TAMPEREEN TEKNILLINEN YLIOPISTO

**SANTERI SILTALA**

# KIISTÄMÄTTÖMYYSPROTOKOLLAT

Kandidaatintyö

Tarkastaja: Pekka Uotila

# TIIVISTELMÄ

TAMPEREEN TEKNILLINEN YLIOPISTO
Signaalinkäsittelyn ja tietoliikennetekniikan koulutusohjelma
**SILTALA, SANTERI**: Kiistämättömyysprotokollat
Kandidaatintyö, 22 sivua.
Kesäkuu 2010
Pääaine: Tietoliikennetekniikka
Tarkastaja: Pekka Uotila
Avainsanat: Kiistämättömyys, tietoturva, protokolla

Tässä työssä tutustutaan lyhyesti kiistämättömyyden käsitteeseen ja tarkoitukseen sähköisessä kaupankäynnissä. Verkossa tapahtuva asiointi, etenkin maksaminen, vaatii nykypäivänä keinon sitoa osapuolet tehtyyn sopimukseen tai kanssakäymiseen. Tämän avuksi on kehitetty kiistämättömyysprotokollia. Näiden avulla osapuolet voivat varmistua toistensa identiteetistä, eivätkä voi kiistää osallistuneensa kanssakäymiseen sen päätyttyä.

Esiteltävänä on kolme erilaista protokollaa, joilla osapuolten välinen kiistämättömyys voidaan saavuttaa. Protokollista esitellään lyhyesti niiden toiminta, sekä arvioidaan subjektiivisesti niiden soveltuvuutta sähköisen kaupankäynnin tukena.

Yhdestäkään tässä työssä käsitellystä protokollasta ei ollut sellaisenaan ratkaisemaan kaikkia sähköiseen kaupankäyntiin liittyviä ongelmia. Protokollien turvallisuus ja tehokkuus riippuvat myös huomattavasti käytettävästä kryptoalgoritmista. Myöskään yksikään protokollista ei ottanut kantaa vuorovaikutukseen olemassa olevien protokollien kanssa.

# SISÄLLYS

# TERMIT JA NIIDEN MÄÄRITELMÄT

| | |
|---|---|
| **CA** | Certificate Authority; *Varmentaja. Myöntää varmenteita niitä tarvitseville osapuolille.* |
| **CE** | Central Entity; *Palveluntarjoaja. Maksua vaativan palvelun tarjoaja.* |
| **DSA** | Digital Signature Algorithm; *Algoritmi digitaalisten allekirjoitusten luomiseen.* |
| **IAA** | Information Archiving Authority; *Luotettava tietovarasto. Säilöö osapuolten välisessä sopimuksessa syntyviä kiistämättömyystodisteita.* |
| **IP** | Internet Protocol; *Verkkokerroksen protokolla.* |
| **MD5** | Message Digest; *Viestitiivistealgoritmi.* |
| **NA** | Notary Authority; *Notaaripalvelu. Toimii avustavana osapuolena asiakkaan ja palveluntarjoajan välisten sopimusten luomisessa* |
| **RSA** | Rivest, Shamir, Addleman; *Epäsymmetrinen julkisen avaimen salausalgoritmi.* |
| **SHA** | Secure Hash Algorithm; *Kryptografinen tiivistefunktio.* |
| **SSL** | Secure Sockets Layer; *Salausprotokolla, jolla voidaan suojata Internet-sovellusten tietoliikenne IP-verkkojen yli.* |
| **TCP** | Transmission Control Protocol; *Yhteydellinen kuljetuskerroksen protokolla* |
| **TLS** | Transport Layer Security; *Uudempi versio SSL:sta.* |
| **TTP** | Trusted Third Party; *Luotettu osapuoli. Varmistaa viestinnän osapuolien identiteetit toisilleen.* |
| **VOD** | Video on Demand; *Tilausvideopalvelu. Asiakas voi halutessaan ostaa videovirtaa palveluntarjoajalta.* |
| **WLAN** | Wireless Local Area Network; *Langaton lähiverkkotekniikka.* |

# 1 JOHDANTO

Tässä kandidaatintyössä luodaan yleiskatsaus olevassa oleviin kiistämättömyysprotokolliin. Suurin osa näistä on olemassa vasta konseptuaalisella tasolla, eikä niitä ole vielä implementoitu mihinkään oikeaan sovellukseen. Usean protokollan toiminta-ajatus on pohjimmiltaan sama, ja suurin osa löytyneistä julkaisusta sisälsikin ainoastaan pieniä parannuksia olemassa oleviin toteutuksiin. Tähän työhön on valittu ne protokollat, jotka pyrkivät tuomaan jotain uutta perinteisiin toteutuksiin.

Toteutusten osalta on perehdytty erityisesti siihen, mitä uusia haasteita kiistämättömyys sisältää sähköisessä ympäristössä verrattuna perinteiseen kanssakäyntiin. Näitä ovat mm. osapuolten identiteetin varmistus, kiistämätön sitominen maksutapahtumiin ja osapuolten anonymiteetin säilyttäminen.

Kunkin protokollan esittelyssä kuvataan ensin lyhyesti ongelma, jonka ratkaisuun se pyrkii, itse protokollan toteutus, sekä analysoidaan sen soveltuvuutta sähköisen kaupankäynnin eri tarkoituksiin. Huomiota on myös kiinnitetty protokollan toimivuuteen mobiililaitteilla, jotka asettavat haasteita protokollan suorituskyvylle.

# 2 KIISTÄMÄTTÖMYYDEN TARKOITUS

Kiistämättömyyden tarkoituksena on varmistaa, että viestintään tai sopimukseen osallistuneet osapuolet eivät jälkikäteen voi kiistää olleensa mukana kanssakäymisessä. Epärehellinen osapuoli voi joko kiistää osallistuneensa kanssakäymiseen ylipäätään tai väittää tehtyä varmistusta, esimerkiksi allekirjoitusta, väärennetyksi.

Kiistämättömyyspalveluita tarvitaan pääasiallisesta verkossa käytävän liiketoiminnan tukena. Sähköisessä kanssakäymisessä osapuolten identiteetistä on huomattavasti vaikeampi varmistua. Lisäksi osapuolten on helpompi kiistää osallistuneensa sopimukseen. Näin ollen tarvitaan menettely, jolla osapuolet voidaan sitoa luotettavasti tehtyyn sopimukseen tai näiden väliseen viestintään. Etenkin rahaliikenteessä on tärkeää, että kumpikaan liiketoimintaan osallistunut osapuoli ei pysty kiistämään liiketointa.

Perinteisissä tilanteissa kiistämättömyyden varmistamiseen on käytetty osapuolten allekirjoitusta. Samalla myös osapuolet ovat helposti voineet varmistua toistensa identiteetistä, koska sopimus on tehty jossain fyysisessä paikassa. Lisäksi kumman tahansa osapuolen on ollut helppo vetäytyä tilanteesta, jos kanssakäymisen yhteydessä on havaittu epärehellisyyttä. On kuitenkin mahdollista, että jälkeenpäin toinen osapuolista voi väittää esimerkiksi allekirjoituksen olevan väärennetty. Näin ollen myös perinteisessä sopimustilanteissa tarvitaan jonkin luotettavan osapuolen, esimerkiksi notaarin tai lakimiehen mukanaoloa.

Kiistämättömyys pyrkii siis luomaan todisteet tietojen eheydestä, alkuperästä ja koskemattomuudesta, jotka jokin kolmas osapuoli voi tarvittaessa varmentaa. Taulukossa 1 on kuvattu ominaisuuksia, joita kiistämättömyysprotokollan tulee toteuttaa. Tyypillisesti kiistämättömyydessä ovat mukana ainakin seuraavat toimijat [1]:

- Lähettäjä. Toimii viestin alkuperäisenä lähettäjänä. Lähettäjän tulee kiistämättömyydessä taata todisteet siitä, että on alunperin lähettänyt viestin.
- Vastaanottaja. Vastaanottaja vastaanottaa lähettäjän lähettämän viestin. Vastaanottajan tulee taata todisteet siitä, että on vastaanottanut alunperin lähetetyn viestin.
- Välittäjä. Tyypillisesti osapuolten välillä oleva tietoverkko. Välittäjän tulee taata todisteet siitä, että on välittänyt lähettäjältä saaneensa viestin vastaanottajalle. Tai vaihtoehtoisesti todisteet siitä, että se on välittänyt viestin edelleen vastaanottajalle.
- Luotettu taho. Varmentaa osapuolten identiteetit. Lisäksi voi säilöä viestinnästä kertyneitä todisteita.

