TAMPEREEN TEKNILLINEN YLIOPISTO
Tietojohtamisen koulutusohjelma

KRISTIAN AF HÄLLSTRÖM

VERKKO-OSTAMINEN JA REILU VAIHTO -PROTOKOLLA

Seminaarityö

TLT-3400 Kryptoprotokollat

7.5.2009

SISÄLLYS

1. JOHDANTO

Verkossa asioiminen on lisääntynyt huomattavasti vuosituhannen vaihteesta. Tietoyhteiskunta mahdollistaa kaupankäynnin verkon yli myös yksityisten ihmisten välillä. Internetin kautta on nopeaa ja vaivatonta ostaa tuotteita myös maailman toiselta puolelta. Digitaalisia tuotteita, kuten pelejä, musiikkia ja ohjelmia ostettaessa välimatkat menettävät merkityksensä, kun ostaminen tapahtuu tietoverkkoja pitkin.

Reilun vaihdon merkitys on erittäin suuri kaikenlaisessa kaupanteossa. Reilun vaihdon ansiosta ostaja saa tuotteen maksettuaan sen sekä myyjä saa rahat luovutettuaan tuotteen asiakkaalle. Käytännössä reilua vaihtoa tapahtuu jokaisessa kaupankäynnissä ja sen voi toteuttaa myös ilman erityistä reilun vaihdon protokollaa. Reilu vaihto on tärkeää myös kasvokkain tapahtuvassa ns. face-to-face-myynnissä. Esimerkiksi käytettyä autoa ostettaessa voidaan sopia, että rahat annetaan myyjälle, kun tarvittavat paperit on tehty. Avaimet, rekisteriote, luovutuskirja ja rahat voidaan antaa sovitussa järjestyksessä kun kaupasta on sovittu ja molemmat osapuolet ovat hyväksyneet kauppasumman.

Tässä seminaarityössä perehdytään reiluun vaihtoon ja verkko-ostamiseen. Toisessa luvussa esitetään reilu vaihto prosessina. Kolmas luku keskittyy keinoihin toteuttaa reilua vaihtoa ilman erityistä reilun vaihdon protokollaa sekä pohditaan asioita mitkä auttavat reilun vaihdon toteutumista ja esitetään muutama esimerkki kaupankäynnistä. Neljäs luku keskittyy reilun vaihdon protokolliin, ensin esitellään tarkemmin reilun vaihdon perusprotokolla ja sen jälkeen käydään läpi anonyymi reilu vaihto -protokollaa. Lopuksi asia kiteytetään yhteenvetoon.

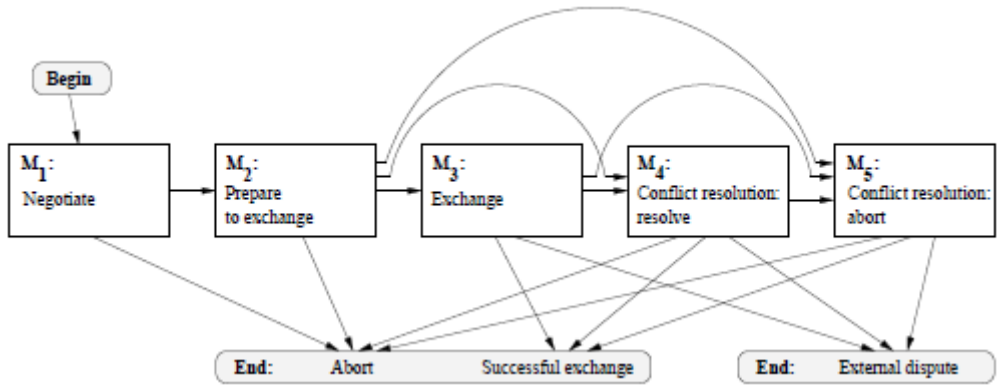
2. REILU VAIHTO –PROSESSIN MALLI

Reilun vaihdon (fair exchange, fairness) toteutuminen on oleellisen tärkeää kaupankäynnissä. Se tarkoittaa yksinkertaisesti sitä, että molemmat osapuolet saavat sen mitä haluavat tai kumpikaan ei saa mitään. Reilua vaihtoa voidaan ajatella käytettävän myös sopimusten allekirjoittamisessa, joissa kumpikaan osapuoli ei halua allekirjoittaa ennen kuin toinen on allekirjoittanut.

Kaupankäynnissä ostajan tulisi aina saada tuote kun on siitä maksanut sekä kauppiaan on aina saatava taloudellinen korvaus ostetusta tuotteesta kun on sen luovuttanut asiakkaalle. Kaupankäynti voi myös keskeytyä missä tahansa vaiheessa. Jos kauppa keskeytyy, kumpikaan osapuoli ei saisi saada kaupasta hyötyä enemmän kuin toinen.

