.

4 Sähköinen raha



Kuva 2: Maksuvälineen evoluutio kullasta biteiksi

4.1 Yleistä

Digitaalinen eli sähköinen raha on nykyisten kolikoiden ja seteleiden sähköinen vastine (kuva 3). Käytännössä rahoja voidaan siis käsitellä normaalien tiedostojen tapaan. Jotta sähköinen raha olisi käyttökelpoinen, sen tulisi vastata ominaisuuksiltaan perinteistä rahaa. Rahan tärkeimpiä ominaisuuksia ovat [Pan96]:

- **anonymiteetti** sekä
- **likviditeetti**.

Anonymiteetti tarkoittaa, että kun asiakas maksaa myyjälle, muut kuin myyjä ei tunnista asiakasta. Tietyissä tapauksissa edes myyjän ei tarvitse eikä välttämättä voi tunnistaa asiakasta. Itse transaktiosta ei välttämättä tallenneta mitään tietoja. Tämä vastaa esimerkiksi lehden ostoa lehtikioskilta. Raha itsessään riittää sertifioimaan maksutapahtuman.

Likviditeetillä tarkoitetaan rahan hyväksyttävyyttä maksuvälineenä: kaikkien myyjien tulisi hyväksyä sama raha (sähköisen rahan tapauksessa koko Internetissä).

Sähköisellä rahalla on monia muita etuja perinteiseen rahaan verrattuna. Sähköisen rahan siirtäminen on huomattavasti helpompaa, halvempaa ja nopeampaa. Myös tal-

lettaminen vaatii paljon vähemmän tilaa. Sähköistä rahaa on vaikeampi väärentää kuin perinteistä, toisaalta sitä on helppo kopioida, mutta monet järjestelmät estävät kopioiden käyttämisen.

4.2 Toteuttaminen

Sähköisen rahan toteutustapoja ovat sekä ennalta ostetut rahakortit (Avant, puhelukortit), että puhtaasti elektroniset järjestelmät. Tulevaisuuden älykortit voivat toimia lompakkoina, joille on talletettu sähköistä rahaa, ja joita voi käyttää niin normaaleissa kaupoissa kuin Internetissäkin tietokoneeseen kytkettyinä.

Suurimpana teknisenä ongelmana sähkörahan toteuttamisessa on turvallisten skaalautuvien järjestelmien puuttuminen. Käytettävät rahat joudutaan nykyisissä ratkaisuissa tarkistamaan rahan liikkeellelaskijalta. Tämä tarkoittaa sitä, että myyjällä täytyy olla Internet-yhteys sähköisen rahan tarkistamista varten. Yksityishenkilöiden välisessä kaupankäynnissä sekä pienessä, liikkuvassa kaupankäynnissä, esimerkiksi jäätelömyynnissä jatkuvan Internet-yhteyden toteuttaminen saattaa olla vaikeaa tai mahdotonta. Toistaiseksi on kuitenkin mahdotonta estää rahan käyttämistä moneen kertaan, ellei sitä jokainen kauppias käy ilmoittamassa pankkiin käytetyksi.

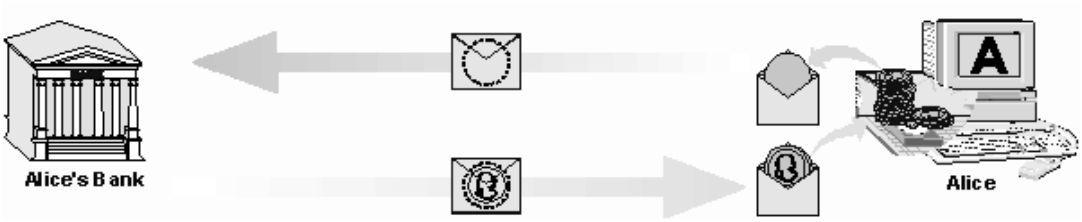
4.3 Elektroninen raha

Ecash on alankomaalaisen DigiCash-yhtiön luoma tekniikka elektronisen rahan toteutukseen. Ecash käyttää turvallisuuden takaamiseksi julkisen avaimen kryptografiaa, sekä anonymiteetin takaamiseksi ns. sokeita allekirjoituksia [Cha92].