**Taulukko 1. Kiistämättömyyden vaatimukset [2].**

| Vaatimus | Kuvaus |
|---|---|
| Todisteet lähettäjästä. | Lähettäjä ei voi kiistää olleensa mukana kanssakäymisessä ja siihen liittyvässä viestinnässä ja sen sisällössä. |
| Todisteet vastaanottajasta. | Vastaanottaja ei voi kiistää olleensa mukana kanssakäymisessä tai saaneensa siihen liittyviä viestejä. |
| Todisteet toimittajasta. | Viestin välittäjä ei voi kiistää hyväksyneensä viestiä välitettäväksi. |
| Todisteet toimituksesta. | Viestin välittävä taho (verkko) ei voi kiistää välittäneensä viestiä vastaanottajalle. |
| Todisteet omistajuudesta. | Kolmas osapuoli ei voi väittää omistavansa viestinnässä käytettyä tietoa. |
| Todisteet siirrosta. | Tarkastelee viestin välittävien tahojen luotettavuutta. |
| Todisteet noudosta. | Tarkastelee tiedon välittäjän ja lähettäjän välisen toiminnan haavoittuvuutta |
| Todisteet hyväksynnästä. | Viestin vastaanottaja ei voi kiistää vastaanottaneensa ja hyväksyneensä viestiä. |

## 2.1 Sähköinen kaupankäynti

Sähköisten tuotteiden kaupankäynnin yhteydessä ongelma on esimerkiksi sellainen, että asiakas haluaa ostaa digitaalisen tuotteen verkossa olevasta liikkeestä, eikä halua maksaa, ennen kuin on saanut tuotteen haltuunsa. Toisaalta kauppias ei halua luovuttaa tuotetta, ennen kuin on saanut maksun. Jos kauppias luovuttaa tuotteen ennen maksua, voi epärehellinen asiakas kadota maksamatta ja epärehellinen kauppias voi puolestaan jättää tuotteen toimittamatta maksun saatuaan.

Toisenlainen ongelma on mikromaksaminen. Asiakas haluaa esimerkiksi käyttää WLAN-yhteyttä tietyn ajan. Jos asiakas maksaa koko käyttöajasta kerralla, voi syntyä tilanne, että yhteys katkeaa teknisen vian takia. Näin ollen asiakas joutuu maksamaan turhaan käyttämättömästä ajasta. Lisäksi asiakkaan on erittäin vaikea todistaa, koska yhteys vikaantui. Tällaiseen tilanteeseen sopii paremmin perinteisessä puhelinliikenteessä käytetty laskutusmalli, jossa maksetaan yhteyden käytöstä sitä mukaa, kun palvelua saadaan. Kiistämättömyysprotokollan avulla palveluntarjoaja voi näyttää toteen, että asiakas on todellakin saanut palvelua ja toisaalta asiakas voi helposti lopettaa käytöstä maksamisen, jos ei mielestään saa tyydyttävää palvelua.

## 2.2 Viestintä

Myös osapuolten välisessä viestinnässä voi syntyä kiistämättömyyden tarve. Esimerkiksi tehtäessä sähköpostin välityksellä sopimus voi syntyä tilanne, jossa toinen osapuoli jälkikäteen alkaa väittämään, ettei ole suostunut siihen tai kiistää koko sopimuksen olemassaolon. Epärehellinen osapuoli voi myös yrittää esiintyä väärällä identiteetillä sopimuksen luontivaiheessa. Myös päinvastoin ajateltuna, joskus voi olla tarve osoittaa, ettei osapuoli ole koskaan lähettänyt tiettyä viestiä.

## 2.3 Sähköinen allekirjoitus

Tyypillisesti osapuolet sitoutuvat viestintään kiistämättömästi sähköisellä allekirjoituksella. Suomen laki määrittelee sähköiselle allekirjoitukselle tiettyjä ehtoja, jotta sen katostaan olevan oikeudellisesti pätevä. Allekirjoituksen luomistietojen tulee olla ainutkertaisia ja niiden tulee säilyä luottamuksellisina. Lisäksi luomistietoja ei saa pystyä päättelemään muista tiedoista. Allekirjoituksen on myös oltava suojattu väärentämiseltä ja allekirjoittajan tulee voida suojata luomistiedot muiden käytöltä. Luomisväline ei myöskään saa muuttaa allekirjoitettavia tietoja tai estää niiden esittämistä allekirjoittajalle ennen allekirjoitustapahtumaa.

Sähköinen allekirjoitus kelpaa oikeustoimeen, jossa vaaditaan allekirjoitus. Sen suositellaan perustuvan laatuvarmenteeseen ja lisäksi täyttämään yllä olevat ehdot. Sähköiseltä allekirjoitukselta ei kuitenkaan evätä suoraan oikeusvaikutuksia, vaikka edellä mainitut ehdot eivät täyttyisi. [3]

# 3 KIISTÄMÄTTÖMYYSPROTOKOLLAT

Kiistämättömyysprotokollan tehtävänä on esittää luotettava toimintamalli luvussa kaksi esitettyjen ongelmien ratkaisemiseen. Kiistämättömyysprotokollat voidaan jakaa toiminnaltaan kahteen pääkategoriaan: Ensimmäisessä kanssakäymisen osapuolet sisällyttävät kiistämättömyystodisteet viestintään palasina vuorotellen, jolloin voidaan varmistaa viestin lähettäjän ja vastaanottajan osallistuminen kanssakäymiseen, kun kanssakäyminen on päättynyt [4]. Toinen tapa on luvussa kaksi esitelty luotetun tahon hyödyntäminen.

## 3.1 Kiistämättömyystodisteet viestinnän mukana

Ensimmäinen tarkasteltava protokollatyyppi perustuu siihen, että salaisuutta paljastetaan palanen kerrallaan viestien mukana. Viestinnän alkaessa osapuolet sopivat siitä, minkä tyyppistä salaisuutta viestinnässä käytetään, kuitenkaan paljastamatta itse salaisuutta. Joka kierroksen jälkeen osapuolten on todistettava, että jaettu palanen, esimerkiksi bitti, on osa jaettavaa salaisuutta. Tämä menetelmä vaatii mm. sen, että molemmilla osapuolilla on suurin piirtein saman verran prosessointitehoa käytössään. Yksi mahdollinen toteutus tämän tyyppiselle kiistämättömyydelle on, että osapuolet muodostavat julkiset avaimet salaisuuden perusteella. Tämän jälkeen ne paljastavat salaisuudesta jotain, jolla jokaisen viestinvaihdon jälkeen voidaan varmentaa, että vaihdettu palanen on varmennettu salaisuuden osalla. Salaisuus voi olla esimerkiksi alkulukupari. Viestinnän päätteeksi salaisuus on paljastunut, jolloin voidaan varmistaa täysin, että kaikki palaset on varmennettu salaisuuteen kuuluvalla osalla.

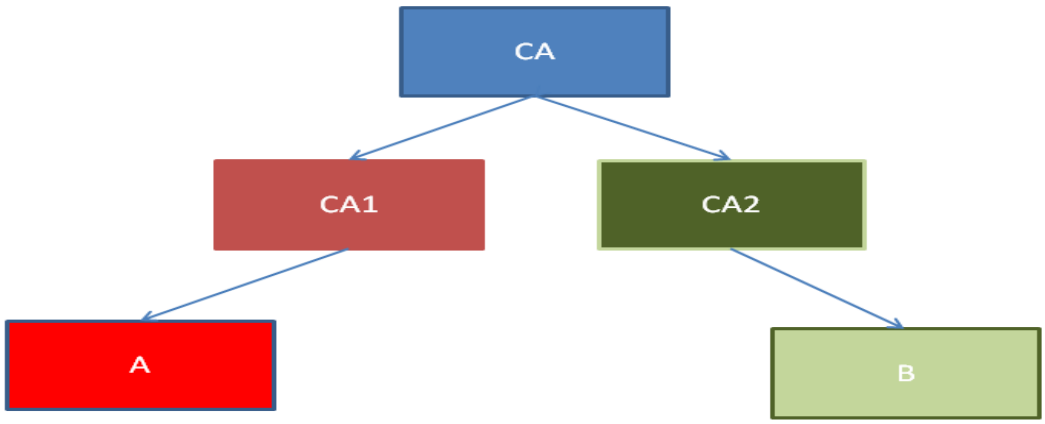
## 3.2 Luotettu taho varmistaa osapuolet

Luotettu osapuoli varmentaa lähettäjän ja vastaanottajan julkiset avaimet esimerkiksi sertifikaatilla. Kuvassa 1 on esitelty esimerkki sertifikaatista, jollaisia luotetut tahot voivat myöntää. Molempien osapuolten tulee luottaa samaan luotettuun tahoon, tai samassa luottamusketjussa oleviin luotettuihin tahoihin.