Tietoliikenneverkon yli käytävässä kaupankäynnissä aina toinen joutuu lähettämään ensin, kauppias tuotteensa tai asiakas rahansa, joten käytännössä aina tarvitaan kolmas osapuoli luotettavan reilun vaihdon varmistamiseen.

Reilu vaihto voidaan ajatella modulaarisena prosessina kuvan 2.1 tavoin. Reilu vaihto alkaa neuvottelusta, jossa neuvotellaan vaihdosta, vaihdon kohteista (tuotteesta ja sen hinnasta) sekä vaihtoprotokollasta. Reilu vaihto voi päättyä keskeytykseen jo suoraan neuvottelusta, esimerkiksi jos hinnasta ei päästä sopimukseen. Kun molemmat osapuolet tietävät mitä tuotteita aiotaan vaihtaa ja millä hinnalla, heidän täytyy hyväksyä myös vaihtoprotokolla ja luotettu kolmas osapuoli (Pagnia et al 2003, s 11). Mikäli molemmat osapuolet haluavat jatkaa siirrytään kohtaan M_2: neuvotteluun valmistautuminen.



Kuva 2.1 Ideoitu reilu vaihto -protokolla käyttäen modulaarista lähestymistapaa (Pagnia et al 2003, s 12).

Ennen vaihtoa osapuolten täytyy tietää, että konfliktin ja keskeytymisen mahdollisuus on olemassa. Valmistautumisessa varmistutaan, että kyse on oikeista vaihdettavista, oikeista tuotteista. Mikäli tarkistus epäonnistuu, voidaan siirtyä M_5:een ja keskeyttää vaihto. Vaihtoon valmistautumisesta siirrytään kohtaan M_3: vaihto.

Osapuoli, jonka vaihdettava tuote tai maksu on peruutettavissa, lähettää ensin, jolloin hän voi peruuttaa, jos toinen osapuoli ei lähetäkään tavaraansa. Peruutettava tuote voi olla raha, jonka voi periä takaisin tai esimerkiksi ohjelmiston lisenssi.

Joissain tapauksissa kolmas osapuoli pystyy tuottamaan ja lähettämään korvaavan tuotteen vaihtoa varten (generatability, esim. myyjän toimiessa virheellisesti) (Liukkonen 2002, s. 9). Se osapuoli, jolla on tämmöinen ominaisuus, odottaa että toinen osapuoli lähettää ensin. Tämä mahdollistaa sen, että hän voi ensin tarkastaa, että toisen tavara vastaa kuvausta ja lähettää itse vasta sen jälkeen. (Pagnia et al 2003, s. 12) Ensin lähettävä osapuoli taas voi luottaa siihen, että jos ei saa tuotetta toiselta, hän saa sen kolmannelta osapuolelta. Korvattava tuote voi olla esimerkiksi raha, tai mikä tahansa sellainen joka on kolmannen osapuolen hallussa.

On tavallista myös että osapuoli, joka luottaa enemmän toiseen osapuoleen lähettää yleensä ensin. Vaihto voi päätyä onnistuneeseen vaihtoon, päätyä ulkoiseksi kiistaksi tai keskeytyä.

M_4-moduuliin siirrytään ristiriitatilanteessa ja se on ainoastaan sen osapuolen käytössä, joka odottaa kolmannelta osapuolelta tavaraa vaihdossa hänen omaa tavaraansa vastaan. Tämä on mahdollista vain, kun generatability-ominaisuus on mahdollinen. M5-moduuliin siirrytään myös ristiriitatilanteessa ja moduuli on sen osapuolen käytössä, joka haluaa peruuttaa vaihdon. Moduuli pyrkii nollaamaan vaihdon niin että kumpikaan osapuoli ei saa mitään hyötyä vaihdosta, vaan pitävät omat tavaransa, kun taas edellisessä moduulissa M4 yritetään päästä onnistuneeseen vaihtoon kolmannen osapuolen avulla. (Pagnia et al 2003, s 12). Vaihto voi päätyä keskeytykseen kaikista moduuleista, mutta onnistuneeseen vaihtoon vain moduuleista M_3, M_4 ja M_5, joista vaihto voi päätyä myös ulkoiseksi kiistaksi.

3. KEINOJA TOTEUTTAA REILU VAIHTO

Nykyään on useita tapoja tehdä kauppaa verkossa ilman varsinaista reilun vaihdon protokollaa. Usein kuitenkin ostaja joutuu luottamaan myyjään, joskus myyjä ostajaan. Luottamus on suurempi, kun toinen osapuoli on tunnettu ja autentikoitu. Ilman reilun vaihdon protokollaa kaupankäynti on helpointa kolmannen luotetun osapuolen välityksellä, esimerkiksi rahan siirtämisessä tai tuotteen lähettämisessä.