Ecash toimii kuten normaali käteinen. Sitä voidaan nostaa ja tallettaa, sekä tehdä tilisiirtoja. Kuitenkin maksettaessa myyjälle, tai siirrettäessä rahaa toiselle henkilölle, pankin täytyy olla transaktiossa mukana.

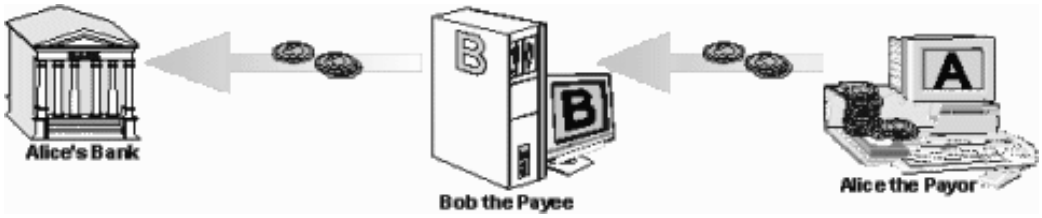
Rahat esitetään bittijonoina. Jokainen raha on eri bittijono, ja rahalla on tietty arvo. Käyttäjän ohjelmisto kokoaa rahaa siirrettäessä haluttua summaa vastaavan määrän mahdollisesti eriarvoisia rahoja. Rahoja nostettaessa asiakkaan ohjelmisto itse asiassa

luo rahan, ja pankki vain allekirjoittaa sen, sekä vähentää asiakkaan tililtä vastaavan summan.



Kuva 3: Sokea allekirjoitus

Anonymiteetin takaaminen turvallisuutta heikentämättä taataan ns. sokeilla allekirjoituksilla (blind signatures) [Cha92]. Ideana sokeassa allekirjoituksessa on yksinkertaistetusti, että asiakas kertoo rahan muodostavan bittojonon jollain satunnaisella numerolla, ennenkuin lähettää sen pankin allekirjoitettavaksi. Kun saatu bittijono jälleen jaetaan samalla satunnaisella numerolla, pankin allekirjoitus säilyy, mutta pankki ei enää tunnista rahaa (muutakuin oman allekirjoituksensa), eikä rahaa näinollen voida jäljittää (kuva 3).



Kuva 4: Ecashilla maksaminen

Maksaminen Ecashilla tapahtuu siten, että käyttäjä saa maksukehoituksen myyjältä, jonka hän hyväksyy. Ecash-ohjelmisto valitsee oikean määrän Ecash-rahoja kiintolevyltä ja lähettää rahat myyjälle. Myyjä tarkistaa rahat pankista, jonka jälkeen tieto hyväksynnästä palautuu asiakkaalle. Jos myyjän ja asiakkaan pankki eivät ole samoja, joutuu

myyjän pankki tarkistamaan rahat edelleen asiakkaan pankista. Tarkistuksen yhteydessä rahat merkitään käytetyiksi (kuva 4).

4.4 Raha älykortilla

Mondex on Mastercardin projekti, jossa älykortilla säilytetään elektronista rahaa. Kortti on normaalin luottokortin kokoinen, mutta sillä on mikroprosessori, kortti on siis suomalaisillekin jo tuttu ISO 7816 -standardin mukainen älykortti. Ensimmäiset spesifikaatiot kortista julkistettiin vuonna 1994. Tällä hetkellä yli 450 yhtiötä yli 40 maassa tekevät työtä määrittelyjen kanssa (http://www.mondex.com).

Kortilla sijaitseva ohjelmisto toimii eräänlaisena elektronisena kukkarona. Rahaa voidaan siirtää kortille ja kortilta erityisellä kortinlukijalla. Kortti on suojattu käyttäjän omalla salaisella tunnusluvulla.

Suomessa pankkikortin yhteyteen on jo jonkin aikaa saanut vastaavan mikroprosessorin, johon voidaan ladata normaaleilla pankkiautomaateilla rahaa, ja jota voidaan käyttää normaalin käteisen tapaan kaupoissa joissa on lukulaite kortille. Järjestelmä ei ole kuitenkaan pankki- ja luottokorttien tapaan yleistynyt.