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Jul  9 16:04:02 1998 GMT
            Not After : Jul  9 16:04:02 1999 GMT
        Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=www.freesoft.org/Email=baccala@freesoft.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
        5a:de:9d:ea:63:cd:cb:cc:6d:5d:01:85:b5:6d:c8:f3:d9:f7:
        8f:0e:fc:ba:1f:34:e9:96:6e:6c:cf:f2:ef:9b:bf:de:b5:22:
        68:9f
```

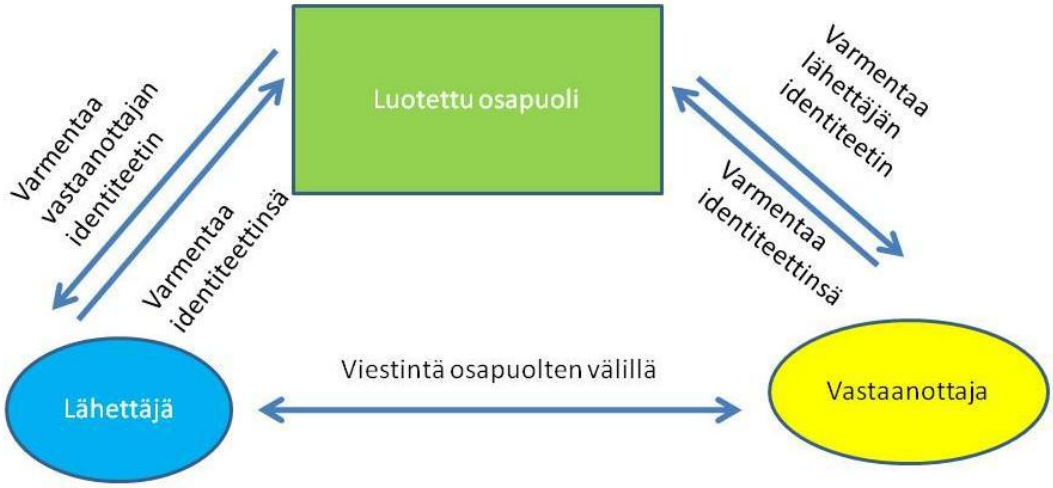
**Kuva 1. Esimerkki sertifikaatista.**

Kuvassa 2 on esitetty varmentajaketju. Vastaanottaja voi luottaa varmentajaan A ja lähettäjä varmentajaan B, koska molemmilla varmentajilla on ketjussa sama juurivarmentaja CA.




**Kuva 2. Varmentajaketju.**

Allekirjoittamalla sertifikaatin luotettu osapuoli varmistuu osapuolen identiteetistä ja että avain kuuluu todellakin kyseiselle osapuolelle. Ongelmaksi voi muodostua se, kuinka luotettu taho voi luottaa siihen osapuoleen, jolle on myöntämässä allekirjoitusta. Toisin sanoen epärehellinen osapuoli voi yrittää huijata identiteettinsä luotetulle taholle. Nyt toisen osapuolen riittää vain varmistaa luotetun osapuolen allekirjoitus, jolloin se voi varmistua avaimen omistajan identiteetistä ja viestintä voi alkaa. Osapuolet allekirjoittavat jokaisen viestinsä yksityisellä avaimellaan. Kuvassa 3 on esitelty luotetun tahon toiminta.




**Kuva 3. Luotettu taho varmentaa osapuolten identiteetin.**

## 3.3 Protokollien arviointikriteerejä

Protokollien arviointiin voidaan käyttää useita erilaisia tapoja. Tässä työssä mukaan on otettu taulukossa 2 esitetyt ominaisuudet [5]. Taulukko on laadittu subjektiivisesti, koska objektiivisesti arviointi on kyseissä tapauksessa erittäin hankalaa muuten kuin suorituskyvyn, salauksen ja allekirjoituksen osalta. Kiistämättömyysprotokollat hyödyntävät tyypillisesti kryptografisia algoritmeja. Näin ollen kiistämättömyysprotokollan luotettavuus on melko pitkälti sidonnainen käytettävän kryptografisen algoritmin luotettavuuteen. Tyypillisesti vahvemman algoritmin käyttö tuo paremman luotettavuuden, mutta samalla suorituskyky kärsii.

Protokollia on myös arvioitu eri käyttötarkoituksiin soveltuvuuden perusteella. Tyypillinen käyttökohde saattaa olla mobiililaite, jolloin protokollan tekemien allekirjoitusten ja salausten määrä viestinnässä on tärkeä arviointikohde. Operaatioiden määrä ja raskaus vaikuttaa laitteen virrankulutukseen. Toisaalta tämän perusteella voidaan myös arvioida, kuinka monta asiakasta tietyn suorituskyvyn omaava palvelun pystyy käsittelemään samanaikaisesti laadun kärsimättä huomattavasti.

**Taulukko 2. Kiistämättömyysprotokollien arviointikriteerejä.**

| **Ominaisuus** | **Heikko** | **Keskitaso** | **Vahva** |
|---|---|---|---|
| Sitominen | Perustuu toiseen osapuoleen tai luotettuun tahoon. | Perustuu kansainvälisesti arvostettuun luotettuun tahoon. | Fyysisesti sidottu kanssakäymiseen ainutlaatuisella tunnisteella tai todisteella, jonka luotettu taho on säilönyt. |
| Peukaloimattomuus (Allekirjoittajan kone on koskematon) | Allekirjoitus on helppo väärentää. | Allekirjoitus on vaikea väärentää. | Allekirjoitus on mahdotonta väärentää. |
| Muunneltavuus | Viesti on helppo vaihtaa huomaamatta. | Viesti voidaan vaihtaa useamman tietokoneen avulla. | Viestiä ei voi vaihtaa. |
| Varmennettavuus | Suora varmennus, verrataan, onko allekirjoitusavain sama. | Epäsuora varmennus, tarvitaan erityistä menettelyä, kuten tiettyä matemaattista algoritmia, allekirjoituksen varmentamiseen. | Varmennukseen tarvitaan luotetun tahon apua. Luotetun tahon tulee olla saavutettavissa tarkistushetkellä, että mahdollinen revokointi havaitaan. |

Lisäksi arviointikriteereissä oletetaan, että luotettua tahoa voidaan pitää koskemattomana ja että luotettu taho on pystynyt varmistamaan osapuolten identiteetin luotettavasti.

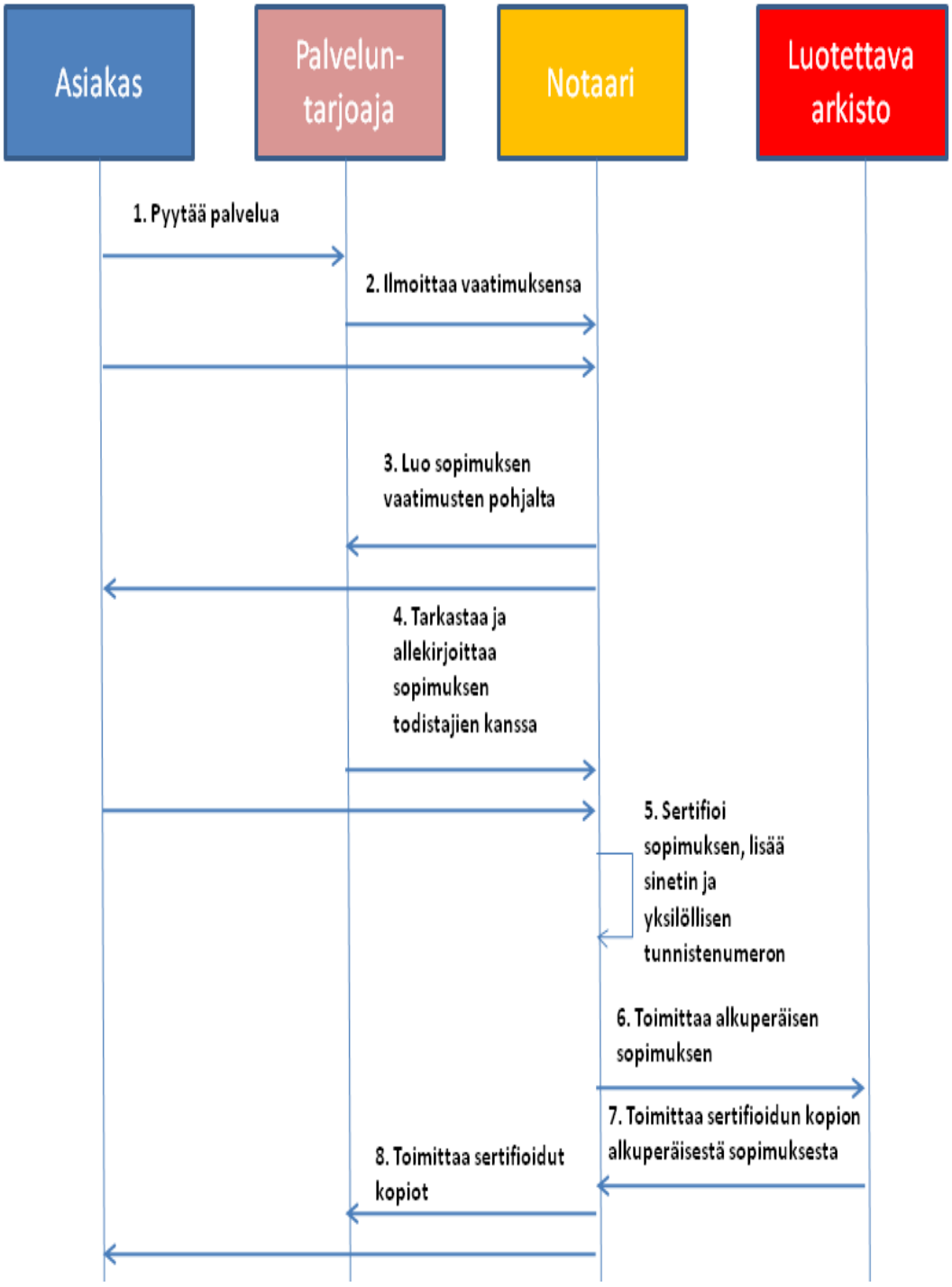
# 4 KIISTÄMÄTTÖMYYSPROTOKOLLIEN TOTEUTUKSIA

Kiistämättömyyden toteutukseen on kehitetty useita eri protokollia. Kuitenkaan tällä hetkellä yksikään ei ole vielä yltänyt standardin tasoiseen toteutukseen. Usein kiistämättömyyden toteutus on tilannekohtaista, jolloin yleispätevän protokollan suunnittelu on erittäin vaikeaa. Tässä luvussa esitellään kuitenkin muutamia mahdollisia toteutuksia. Toteutuksissa on pääasiallisesti keskitytty siihen, kuinka verkossa tapahtuva kaupankäynti ja erityisesti maksuliikenne voidaan toteuttaa kiistämättömästi.

## 4.1 Kiistämättömyyden tehokkaasti sähköisessä ympäristössä toteuttava protokolla

Toteutuksessa on pyritty luomaan menettely verkossa tapahtuvan kertaluonteisen tapahtuman toteuttamiseen. Protokollan toteutuksessa lähtökohtana on käytetty perinteistä menettelyä kiistämättömyyden toteuttamiseen. Lisäksi on pyritty parantamaan yleisesti käytössä olevien SSL(Secure Sockets Layer)/TLS(Transport Layer Security)-protokollien kiistämättömyysominaisuuksia. Joitain muutoksia on kuitenkin tehty tehokkuuden parantamiseksi. Perinteinen kiistämättömyysprosessin kulku on esitelty kuvassa 4. [6]

Menettelyyn tarvitaan kuitenkin useita osapuolia, koska asiakkaan ja palveluntarjoajan lisäksi mukana on notaari, todistajat molemmilta osapuolilta, sekä arkisto. Lisäksi signalointia tulee suhteellisen runsaasti. Todistearkistona voisi toimia esimerkiksi pankki tai vastaava luotettavaksi tiedetty taho.