Yksi tapa toteuttaa reilua vaihtoa on tehdä se pienissä palasissa. Esimerkiksi sopimusta allekirjoitettaessa kumpikaan osapuoli ei suostu siihen ennen toista. Luotetun kolmannen osapuolen avulla tämä on helppoa, mutta ilman sitä voidaan käyttää pienten askelten menetelmää, jossa kumpikin vuorollaan osoittaa lisää sitoutumista sopimukseen. (Koskinen, 2004). Tuotteen ostaminen pienissä paloissa, esimerkiksi ohjelmiston ostaminen koodirivi kerrallaan ei onnistu, sillä ohjelma ei toimi ennen kuin kaikki rivit ovat tallella. Myyjä hyötyy, jos lopettaa kesken ja pitää rahat.

Kaupankäyntiä varten voidaan kuitenkin tehdä sopimus, jonka molemmat allekirjoittavat. Allekirjoituksen jälkeen myyjä lähettää tavaran ja ostaja rahat, sopimuksen mukaisesti. Mikäli toinen osapuoli rikkoo sopimusta, eikä anna rahoja tai tuotetta, asia voidaan riitauttaa ja ratkaista oikeuden edessä. Pienissä palasissa lähetettävä sopimus aiheuttaa lukuisia viestejä, jonka takia menetelmä ei ole kovin käytännöllinen.

Reilua vaihtoa voidaan varmistaa dokumentaatiolla, tilatessa lähetetään tilausvahvistus ja maksusta sekä toimituksesta tulostetaan kuitti, joihin molemmat osapuolet voivat tarvittaessa vedota. Kuitin voi tuottaa myös pankki, jos myyjä ei sitä tarjoa.

3.1. Autentikointi

Usein verkkokauppoihin tulee rekisteröityä ja antaa paljon henkilötietoja. Ostaja pyritään autentikoimaan hyvin, usein käytetään myös pankkitunnuksia tai henkilökohtaisen sirukortin HST:n varmenteen avulla varmistutaan käyttäjän henkilöllisyydestä. Ostaja puolestaan luottaa myyjään, useimmiten tuntee myyjän ja/tai saa verkkosivuilta avoimesti tietoa yrityksestä ja esimerkiksi sen Y-tunnuksen.

Vaikka osapuolet ovat autentikoituneet toisilleen hyvin, joutuvat he silti luottamaan toisiinsa, mutta voivat riitauttaa tarvittaessa tuomioistuimeen toisen osapuolen rikkoessa sopimusta. Riitauttaminen on kuitenkin yleensä hyvin kallista, joten reilun vaihdon toteutuminen varmistetaan myös muilla keinoin.

3.2. Maksutavat

Verkkokauppojen reilu vaihto varmistetaan yleensä oikeanlaisilla ja turvallisilla maksutavoilla. Erilaisia maksutapoja on lasku, ennakkomaksu, verkkotilisiirto, nouto, jälkivaatimus, postiennakko ja luottokortti (TIEKE). Laskulla maksettaessa myyjä joutuu luottamaan ostajaan ja taas ennakkomaksussa sekä verkkotilisiirrossa ostaja myyjään. Ennakkomaksua ja verkkotilisiirtoa ei kannata käyttää kovin suuriin ostoksiin ja myyjän tulee olla luotettava. Nouto ja käteisellä maksaminen on luotettavaa, mutta aiheuttaa ostajalle esimerkiksi matkakuluja, eikä ole täysin verrattavissa muuhun verkko-ostamiseen.

Jälkivaatimuksessa tuote maksetaan kuljettajalle sen tuodessa tuotetta ja postiennakossa tuote maksetaan postissa noudettaessa tuotetta. Molemmissa tapauksissa on kolmas luotettu osapuoli, joka varmistaa että ostaja maksaa ja myyjä luovuttaa tuotteen. Tästäkin voi aiheutua lisäkustannuksia, jos ostaja tilaa paljon tavaraa aikomattakaan maksaa. Postiennakossa reilun vaihdon toteutumista varmistaa lisäksi pakettiin kirjoitettu merkintä, että asiakas saa postivirkailijan läsnä ollessa avata ja tarkistaa paketin sisällön.

Luottokortilla ostettaessa luotettuna osapuolena toimii luottokorttiyhtiö. Jotkut luottokorttiyhtiöt tarjoavat ns. charge back -palvelua, joilla pyritään lisäämään verkko-ostamisen turvallisuutta. Charge back -palvelu tarkoittaa sitä, että jos tuotteessa, palvelussa tai laskussa on virhe tai puute, myös luotonantaja saattaa olla vastuussa suoritetun maksun palauttamisesta (TIEKE). Luottokortti on melko turvallinen tapa maksaa, mutta pitää kuitenkin varmistua, ettei luottokortin numero joudu vääriin käsiin.