5 Yhteenveto

Tällä hetkellä yleisimpiä elektronisia maksujärjestelmiä Suomessa ovat ns. Web-maksut (Kultaraha, Solo), jotka ovat pankkikohtaisia. Internet-kaupassa maailmanlaajuisesti suurin osuus on perinteisillä luottokorteilla. Luottokortin numero voidaan välittää salattua yhteyttä pitkin kauppiaalle, joten asiointi on yhtä turvallista kuin kaupassa paikan päällä. Myyjän tunnistaminen verkossa on kuitenkin ongelmallisempaa kuin normaalissa kaupassa. Vastaavasti myyjän näkökulmasta luottokortin käyttäjän tunnistaminen on ongelma. SET-standardi ratkaisee nämä ongelmat käyttämällä nykyisin tunnettuja salaus- ja autentikointitekniikoita.

Erilaisia puhtaasti sähköisen rahan toteutuksia on useita, jotka eivät kutenkaan ole edenneet kokeiluvaihetta pidemmälle, lukuunottamatta ns. korttirahaa, joka on useassa maassa jonkinasteisessa käytössä. Sähköinen raha on kuitenkin uusi järjestelmä joka ei pohjaudu olemassaoleviin, tilisiirtoihin perustuviin järjestelmiin. Sähköisen rahan käyttöönottoa hidastavina tekijöinä ovat ennenkaikkea lainsäädännölliset ja poliittiset ongelmat, sekä perinteisen pankkialan epäröinti. Myöskin teknisesti sähköistä rahaa on vielä vaikea toteuttaa, sillä sitä on helppo kopioida, joten nykytekniikalla sen käyttö joudutaan aina tarkastamaan sitä käytettäessä.

SET:in vakiinnutettua asemansa, ja luottokorttien käyttäjien suuren määrän ja luottokorttiyhtiöiden markkinavoiman huomioonottaen, sen asema tulee entisestään vahvistumaan, ja päässee käytännössäkin standardin asemaan lähivuosina [Smi98]. Myös erilaiset matkapuhelimeen tai muuhun henkilökohtaiseen kannettavaan liitettävät älykortit (esimerkiksi uuden sukupolven monitoimi-SIM-kortit) ja verkon kautta ladattavat sovellukset tulevat muodostamaan uuden tavan maksaa niin Internetissä kuin perinteisissäkin kaupoissa [Bir99].

Viitteet

AB96 R. Anderson and S. Bezuidenhoudt. On the reliability of electronic payment systems. *IEEE Transactions on Software Engineering*, 22(5):294–301, May 1996.

AK96 R. Anderson and M. Kuhn. Tamper resistance - a cautionary note. In *The second USENIX workshop on electronic commerce*, pages 1–11, November 1996.

Bir99 D. Birch. Mobile financial services: The internet isn't the only digital channel to consumers. http://www.arraydev.com/commerce/jibc/9909-05.htm, October 1999.

Cha92 D. Chaum. Achieving electronic privacy. *Scientific American*, pages 96–101, August 1992.

Pan96 P. Panurach. Money in electronic commerce. *Communications of the ACM*, 39(6):45–50, June 1996.

Smi98 S. Smith. Is set ready for prime time? http://www.arraydev.com/commerce/jibc/9801-10.htm, January 1998.

TIV TIVEKE. Sähköinen kaupankäynti. http://www.telmo.fi/tiveke/kauppa.htm.

VM97 Visa and Mastercard. Set secure electronic transaction specification book 1: Business description. Technical report, May 1997.

A Aihepiirin www-linkkejä

Tässä liitteessä on muutamia linkkejä tärkeimmille aihepiiriä käsitteleville sivuille.

`http://www.setco.org` - SetCo

- SetCo on SET-projektin virallinen kotisivu.

`http://www.mondex.com` - Mondex

- Mondex on eräs tunnetuimpia älykorttiprojekteja.

`http://www.ex.ac.uk/ rdavies/arian/emoney.html` - Electronic money

- Erittäin kattava linkkikokoelma elektronisesta rahasta.

`http://www.ecashtechnologies.com/` - eCash technologies inc.

- eCash technologies inc. osti ECash-teknologian DigiCashilta.

`http://www.ispo.cec.be/fiwg/` - EC FIWG

- EU:n Financial Issues Working Group. Tietoa elektronisista maksujärjestelmistä.