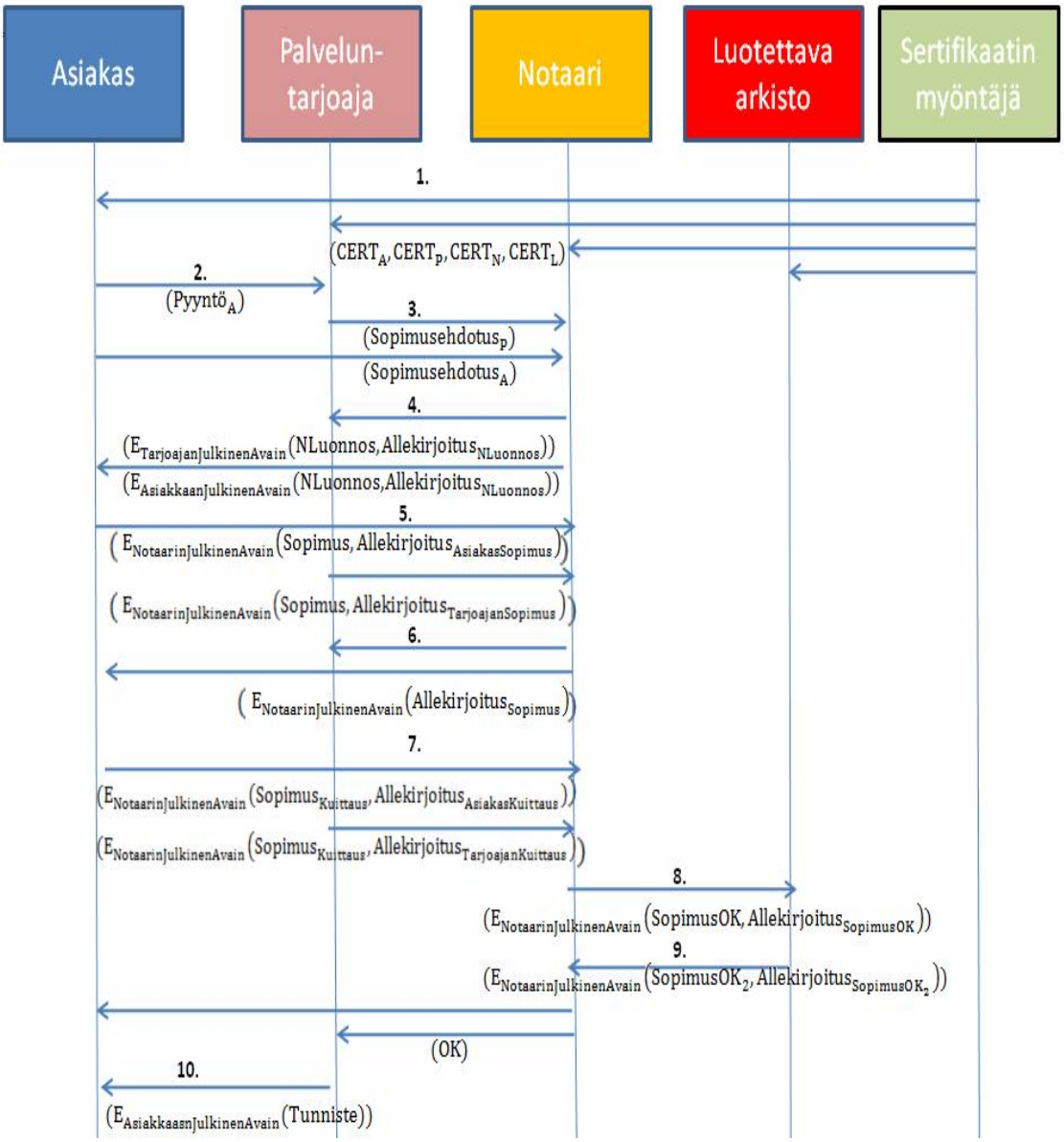



**Kuva 4. Perinteinen kiistämättömyyden toteutus lähdettä [6] mukaillen.**

Toiminnassa oletetaan, että notaari ja todistearkisto ovat täysin luotettavia. Tosielämässä näin ei kuitenkaan ole.

### 4.1.1 Toteutus

Protokollan toteutuksessa on alkuperäisten osapuolten lisäksi mukana CA (Certificate Authority), jonka tehtävänä on varmentaa molempien osapuolten sähköiset allekirjoitukset. Näin ollen CA toimii molemmille osapuolille todistajan roolissa verrattuna perinteiseen malliin. Mukana ovat lisäksi NA (Notary Authority) ja IAA (Information Archiving Authority), joista NA toimii notaarin roolissa. Tämä tarkoittaa käytännössä sitä, että NA toimii luotettavana tahona, eli avustaa sopimuksen luomisessa. IAA toimii puolestaan luotettavana todistearkistona. IAA allekirjoittaa ja kryptaa säilömänsä sopimukset, joten voidaan olettaa, että ne säilyvät peukaloimattomana. Palveluntarjoaja voi olla rekisteröityneenä useammalle notaarille, mutta yhtä notaaria kohden voi olla vain yksi todistearkisto.




**Kuva 5. Protokollan sekvenssikaavio.**

Kuvassa 5 on esitetty protokollan toiminta eri vaiheissa sopimuksen syntymisessä. Ensimmäisessä vaiheessa sertifikaattitaho myöntää kaikille osapuolille (asiakkaalle, palveluntarjoajalle, notaarille ja luotettavalle tietovarastolle) sertifikaatit ($CERT_A, CERT_P, CERT_N, CERT_L$). Toteutuksessa ei ole otettu kantaa siihen, kuinka kyseiset osapuolet ovat aiemmin todistaneet identiteettinsä varmenteet myöntävälle taholle. Varmenteet on toimitettu osapuolille ennen viestinnän alkua.

Toisessa vaiheessa asiakas pyytää haluamaansa palvelua palveluntarjoajalta. Tämän pyynnön perusteella palvelun tarjoaja tekee asiakkaalle sopimusehdotuksen palvelun käytöstä.

Vaiheessa kolme asiakas ja palveluntarjoaja toimittavat sopimusehdotuksen valitulle notaarille. Kohdassa neljä notaari valmistelee tämän perusteella sopimusehdotuksen ja allekirjoittaa sen omalla yksityisellä avaimellaan($Allekirjoitus_{NLuonnos}$), jossa ($Allekirjoitus_{NLuonnos} = (E_{NotaarinYksityinenAvain}(H(Luonnos))$. Asiakkaalle lähtevä versio salataan asiakkaan julkisella avaimella. ja palveluntarjoajalle lähtevä versio tarjoajan julkisella avaimella salattuna

Viidennessä kohdassa asiakas ja palvelin purkavat viestin salauksen yksityisillä avaimillaan ja tarkistavat, täyttääkö sopimusehdotus näiden haluamat ehdot. Osapuolet hyväksyvät sopimuksen allekirjoittamalla sen yksityisillä avaimillaan ($Allekirjoitus_{AsiakasSopimus} = (E_{AsiakkaanYksityinenAvain}(H(Sopimus))$, ($Allekirjoitus_{TarjojanSopimus} = (E_{TarjoajanYksityinenAvain}(H(Sopimus))$, ja toimittavat tämän jälkeen allekirjoitetut versiot notaarille. Notaarille lähtevät sanomat on kryptattu notaarin julkisella avaimella.

Vaiheessa kuusi notaari tarkistaa molempien osapuolten allekirjoitukset ja luo sopimuksesta version, joka sisältää asiakkaan ja palveluntarjoajan allekirjoituksen ja lähettää sen osapuolille ($Allekirjoitus_{Sopimus} = Sopimus, Allekirjoitus_{AsiakasSopimus}, Allekirjoitus_{TarjoajanSopimus}$) . Se myös lisää oman allekirjoituksensa uuteen versioon. Lähetettävät viestit on jälleen kryptattu osapuolten julkisilla avaimilla.

Seitsemännessä kohdassa saatuaan molempien allekirjoituksen sisältävän version sopimuksesta osapuolet tarkistavat toistensa allekirjoitukset ja ilmoittavat hyväksynnästä tai kieltäytymisestä notaarille
($Allekirjoitus_{AsiakasSopimus} = (E_{AsiakkaanYksityinenAvain}(H(Sopimus_{Kuittaus}))$,
($Allekirjoitus_{TarjoajanSopimus} = (E_{TarjoajanYksityinenAvain}(H(Sopimus_{Kuittaus}))$. Lähtevä viesti on kryptattu notaarin julkisella avaimella.

Jos molemmat osapuolet hyväksyivät allekirjoitukset. Ne lähettävät tästä notaarin julkisella avaimella kryptatun viestin. Tämän jälkeen notaari lisää sopimukseen ainutkertaisen tunnisteen, allekirjoittaa tunnisteen sisältävän sopimuksen ($Allekirjoitus_{NotaariSopimus} = E_{NotaarinYksityinenAvain}(Allekirjoitus_{SopimusOK})$) ja toimittaa sen luotettavaan tietovarastoon. Sanoma on kryptattu tietovaraston julkisella avaimella. Toimenpide näkyy kaaviossa kohdassa kahdeksan.

Kohdassa yhdeksän tietovarasto tarkistaa vielä sopimuksen allekirjoitukset. Jos kaikki on kunnossa, tietovarasto lisää oman allekirjoituksensa ja ilmoittaa hyväksynnästä notaarille ($Allekirjoitus_{SopimusOK_2} = E_{ArkistonYksityinenAvain}(Allekirjoitus_{SopimusOK_2})$). Viesti on jälleen kryptattu notaarin julkisella avaimella. Toimenpide näkyy kaaviossa kohdassa kahdeksan. Lisäksi notaari ilmoittaa asiakkaalle ja tarjoajalle hyväksynnästä.

Lopuksi palveluntarjoaja toimittaa asiakkaalle tunnisteen, jolla asiakas pystyy käyttämään haluamaansa palvelua. Tunniste on allekirjoitettu palveluntarjoajan yksityisellä avaimella ja se sisältää käytettävän palvelun tunnisteen ja voimassaoloajan ($Tunniste = E_{TarjoajanYksityinenAvain}(asiakastunnus, palvelutunnus, aikaleima)$).

### 4.1.2 Analyysi

Esitelty protokolla soveltuu parhaiten verkossa tapahtuviin kertaluonteisiin maksutapahtumiin. Suuresta viestinnän määrästä eri osapuolten välillä johtuen protokolla ei sovi kovinkaan hyvin tilanteisiin, joissa tarvittaisiin mikromaksamista. Protokollan luotettavuus riippuu myös paljon allekirjoituksessa ja salauksessa käytettävästä kryptografia-algoritmista. Osapuolet joutuvat viestinnän aikana tekemään useita allekirjoituksia johtuen edestakaisesta viestinnästä, että soveltuvuus mobiililaitteisiin on huono, jos halutaan käyttää pitkiä avaimia.