Suomen Maksuturva tarjoaa reilua vaihtoa kolmantena osapuolena pitämällä huolen siitä, että maksu ja ostettu tavara vaihtavat omistajaa samanaikaisesti (Suomen Maksuturva, 2009). Maksuturva-palvelu on kuluttajalle maksuton, mutta verkkokauppa joutuu maksamaan käytöstä. Palvelu on turvallinen, mutta se on käytössä kuitenkin hyvin pienellä osalla verkkokauppoja. Se on kuitenkin uusi palvelu ja vasta hakemassa jalansijaa, joten aika näyttää, kuinka suosittu se tulee olemaan.

3.3. Käytännön esimerkkejä

Reilua vaihtoa pyritään toteuttamaan kaikenlaisessa kaupanteossa. Erittäin tärkeätä on sen toteutuminen C2C-kaupassa eli yksityisten ihmisten välisessä kaupassa, kuten esimerkiksi nettihuutokaupoissa ja käytettyjen autojen kaupassa. Aina reilu vaihto ei toteudu vaan toinen osapuoli saattaa menettää suuriakin summia rahaa. Nettiauto.com on ilmainen käytettyjen autojen myyntipalvelu, jossa voi tehdä myynti-ilmoituksen omasta autosta tai etsiä itselle sopivaa autoa.

Nettiautossakin toimii henkilöitä pahassa mielessä; ulkomaalainen henkilö on ostanut auton väärennetyillä shekeillä ja maksanut ylihinnan. Auton myyjä on saanut rahat vietyään shekit pankkiin ja lähettänyt auton ostajalle. Ostaja on ilmoittanut myyjälle, että hänen sihteerinsä on epähuomiossa kirjoittanut shekkiin väärän summan ja pyytää lähettämään erotuksen takaisin. Hyväuskoinen myyjä palauttaa rahat, mutta pian pankista ilmoitetaan että shekit olivat väärennettyjä, jolloin autonmyyjä menettää sekä rahansa, että autonsa.

Myös auton ostaminen voi tulla kalliiksi. Samassa nettiauto-palvelussa on myynnissä autoja epäilyttävän halvalla. Auton myyjä selittää olevansa ulkomailla, mutta auto on ostettu Suomesta ja tarjoaa siihen palautusoikeutta. Pian kuljetusyhtiöstä ilmoitetaan, että auto on heillä ja pyytää puolet kauppahinnasta etukäteismaksuna. Todellisuudessa autosta ei ole mitään takeita, mutta tarina on keksitty hyvin ja sähköpostivastaukset voivat olla hyvinkin asiallisia. Vaikka käytettyjen auton myynti tapahtuu lähes poikkeuksetta kasvotusten ja melko turvallisesti, myös epäonnistuneita reiluja vaihtoja ja huijausyrityksiä sattuu silloin tällöin.

Huuto.net on nettihuutokauppa, jossa kuka tahansa palveluun rekisteröitynyt henkilö voi myydä omaisuuttaan. Palvelu tarjoaa hyvät ohjeet turvalliseen ostamiseen: tiedot ostettavasta tuotteesta tulee lukea huolellisesti ja maksu kannattaa hoitaa postiennakolla tai noudettaessa käteisellä. Myös etukäteismaksua pyydetään useista halvemmista tuotteista. Ohjeet pyytävät tekemään rikosilmoituksen poliisille välittömästi väärinkäytön havaittua, esimerkiksi tuotetta ei lähetetä ostajalle (Huuto.net 2009). Huuto.net:iin tulee aina rekisteröityä, jolloin tarvittavat henkilötiedot on annettava palvelulle. Käyttäjille voidaan antaa positiivista tai negatiivista palautetta, joilla pyritään lisäämään luottamusta paljon tavaroita myyneisiin henkilöihin.

Huuto.net tarjoaa myös tunnistautumispalvelua matkapuhelimen tai verkkopankkitunnusten avulla. Tunnistautuneille käyttäjille tarjotaan lisäpalveluja, niihin voidaan luottaa paremmin autentikoinnin ansiosta, ja lisäksi tunnistautuminen on yksi keino rahoittaa palvelun toimintaa. Tavaroita voidaan huutokaupata myös ainoastaan tunnistautuneille henkilöille, jolloin myyjä haluaa kasvattaa luottamusta ostajaan vahvemman autentikoinnin avulla. Silti lähes kaikki ostajat ja myyjät ovat tuntemattomia yksityisiä henkilöitä, joten kaupankäynnissä tulee olla hyvin huolellinen ja varovainen. Myös verkkokaupoissa asioidessa tulee noudattaa erityistä varovaisuutta.