Taulukon 2 perusteella protokolla saavuttaa vahvan tason sitomisen osalta. Luotettu tahto, eli tässä tapauksessa luotettava arkisto, säilöö kaikki sopimukseen liittyvät todisteet. Osapuolet puolestaan sidotaan tapahtumaan luotettavan osapuolen varmentamilla allekirjoituksilla.

Peukaloimattomuuden osalta saavutetaan myös vahva taso. Koska allekirjoituksiin käytetään luotetun tahon varmentamia julkisia avaimia, on allekirjoitusten väärentäminen käytännössä mahdotonta. Se vaatisi luotettavan tahon epärehellisyyttä, mutta tässä tapauksessa sen oletetaan olevan täysin luotettava. Myös todistearkistoa pidetään täysin luotettavana tässä tarkastelussa.

Muunneltavuuden suojaus on vahvalla tasolla. Koska jokainen osapuolten välillä lähetettävä viesti on allekirjoitettu julkisella avaimella, ei viestin muuntelu osapuolten huomaamatta ole mahdollista. Varmennettavuuden vahva taso saavutetaan sillä, että kaikki allekirjoitusten varmennukset tehdään luotettavan osapuolen kautta.

Esitelty protokolla on kokonaisuutena erittäin luotettava. Se vaatii kuitenkin paljon signalointia osapuolten välillä ja toisaalta vaatii erillisen notaarin ja todistearkiston apua toimintaansa. Lisäksi sekä asiakkaan, palveluntarjoajan, notaarin että todistearkiston tulee saada sertifikaattinsa samalta luotetulta taholta. Jos osapuolet omistavat toistensa sertifikaatit jo entuudestaan, yhteyttä luotettuun tahoon ei välttämättä tarvita.

## 4.2 Yksityisyyden suojaava protokolla

Yksi kiistämättömyyteen liittyvä tekijä on yksityisyydensuoja. Koska kiistämättömyydessä pyritään sitomaan osapuolen identiteetti viestintään vahvasti, muodostuu ongelmaksi tilanne, jossa osapuoli haluaa pysyä anonyymina vastakkaiselle osapuolelle. Tällainen tilanne luo kuitenkin huijarille mahdollisuuden tehdä rikoksia, joita on mahdoton jäljittää. Tarvitaan siis keino, jolla käytettyjen maksuyksikköjen anonymiteetti on mahdollista poistaa luotetun tahon avulla, jos kanssakäymiseen epäillään liittyvän rikollista toimintaa. Esiteltävä protokolla pyrkii esittämään ratkaisun näihin ongelmiin.[7]

### 4.2.1 Lähtökohta

Tyypillinen sähköinen maksutapahtuma voisi mennä seuraavasti. Tapahtumaan kuuluvat osapuolina asiakas, sokea notaari, pankki, tuomari ja kauppa. Aluksi asiakas saa pankilta kolikon, jota käytetään maksuvälineenä tapahtumassa. Kolikko sisältään pankin tekemän sokean allekirjoituksen. Sokeassa allekirjoituksessa allekirjoitettavan viestin sisältö naamioidaan ennen allekirjoitusta. Tarkoituksena on estää allekirjoittajaa näkemästä viestin sisältöä selville. Allekirjoituksen toimeksiantaja pystyy puolestaan muuntamaan allekirjoituksen vastaamaan alkuperäistä viestiä. Pankilla on tiedossa yhteys käyttäjän todellisen, ja viestinnässä käytettävän näennäisidentiteetin välillä. Notaari osallistui sokeaan allekirjoitukseen ja näin ollen myös se tietää myönnetyn kolikon ja käyttäjän näennäisidentiteetin välisen yhteyden.

Ostotapahtuman yhteydessä asiakas osoittaa kaupalle, että sillä on tietoa kolikkoon liittyvästä salaisesta avaimesta $x$. Jos kolikkoa väärinkäytetään, esimerkiksi suoritetaan sillä maksu kahteen kertaan, pankki ja notaari yhdessä muodostavat siteen käyttäjän todellisen identiteetin ja kolikon välille. Näiden tietojen perusteella tuomari langettaa tuomion.

Oletetaan, että käytössä on eksponenttipohjainen allekirjoitusalgoritmi, kuten RSA. Asiakkaalla on kaksi avainta ($S_U$ ja $V_U$), samoin pankilla ($S_B, V_B$). $S_U$ ja $S_B$ ovat yksityisiä ja $V_U$ , sekä $V_B$ julkisia avaimia. Pankilla on tiedossa asiakkaan julkinen avain $V_u$ ja asiakkaalla on puolestaan tiedossa pankin julkinen avain $V_B$. Lisäksi notaarilla on käytössään eksponenttipohjainen julkisen avaimen salausjärjestelmä, jonka tunnuksena on $(E_o, D_o)$. Käyttäjä, pankki ja tuomari tietävät $E_o$:n.

Käytettävä kolikko sisältää kolme kenttää. Ensimmäisessä on eksponenttiavain $y$. Tätä vastaa yksityinen avain $x$. Jokaista kolikkoa varten on omat avaimet. Toisessa kentässä on jotain kolikkoon liittyvää tietoa, kuten arvo ja voimassaoloaika. Kolmannessa kentässä on pankin digitaaliset allekirjoitukset $y$:lle ja informaatiokentälle.

Informaatiokentän allekirjoitukseen on kaksi tapaa. Ensimmäisessä informaatiokenttä yhdistetään $y$:n kanssa notaarin avulla, ennen sokean eksponenttiavaimen $y^{-}: n$ luomista. Toinen vaihtoehto on käyttää kenttään perustuvaa avainta. Pankin käyttämällä allekirjoituksella tulee olla seuraavat ominaisuudet:

- $S_B(m_1) * S_B(m_2) = S_B(m_1 * m_2)$, tämä saavutetaan RSA:n käytöllä. Tästä johtuen RSA:n kanssa viesteihin $m_1, m_2$ tulee käyttää jotain yhdensuuntaista tiivistefunktiota. Tässä toteutuksessa on käytetty jälkimmäistä vaihtoehtoa.
- Kun käytössä on sokeutusfunktio $F_B$, vaaditaan että $S_B(F_B(m_1)m_2) = m_1 * S_B(m_2)$. Myös notaari tietää $F_B$:n.

Protokolla sisältää kolme vaihetta, jolla saavutetaan aiemmin kuvattu toiminnallisuus:

1. Käyttäjä ja pankki luovat jaetun salaisuuden $s$.
2. Pankki allekirjoittaa $s$:sta muodostetun tiivisteen, jota käytetään näennäisidentiteetin luomisessa lisäämällä siihen operaatiosta $E_o(s)$ saatu tulos. Tällä toimenpiteellä saavutetaan kiistämättömyys ja sidotaan asiakas viestintään.
3. Pankki säilyttää todisteet asiakkaan identiteetin ja salaisuuden $s$ välisestä yhteydestä.

### 4.2.2 Kolikon nostaminen

Kun asiakas haluaa kolikon käyttöönsä, pankki luo kolikon käyttämällä sokeaa allekirjoitusta. Näin menettelemällä pankki ei saa tietoonsa kolikon käyttäjän identiteettiä. Tällä varmistetaan se, että asiakas voi suorittaa maksutapahtumat anonyymisti, kuten käteisellä rahalla perinteisessä maksutapahtumassa on mahdollista.

1. Asiakas valitsee yksityisen avaimen satunnaisesti, laskee siitä $y$:n arvon ja lähettää $E_o(y)$ tuloksen notaarille.
2. Asiakas ja notaari luovat jaetun salaisuuden $w$ käyttäen Diffie-Hellman -avaimenvaihtoa [8].
3. Notaari laskee $y^- = F(w) * y$ ja ilmoittaa tuloksen asiakkaalle.
4. Asiakas todentaa $y^-$:n, laskemalla $y^- = F(w) * y$ ja vertaamalla sitä notaarilta saatuun arvoon. Tämän jälkeen asiakas lähettää sen edelleen pankille allekirjoitettuna asiakkaan yksityisellä avaimella $S_U$. Lähetettävä viesti sisältää $s$:n, $y^-$:n ja notaarin nimen, sekä lisätietoja, kuten aikaleiman. Näillä tiedoilla voidaan osoittaa viestin ainutkertaisuus.
5. Pankilla on asiakkaan allekirjoitustiedot, joten se veloittaa todellisen kolikon asiakkaan tililtä ja lähettää asiakkaalle viestin $T$, $T = E_o(S_B(y^-))$. Tämän jälkeen asiakas lähettää $T$:n notaarille.
6. Notaari käyttää $T$:a saadakseen selville $S_B(y^-)$, eli sokaisun sisällä olevan eksponenttiavaimen. Tämän jälkeen se purkaa sokaisun saadakseen $S_B(y)$ eli alkuperäisen eksponenttiavaimen ja edelleen rakentaa tällä tiedolla kolikon. Sitten se lähettää kolikon edelleen asiakkaalle. Tämän jälkeen notaari säilyttää asiakkaan identiteetin ja kolikon. Se sisältää tiedot julkisen avaimen salauksen arvot $T$:sta ja $E_B(y)$:sta $s$:n kanssa.

### 4.2.3 Kolikon käyttö

Kun asiakas haluaa suorittaa maksun kolikolla, suoritetaan kolme vaihetta:

1. Asiakas allekirjoittaa viestin, joka on vastaus kaupan esittämään haasteeseen, jolla asiakas todistaa tietävänsä $x$:n
2. Kauppa lunastaa todellisen kolikon pankilta takaisin myöhemmin.
3. Jos asiakas yrittää käyttää kolikkoa useampaan kertaan, pankki luo notaarin avulla ketjun, jolla voidaan selvittää kolikkoon liittyvän asiakkaan identiteetti.

### 4.2.4 Turvallisuusnäkökohtia

Protokollan toiminnasta on helppo havaita kolme ominaisuutta, joihin sen luotettavuus perustuu. Notaari ei voi käyttää kolikkoa, koska se ei tiedä $x$:aa. Notaari ja asiakas luovat yhdessä salaisuuden $w$. Tämä takaa sen, että kumpikaan ei yksin voi vaikuttaa $w$:n arvoon ja näin ollen yksi sokea allekirjoitus on sidottu yhteen kolikkoon. Toisaalta pankilla on asiakkaan allekirjoittama $y^-$, joten pankilla on todisteet asiakkaan identiteetin sitomisesta $y^-$:n. Tämä takaa sen, että asiakas ja pankki eivät voi viestiä siitä, kuka julkaisi $x$:n.

Asiakas ei myöskään pysty luomaan kolikkoa tyhjästä, koska sen olisi kyettävä laskemaan $S_B(y^-)$ joko $y^-$:n tai $E_o(S_B(y^-))$:n perusteella, jonka katsotaan olevan mahdotonta.

Toisaalta vieras taho ei voi käyttää x:aan sidottua kolikkoa. Koska x:n selvittäminen on mahdotonta y:n ja muun yhteisen tiedon perusteella ja vain x:n julkaisija tietää sen arvon, voi x:n sidottua kolikkoa käyttää ainoastaan sen alkuperäinen luoja.

Myöskään notaari ei pysty esittämään olevansa pankin tai kaupan asiakas. Jotta notaari voisi esiintyä asiakkaana pankille, sen tulisi saada selville asiakkaan $y^-$:n kuuluva allekirjoitus, jonka katsotaan olevan mahdotonta. Jotta notaari voisi esiintyä asiakkaana kaupalle ja käyttää tämän kolikon, sen tarvitsisi saada selville kolikon tiedot ja x.

Jos pankki haluaisi esiintyä asiakkaana ja käyttää tämän kolikoita, sen tulisi kyetä laskemaan $y^-$:n digitaalinen allekirjoitus, mikä ei ole mahdollista edes notaarin avulla.

### 4.2.5 Analyysi

Protokolla sisältää kohtuullisen määrän kryptausta ja allekirjoituksia asiakkaan osalta, joten käytännössä asiakkaana voi toimia myös mobiililaite. Tyypillisimmät käyttötilanteet voidaan katsoa olevan kolikon hankkiminen ja käyttäminen, joista molemmat sisältävät asiakkaan osalta vai yhden raskaan allekirjoitusoperaation. Suurin kuorma kohdistuu pankkiin, joka joutuu tekemään kaksi allekirjoitusta jokaista kolikkoa kohti.

Tutkittaessa protokollan ominaisuuksia taulukon 2 perusteella voidaan sitomisen katsoa olevan keskitasoa. Osapuolten identiteetit ovat tässä tapauksessa luotettavaksi ta-

hoksi katsotun pankin tiedossa, mutta niitä ei ole mitenkään fyysisellä tasolla sidottu identiteettiin.

Peukaloimattomuus on vahvalla tasolla, koska käytettyjä allekirjoituksia ei voi väärentää huomaamatta.

Myös muunneltavuus on vahvalla tasolla, koska kaikki viestintä on kryptattua, ei sisällön vaihtaminen ole mahdollista.

Varmennus on keskitasolla, allekirjoitusten tarkistukseen on erityinen menettely, joka perustuu sokeaan eksponenttiavaimeen $y^{-}$. Allekirjoitusten varmennukseen ei kuitenkaan käytetä mitään luotettua tahoa.

## 4.3 Mikromaksamisprotokolla

Kaksi aiempaa protokollaa keskittyi erityisesti siihen, kuinka osapuolet sidotaan kiistämättömästi sopimukseen tai käytettyyn kolikkoon. Seuraavaksi tarkastellaan vielä mikromaksamiseen soveltuvaa protokollaa, jolla voidaan hoitaa luvussa 2.1 esitelty aikaperustaiseen laskutukseen liittyvä ongelma.