4. REILU VAIHTO -PROTOKOLLA

4.1. Reilun vaihdon perusprotokolla

Ray, Ray ja Natarajan ovat kehittäneet melko yksinkertaisen reilun vaihdon protokollan, joka tarvitsee toimiakseen kolmatta luotettua osapuolta (Ray et al 2005). Protokollaa voidaan käyttää esimerkiksi ostettaessa verkkokaupasta sähköisesti lähetettäviä tuotteita, kuten musiikkia, tietokoneohjelmia. Protokolla käyttää hyväkseen ns. ristiinvalidointia mm. tuotteen oikeellisuuden tarkistamisessa. Kolmas osapuoli varmistaa, että asiakas saa tuotteensa, kun hän voi osoittaa maksaneensa tuotteen.

4.1.1. Protokollan symbolit

Symboli	Selitys
TP, C, M	luotettu kolmas osapuoli (TP), asiakas (C), myyjä (M)
m	tuote
r	myyjän valitsema satunnaisluku
K_m	myyjän luoma avain TP:lle
K_{m1}	myyjän itse käyttämä avain joka vastaa edellistä avainta
K_c	asiakkaan luoma avain
PO	ostotilaus tuotteesta
PT	maksusitoumus tuotteen maksamiseen
C_{sign}, M_{sign}	C:n allekirjoitus, M:n allekirjoitus

Taulukko 4.1 Käytetyt symbolit ja niiden selitykset (Ray et al 2005, s. 276 ja Liukkonen 2002, s. 13)

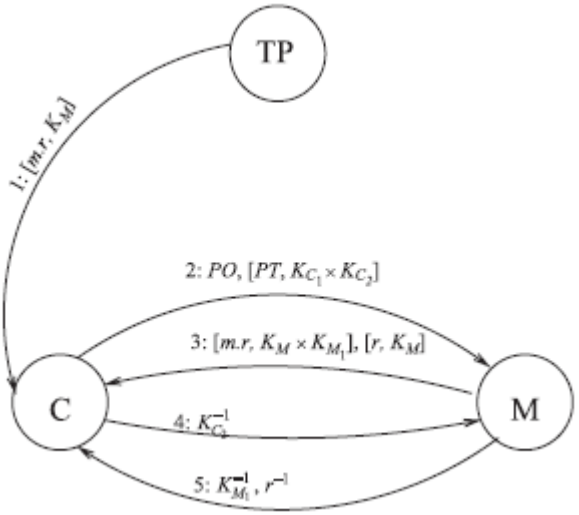
4.1.2. Protokollan toiminta

Kauppias (M) on lähettänyt aikaisemmin kaikki tuotteensa ja avaimensa kolmannelle luotetulle osapuolelle (TP). Asiakas (C) valitsee haluamansa tuotteen ja pyytää sen TP:ltä kuvan 4.1 mukaisesti (1. viesti). Tuote (m) on salattu kauppiaan valitsemalla salausavaimella (K_m), sekä kerrottu myyjän valitsemalla satunnaisella luvulla (r).

Toisessa viestissä asiakas lähettää kauppiaalle ostotilauksen tuotteesta ja maksusitoumuksen salattuna asiakkaan omalla salausavaimella. Kolmannessa viestissä kauppias lähettää tuotteen kerrottuna satunnaisluvulla ja salattuna omalla salausavaimella sekä lisäksi satunnaisluku salattuna erikseen. Nyt asiakas tarkistaa tuotteen oikeellisuuden vertaamalla TP:lta saatua salattua tuotetta kauppiaalta saatuun tuotteeseen. Asiakkaalla ei itsellään ole avainta, joten ei näe tuotetta, mutta voi verrata niitä. Jos tuotteet

täsmäävät, asiakas lähettää oman purkuavaimensa kauppiaalle (viesti 4), jolloin kauppias saa rahansa.

Viimeisessä viestissä kauppias lähettää asiakkaalle tuotteen purkuavaimen ja satunnaisluvun käänteisluvun. Ristiinvalidoinnin mukaan asiakas voi purkaa kumman tahansa saamansa tuotteen (viestissä 1 ja 3) nyt saamallaan avaimella. Teorian mukaan tuote voidaan salata toisella avaimella, tai molemmilla sekä voidaan purkaa kummalla avaimella vain. Tämä johtuu avaimien yhteisestä salauseksponentista (Liukkonen 2002).