Ad Hoc -tyyppisten verkkojen tyypillinen ongelma on, että siellä muodostetut yhteydet eivät ole pitkäikäisiä ja näin ollen ei ole mahdollista muodostaa langallisessa verkossa esiintyviä luottamussuhteita. Lisäksi yhteyttä luotettuun tahoon ei aina ole saatavilla, jonka avulla identiteetit tai maksuyksiköt voitaisiin varmentaa. Ratkaisuksi onkin ehdotettu tiivisteketjujen käyttöä maksuyksikkönä. Yhdellä maksuyksiköllä on korkea granulariteetti, eli yksittäisen yksikön väärinkäyttö tai menetys ei tuota suuria tappioita. [9]

### 4.3.1 Tiivisteketju

Tiivisteketju saadaan muodostettua, kun johonkin siemenarvoon kohdistetaan tiivistefunktio $H$, ja saatuun funktioon kohdistetaan tämä uudelleen ja uudelleen. Tyypillisesti tiivisteiden luontiin käytetään joko MD5 tai SHA1 funktioita. Nämä ovat laskennallisesti huomattavasti kevyempiä kuin esimerkiksi asymmetrisen avaimen algoritmi RSA. Näin ollen ketjujen luonti ja arvojen tarkistus on nopeaa. Neljästä elementistä koostuva ketju voidaan luoda seuraavasti:

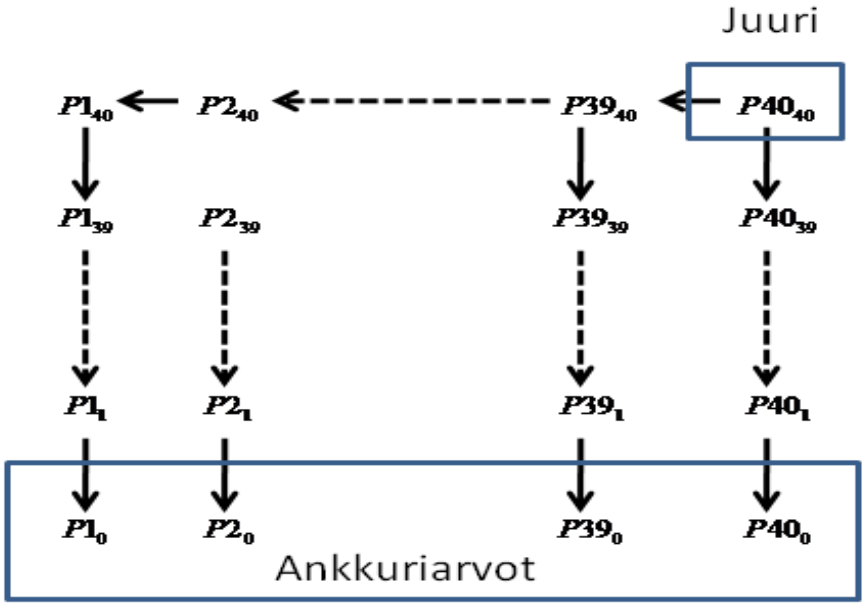
$$H\left(H\left(H\left(H(siemen)\right)\right)\right)$$

Nyt muodostettua ketjua voidaan käyttää maksuvälineenä. Asiakas aloittaa lähettämään ketjua viimeisestä, ns. ankkuriarvosta lähtien. Koska tiivistefunktio on yhdensuuntainen, ei yksittäisellä arvolla ole mahdollista muodostaa ketjun arvoja taaksepäin. Tarjoajan on saadulla arvolla aina mahdollista varmistaa, että edellinen saatu arvo kuuluu kyseiseen ketjuun. Näin ollen voidaan varmistua siitä, ettei asiakas yritä huijata tekaistuilla ketjun arvoilla.

Yhden maksuyksikön rahallinen arvo pyritään myös pitämään suhteellisen pienenä, tyypillinen arvo voi olla enintään muutamia senttejä. Näin ollen minimoidaan osapuol-

ten tappiot mahdollisissa ongelmatilanteissa. Maksaja sitoutuu jokaiseen tiivistearvoon allekirjoittamalla tiivisteketjun ankkurin ja pituuden yksityisellä avaimellaan.

Esiteltävä protokolla hyödyntää tiivisteketjun erikoistapausta, tasapainottamatonta binääripuuta. Siinä luodaan ensin yksittäinen tiivisteketju ja jokainen tämän ketjun arvo toimi siemenarvona uudelle ketjulle. Näin ollen saadaan luotua suuri ketju, jonka jokainen arvo on sidottu toisiinsa. Kuvassa 6 on kuvattu tiivisteketjuista muodostettu puu.




**Kuva 6. Tiivisteketjupuu. Lähdettä [9] mukaillen.**

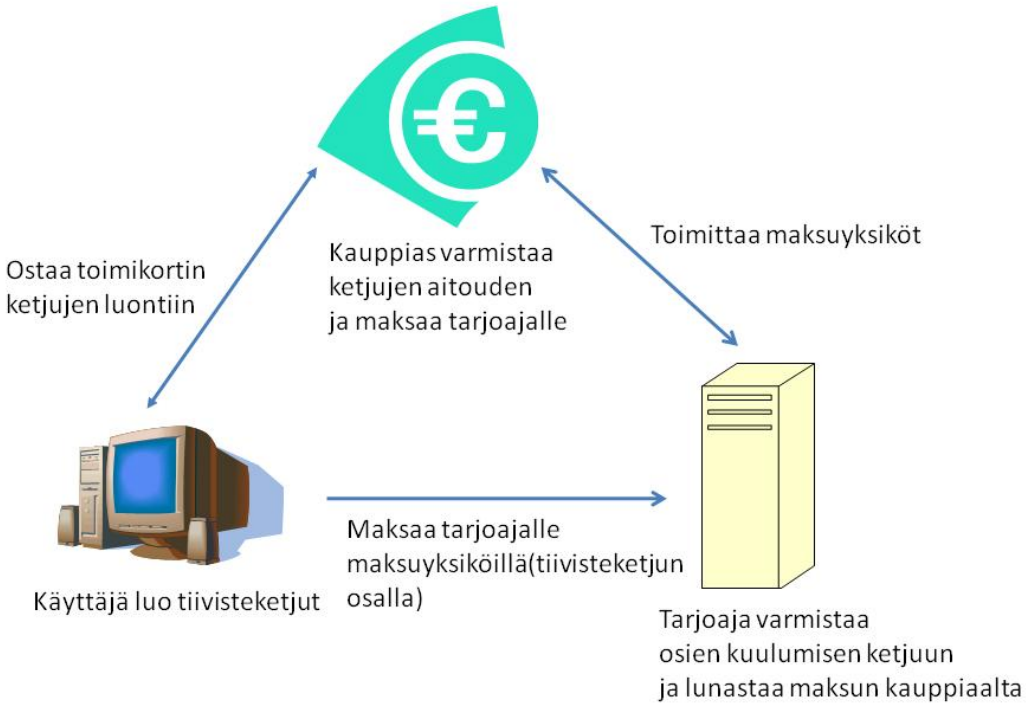
### 4.3.2 Toiminta

Tarkastelussa kiinnitetään huomiota lähinnä mikromaksamistoiminnallisuuteen, eikä niinkään Ad Hoc -ominaisuuksien toteuttamiseen. Aluksi käyttäjän ja tarjoajan välille luodaan suhde, jossa asiakkaalle toimitetaan palveluntarjoajan sertifikaatti, joka sisältää tarjoajan julkisen avaimen. Tarjoaja toimittaa asiakkaalle myös avaimet toimikortilla, joiden avulla asiakas pystyy luomaan tiivistepuun ja allekirjoittamaan yksittäisen ketjun ankkurin. Näin ollen asiakkaan identiteetti saadaan sidottua maksuliikenteeseen.

Jotta myös tarjoaja saadaan sidottua liikenteeseen, asiakas lähettää jokaisen muodostetun ketjun ankkuriarvojen tarjoajalle kryptattuna sen julkisella avaimella. Tarjoaja luo jokaista ankkuriarvoa kohden varmennusarvon, joka sisältää

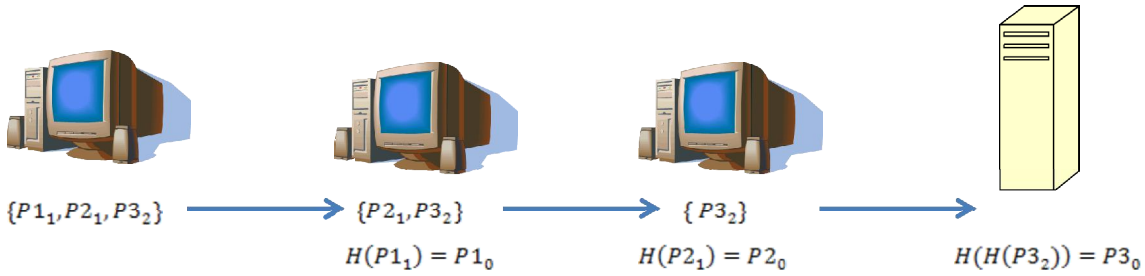
- ankkuriarvon
- ketjun pituuden
- asiakkaan identiteetin
- voimassaoloajan
- tarjoajan allekirjoituksen.

Tarjoaja luo kaikista varmennusarvoista ns. sitoumuksen, jonka se toimittaa kryptattuna asiakkaalle. Asiakas ei pysty tarkastelemaan näitä arvoja, ainoastaan lähettämään tällaisen maksun yhteydessä. Kuvassa 7 on kuvattu mikromaksuhierarkia, jossa mukana ovat asiakas, tarjoaja ja kauppias.




**Kuva 7. Mikromaksuhierarkia.**

Kun yhteys luodaan asiakkaan ja päätepisteen välillä, asiakas toimittaa yhden ketjun varmennusarvon jokaiselle asiakkaan ja tarjoajan välissä olevalle solmulle. Varmennusarvot on kryptattu jokaisen solmun julkisella avaimella, jotka on saatu solmuilta aiemmin. Näin ollen solmut kykenevät varmistamaan jokaisen niiden kautta kulkevan maksuyksikön. Samalla jokainen viestiä välittävä solmu veloittaa asiakkaalta yhden maksuyksikön. Kun asiakas haluaa liikennöidä tarjoajalle, se maksaa ensimmäisestä ketjusta ensimmäiselle solmulle viestien välittämisestä. Toisesta ketjusta maksetaan toiselle solmulle ja niin edelleen. Jokainen solmu varmistaa maksuyksikön aiemmin vastaanottamallaan varmennusarvolla ja kohdistaa viimeisen ketjun arvoon tiivistefunktion. Koska ketjut ja niiden arvojen varmentaminen on sidottu toimikorttiin, ei ulkopuolinen osapuoli voi hyödyntää arvoja murtamatta toimikorttia. Näin ollen jokainen solmu voi todentaa ketjun jatkumisen vertaamalla arvoa edelliseen vastaanotettuun arvoon. Lopuksi vastaanottajalle lähetetään solmujen verran ketjua eteenpäin, jolloin maksetaan koko matkasta. Kuvassa 5 on kuvattu maksutapahtuman kulku.




**Kuva 8. Kuljetuksen maksaminen tiivisteketjuilla.**

### 4.3.3 Analyysi

Protokolla soveltuu erittäin hyvin käytettäväksi mobiililaitteiden kanssa. Sen avulla on mahdollista toteuttaa joustava aikaperusteinen laskutus, esimerkiksi puhelu- tai videoneuvottelukäytössä.

Ketjun luominen ja arvojen varmistaminen on erittäin kevyt ja nopea operaatio verrattuna julkisen avaimen algoritmeihin, kuten DSA ja RSA. Tästä johtuen protokollan turvallisuusominaisuudet eivät kuitenkaan ole niin hyvät kuin kahden kohdissa 4.1 ja 4.2 esitellyn protokollan. Tämä ei kuitenkaan haittaa, koska vaikka viestinnässä menetettäisiin yksittäisiä maksuyksiköitä, niiden arvo on kuitenkin pieni.

Tarkasteltaessa protokollaa taulukon 2 pohjalta, sitominen on heikkoa tai keskitasoa. Protokolla mahdollistaa luotetun osapuolen käytön, muttei määrittele sen käyttöä tarkemmin.

Peukaloimattomuus on vahvaa tasoa. Vaikka välittävät solmut näkevät ketjujen arvot, ne eivät voi käyttää niitä, koska se vaatisi tarjoajan allekirjoittaman varmennusarvon. Koska viestit sisältävät ainoastaan ketjun arvon, muunneltavuus kuuluu tähän samaan kategoriaan.

Varmennettavuus on heikkoa tasoa, koska solmut vertaavat vastaanotettuja paketteja suoraan saatuun varmennusarvoon.

# 5 YHTEENVETO

Lähdeaineistoja tarkastellessa kävi ilmi, että kiistämättömyys on suosittu tutkimuskohde. Suurin osa ratkaisuista oli kuitenkin hyvin lähellä toisiaan ja ne keskittyivät lähinnä parantamaan toistensa huonoja puolia. Tässä työssä käsitellyt protokollat edustavat näitä havaittuja pääsuuntauksia. Protokollien toiminta on esitelty vain päällisin puolin, koska syvällisempi tarkastelu ei olisi mahtunut tämän opinnäytetyön suosituspituuteen. Lisäksi tarkoituksena oli luoda yleiskatsaus tällä hetkellä olemassa oleviin toteutuksiin.

Jokainen käsitellyistä protokollista pyrkii ratkaisemaan yhden kiistämättömyyteen liittyvän osaongelman. Kohdassa 4.1 esitelty protokolla keskittyy parhaisiin mahdollisiin kiistämättömyysominaisuuksiin. Protokolla ei puolestaan ota juurikaan kantaa käyttäjän yksityisyyteen. Lisäksi se käyttää raskaita allekirjoitusalgoritmeja, joilla saavutetaan vahvat kiistämättömyysominaisuudet suoritustehon kustannuksella. Se on myös liian raskas käytettäväksi mobiililaitteissa. Protokolla soveltuu parhaiten esimerkiksi yksittäisen kahden osapuolen välisen tehtävän sopimuksen tekoon.

Toinen protokolla, joka käsiteltiin kohdassa 4.2, pyrki puolestaan takaamaan mahdollisimman hyvän yksityisyydensuojan asiakkaalle. Se onnistuu siinä hyvin mutta se sisältää kuitenkin paljon raskaita allekirjoituksia ja signalointia osapuolten välillä. Näin ollen sopivuus mobiililaitteisiin on jälleen huono. Protokolla tarjoaa erittäin toimivan ratkaisun anonyymina tehtäville ostotapahtumille. Väärinkäyttötapauksessa asiakkaan identiteetti on selvitettävissä. Näin ollen protokolla omaa hyvän potentiaalin käytettäväksi sähköisessä kaupassa.

Viimeinen esitelty protokolla keskittyy nimenomaan mikromaksamiseen. Tiivisteketjut tarjoavat hyvän toimintatavan aikaperusteiseen maksamiseen. Protokolla ei sellaisenaan sovellu esimerkiksi WLAN:in kanssa käytettäväksi, mutta pienillä muokkauksilla siitä on mahdollista saada hyvin toimiva. Lisäksi suunnittelussa on keskitytty huomioimaan erityisesti mobiililaitteet. Taulukossa 3 on vertailtu tarkasteltujen protokollien kiistämättömyysominaisuuksia.

**Taulukko 3. Vertailtujen protokollien kiistämättömyysominaisuudet.**

| **Ominaisuus** | **Protokolla 4.1** | **Protokolla 4.2** | **Protokolla 4.3** |
|---|---|---|---|
| Sitominen | Vahva | Keskitaso | Heikko/Keskitaso |
| Peukaloimattomuus (Allekirjoittajan kone on koskematon) | Vahva | Vahva | Vahva |
| Muunneltavuus | Vahva | Vahva | Vahva |
| Varmennettavuus | Vahva | Keskitaso | Heikko |

Näin ollen yksikään tutkituista protokollista ei sovellu sellaisenaan ratkaisemaan sähköiseen kaupankäyntiin liittyviä ongelmia. Myös aiemmin tiedossa ollut tasapainottelu käytettävien kryptoalgoritmien ja protokollan turvallisuuden välillä tuli hyvin esiin. Jatkokehittämällä esiteltyjä protokollia ja yhdistelemällä niiden hyviä puolia on kuitenkin mahdollisuus rakentaa melko yleiskäyttöinen protokolla sähköiseen kauppaan.

Kaikki protokollat esittävät toteutukset hyvin konseptuaalisella tasolla, eikä yksikään ota kantaa todelliseen implementointiin. Näin ollen protokollien osalta ei ole määritelty sitä, millä kerroksella TCP(Transmission Control Protocol)/IP(Internet Protocol)-mallia niiden on ajateltu toimivan. Myöskään vuorovaikutuksesta olemassa olevien linkki-, verkko- ja kuljetuskerroksen protokollien kanssa, ei ole mainintoja.

# LÄHTEET

[1] P. Louridas, “Some guidelines for non-repudiation protocols”, ACM SIGCOMM Computer Communication Review, v.30 n.5, October 2000.
[2] S. Herda, "Non-repudiation: Constituting evidence and proof in digital cooperation," Computer Standard & Interfaces, vol. 17, pp. 69-79, 1995.
[3] L 7.8.2009/617 Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista.
[4] M. Blum, “How to Exchange (Secret) Keys”, ACM Transactions on Computer Systems, Vol 1, No. 2, May 1983.
[5] J. Adikari, "Efficient PKI based non-repudiation," M.S. Thesis, Royal Institute of Technology (KTH), Stockholm, Sweden, July, 2005.
[6] J. Adikari, "Efficient Non-Repudiation for Techno-Information Environment", First International Conference on Industrial and Information Systems, ICIIS 2006, 8 - 11 August 2006, Sri Lanka.
[7] J. Aboud Sattar ja A. Mohammed, "Anonymous and Non-Repudiation E-Payment Protocol", American Journal of Applied Sciences 4 (8) , pp. 538-542, 2007.
[8] E. Rescorla, “Diffie-Hellman Key Agreement Method”, IETF RFC 2631, June 1999
[9] H. Tewari ja D. O’Mahon, “Multiparty micropayments for Ad Hoc Networks”, Proceedings of the IEEE Wireless Communications and Networking Conference. Mar 2003.