Kuva 4.1 Reilun vaihdon perusprotokolla (Ray et al 2005, s. 277)

Jos satunnaislukua (r) ei olisi mukana, asiakas voisi tilata paljon tuotteita yhtäaikaisesti lähettämättä kuitenkaan maksumääräysten purkuavaimia ja saatuja tuotteita yrittää saada purettua löytämällä sopiva purkuavain. Koska satunnaisluku on mukana, ei riitä että löytää oikean avaimen vaan täytyy myös satunnaisluvun käänteisluvun tuntea. Oikeita purkuavaimia ei voi yrittää arvata, sillä asiakas ei voi tarkistaa mikä avain on oikea.

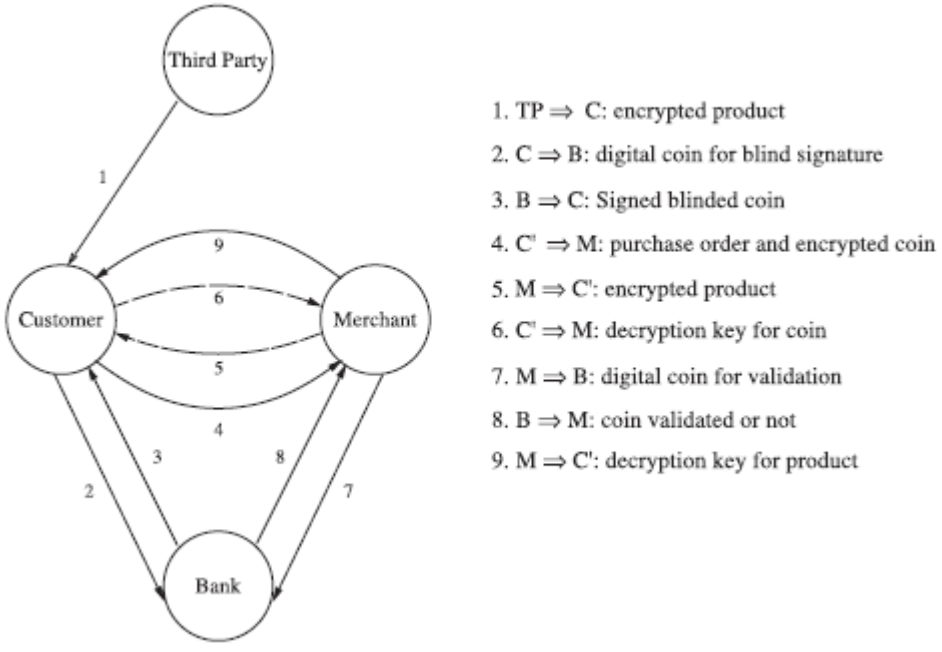
Mikäli asiakas ei saa avainta kauppiaalta, hän voi pyytää purkuavaimen myös kolmannelta osapuolelta todistettuaan maksaneensa tuotteen, eli lähettäneensä maksumääräyksen ja sen purkuavaimen. Myyjä ei lähetä purkuavainta, ennen kuin on tarkistanut maksumääräyksen oikeaksi ja saanut rahat.

Ongelmana on kuitenkin, miten asiakas todistaa lähettäneensä oikean maksumääräyksen ja purkuavaimen. Tämän takia, tai muutenkin kauppias voi olla lähettämättä viimeistä viestiä, jotta asiakas saisi tuotteensa purettua. Tämä ongelma voidaan korjata esimerkiksi niin että kauppias lähettää viimeisen viestin TP:n kautta, mutta mikäli ei tietyssä ajassa lähetä, TP lähettää sen itse. Ongelma voidaan korjata myös lähettämällä kaikki viestit kolmannen luotetun osapuolen kautta.

Jotta TP:n ei tarvitsisi olla aktiivisena osapuolena riittää, että asiakas lähettää TP:lle muutaman viestin. Ensinnä asiakas lähettää allekirjoitetun ostotilauksen hash-funktion kauppiaalle, joka myös allekirjoittaa sen ([H(PO), C_{sign}]M_{sign}) ja lähettää asiakkaan kautta TP:lle todistukseksi mitä ollaan ostamassa sekä tietysti myös tiedon kuka kauppias on kyseessä. Asiakkaan täytyy lähettää TP:lle myös kauppiaan allekirjoittamat hash-funktiot salatusta tuotteesta ([H(m·r, K_M·K_{M1})] M_{sign}) ja salatusta satunnaisluvusta ([H(r, K_M)]M_{sign}), jotka hän saa kolmannessa viestissä. Kauppias lähettää myös maksumääräyksen salattuna asiakkaan avaimella ja asiakkaan allekirjoittamana ([PT, K_C]C_{sign}), jonka kauppias saa aluksi (Ray et al 2005, s. 279). Nämä hash-funktiot todistavat että kaksi ensimmäistä viestiä on vaihdettu, mutta ne eivät todista onko maksumääräys oikea, onko asiakas lähettänyt purkuavaimen tai onko viestit edellisistä ostoksista saatuja. Lisäksi asiakas voi yrittää purkaa kauppaa, kun purettuaan tuotteen salauksen ja väittämällä että se ei ole oikea tuote.

4.2. Anonyymi reilu vaihto -protokolla

Ray ym. ovat kehittäneet myös toisen, melko samankaltaisen reilun vaihdon protokollan ja esitelleet sen samassa artikkelissa (Ray et al 2005). Se eroaa edellisestä protokollasta sen verran, että asiakas pysyy anonyyminä, eikä kauppias saa selville edes asiakkaan pankkiyhteyttä. Protokolla tarvitsee toimiakseen bittikäteistä (Koskinen 2009).



Kuva 4.2 Anonyymi reilu vaihto (Ray et al 2005, s. 284)

Ensimmäinen viesti TP:ltä asiakkaalle on sama kuin aiemmassa protokollassa, viestissä on tuote salattuna. Ja samoin kuin perusprotokollassa, kauppias on lähettänyt kolman-

nelle osapuolelle aikaisemmin tuotteensa kryptattuna luomallansa avaimella. Toisessa viestissä asiakas lähettää pankille sokaistun bittisetelin. Pankki veloittaa asiakkaan tililtä, allekirjoittaa setelin ja lähettää sen takaisin asiakkaalle, joka poistaa sokaisun.

Tämän jälkeen asiakas toimii anonyymisti lähettäessään viestejä kauppiaalle. Ensimmäisessä viestissä on perusprotokollan tavoin ostotilaus, mutta salatun maksumääräyksen tilalla salattu bittiraha. Viidennessä viestissä kauppias lähettää asiakkaalle salatun tuotteen, jota asiakas vertaa TP:ltä saamaansa tuotteeseen. Jos tuote täsmää TP:ltä saadun tuotteen kanssa, asiakas lähettää bittisetelin purkuavaimen kauppiaalle.

Seitsemännessä viestissä kauppias lunastaa omalta pankiltaan digitaalisen rahan ja saa vastauksen rahan pätevyydestä. Mikäli raha on oikea, kauppias lähettää tuotteen purkuavaimen asiakkaalle.

Tässä protokollassa kauppias voi heti varmistaa pankista, että bittiraha on oikea. Perusprotokollan parannusehdotuksessa esitetyt viestien allekirjoitetut hash-funktiot lähetetään ko. viestien mukana (Ray et al 2005, ss. 285-286). Näin voidaan todistaa, mitä viestejä on lähetetty. Yksi protokollan eduista on se, että jotkin reiluuteen liittyvät riidan voidaan selvittää automaattisesti. Erityisesti TP voi toimittaa tuotteen, jos C toimittaa sille näytön maksusta eikä kauppias vastaa. Tällöin TP:n ei pidä antaa tuotteen avainta K_M vaan pelkkä tuote, jotta kauppiaan muut tuotteet eivät vaarannu. (Koskinen 2008). Myyjä voi yrittää toimia virheellisesti ja olla lähettämättä purkuavainta, mutta kun kyse on sähköisesti lähetettävästä tuotteesta, sen kopioimisesta ja myymisestä ei kauppiaalle tule kustannuksia. Tästä johtuen ei ole mitään estettä miksi kauppias ei lähettäisi purkuavainta. Kauppiaan ei kannata olla lähettämättä myöskään sen takia, että huono maine leviää nopeasti ja kauppa ei menesty.

Protokolla vaatii pankkien lähtemistä mukaan bittikäteisen käyttämiseen ja luomiseen. Tämä vaatii kaikilta pankeilta panostuksia ja investointeja sekä sähköisen rahan yleisempää käyttöä. Protokolla voitaisiin rakentaa myös maksumääräysten tms. ympärille, mutta anonyymius kärsisi.

5. YHTEENVETO

Reilua vaihtoa pyritään varmistamaan erilaisilla toimitus- ja maksutavoilla. Vastuuta pyritään usein myös jakamaan kolmannelle osapuolelle. Vahva autentikointi ja riitauttamisen mahdollisuus parantaa myös reilun vaihdon toteutumista. Protokollia on kehitelty varmistamaan reilun vaihdon toteutumista, mutta niiden yleistyminen on vielä kyseenalaista. Herää kysymys, onko protokollille edes tarvetta, kun tuotteita voidaan lähettää postiennakolla, maksaa turvallisella tavalla ja autentikoitua sekä viime kädessä voidaan myös riitauttaa asia ja ratkaista se tuomioistuimessa.

Reilun vaihdon protokollissa tarvitaan kolmatta luotettua osapuolta, mutta myös ilman protokollaa on hyvä olla kolmas osapuoli. Se voi olla jonkinlainen palveluntarjoaja, maksettaessa esimerkiksi aiemmin esitelty Suomen Maksuturva tai luottokorttiyhtiöt, jotka tarjoavat charge back -palvelua. Kolmas osapuoli haluaa itsekin hyötyä, joten sen käyttäminen voi olla kallista, mikäli se joutuu toimimaan aktiivisena osapuolena. Tämän takia protokollat on suunniteltukin niin, että kolmatta osapuolta tarvitaan vain ristiriitatilanteissa.

Kolmas luotettu osapuoli on protokollassa melko teoreettinen. Se on kauppiaan valitsema, joten varmasti kauppias siihen luottaa, mutta asiakas ei välttämättä. Kolmansia osapuolia tulisi olla useampi, joista asiakas voisi valita luotettavimman, jotta molemmat voisi luottaa siihen. Protokollassa ei ole myöskään kerrottu tarkemmin minkälainen toimija kolmas osapuoli olisi.

Selkeä reilu vaihto -protokollan etu on anonyymius. Kauppaa on vaikea, ellei mahdotonta käydä täysin anonyymisti ilman toimivaa reilun vaihdon protokollaa. On hyvin tavallista, että verkkokaupoissa pitää rekisteröityä ja antaa kaikki henkilötiedot, ennen kuin voi tehdä ostoksia. Rekisteröidyistä käyttäjistä tulee kuitenkin henkilörekisteri, jota suojaa henkilötietolaki. Kuitenkin on selvää, että anonyyminä toimiminen on turvallisempaa asiakkaan näkökulmasta, mikäli se on mahdollista.

Reilua vaihtoa varmistamaan on luotu erilaisia menetelmiä ja protokollia. Tulevaisuudessa varmasti protokollat tulevat yleisempään käyttöön, kun niitä edelleen kehitellään. Verkkokaupoissa kuitenkin kauppiaan tulee olla rehellinen, muuten ei voi menestyä liiketoiminnassa. Tästä johtuen asiakas voi yleensä luottaa kauppiaaseen, kun se on vähänkin tunnettu ja ihmisten tiedossa.

LÄHTEET

Huuto.net 2009. Kuinka teen huuto.netissä kauppaa turvallisesti? Huuto.net-verkkohuutokauppa. Saatavilla [http://huuto.net/fi/ohje-turvallisesti.php3]. Viitattu: 2.5.2009.

Koskinen, J. 29.4.2004. Erityisiä allekirjoituksia, Tietoturvallisuuden jatkokurssin verkkomateriaali. Saatavilla: [http://sec.cs.tut.fi/maso/materiaali.php?id=328]. Viitattu: 23.4.2009.

Koskinen, J. 2008. Reilu vaihto, kurssin TLT-3400 Kryptoprotokollat luentomateriaali, 9. luento. Saatavilla [http://www.cs.tut.fi/kurssit/TLT-3400/b-luento-9.html]. Viitattu 29.4.2009.

Koskinen, J. 2009. Anonyymin bittikäteisen laajennuksia, kurssin TLT-3400 Kryptoprotokollat luentomateriaali, 3. luento. Saatavilla [http://www.cs.tut.fi/kurssit/TLT-3400/luento3.html]. Viitattu 7.5.2009.

Liukkonen, J. 2002. Anonyymi ja Reilu Elektroninen Kaupankäynti. Seminaarityö. Tampereen teknillinen korkeakoulu, tietoliikennetekniikan osasto, kurssi: 8306500 tietoturvaprotokollat. 24 sivua.

Pagnia, H., Vogt, H., Gärtner, F. C. 2003. Fair Exchange. The Computer Journal, 2003, vol 46, Issue 1, pages 55-75.

Ray, I., Ray, I., Natarajan, N. 2005. An anonymous and failure resilient fair-exchange e-commerce protocol. Decision Support Systems. Vol. 39, Issue 3, May 2005, pages 267-292.

Suomen Maksuturva, 12.2.2009. Verkosta ostaminen pian entistä helpompaa ja turvallisempaa, tiedote. Saatavilla: [https://www.maksuturva.fi/documents/Maksuturva_lehdistotiedote_20090212.pdf]. Viitattu: 23.4.2009.

TIEKE, Tietoyhteiskunnan kehittämiskeskus Ry: Maksu- ja toimitustavat. Saatavilla: [http://www.tieke.fi/julkaisut/oppaat_kansalaisille/ostoksilla_verkkokaupassa/onnistu_ostoksilla/maksu-ja_toimitustavat/]. Viitattu: 23.4.2009.