LAPPEENRANNAN TEKNILLINEN YLIOPISTO

TIETOTEKNIIKAN OSASTO

Henkilökohtaisen päätelaitteen käyttö lähimaksujärjestelmässä

Diplomityön aihe on hyväksytty tietotekniikan osaston osastoneuvostossa 15.10.2003.
Diplomityön tarkastajina toimivat professori Jari Porras ja assistentti Pekka Jäppinen.
Diplomityön ohjaajana toimi assistentti Pekka Jäppinen.

Lappeenrannassa 1.3.2004

Tuomo Repo
Kaivosuonkatu 1 B 13
53850 LAPPEENRANTA
+358 50 4684436

TIIVISTELMÄ

Tekijä: Repo, Tuomo

Nimi: Henkilökohtaisen päätelaitteen käyttö lähimaksujärjestelmässä

Osasto: Tietotekniikan osasto

Vuosi: 2004

Paikka: Lappeenranta

Diplomityö. Lappeenrannan teknillinen yliopisto. 69 sivua ja 21 kuvaa.

Tarkastajat: Professori Jari Porras, assistentti Pekka Jäppinen

Hakusanat: langaton maksujärjestelmä, PTD, PKI, Bluetooth

Henkilökohtaista luotettavaa päätelaitetta voidaan käyttää maksuvälineenä langattomissa maksujärjestelmissä. Päätelaitteen luotettavuus saadaan aikaan sen sisältämien tietojen salauksen ja käyttäjän tunnistuksen avulla. Kaupankäynnin tietoturvan kannalta järjestelmien tärkeimpiä tehtäviä ovat osapuolten tunnistaminen ja tietoyhteyden suojaaminen.

Tässä työssä esitellään automaatti- ja ruokalamaksamisen järjestelmä, jossa käytetään maksuvälineenä Bluetooth-ominaisuudella varustettua kämmentietokonetta. Henkilökohtaisen luotettavan päätelaitteen vaatimuksia ja uhkia käydään läpi. Samoin erilaisia menetelmiä käyttäjän ja laitteiden tunnistukseen sekä tietoyhteyden suojaamiseen. Käyttäjän tunnistus perustuu julkisten avainten varmenteisiin, joihin on sisällytetty tietoa niin asiakkaasta, maksuvälineestä kuin maksumenetelmästäkin. Maksumenetelmäksi on valittu tilien käyttö. Tietoyhteyden suojaamiseen käytetään epäsymmetristä salausta.

ABSTRACT

Author: Repo, Tuomo

Subject: Using personal terminal device in local environment payment system

Department: Department of Information Technology

Year: 2004

Place: Lappeenranta

Master's thesis. Lappeenranta University of Technology. 69 pages and 21 figures.

Supervisors: Professor Jari Porras, assistant Pekka Jäppinen

Keywords: Mobile payment system, PTD, PKI, Bluetooth

Personal trusted device (PTD) can be used as a payment equipment in mobile payment systems. The PTD can be made trustworthy by encrypting the data of it and applying user authentication. Trading security point of view the most important tasks in payment systems are authentication of parties and securing the connections between them.

In this thesis local environment payment system applied for vending machines and cafeterias will be introduced. Bluetooth enabled PDA is applied as a payment equipment. The requirements and threats for PTD will be introduced as well as different methods for user authentication, device authentication and securing connections. Authentication is based on certificates, which include information about user, payment device and payment method. Prepaid accounts are chosen for payment method. Asymmetric encryption is used for securing connections.

ALKUSANAT

Tätä diplomityötä on kirjoitettu syyskuun 2003 alusta helmikuun 2004 loppuun Lappeenrannan teknillisen yliopiston tietoliikennetekniikan laitoksen *Lyhyen kantaman radiotekniikat* -projektin merkeissä. Kiitän professori Jari Porrasta siitä, että olen saanut työstää lopputyötäni mielenkiintoisen tutkimuksen ympäröimänä akateemisessa ympäristössä. Kiitokset ohjaajilleni TkT Jari Porrakselle ja DI Pekka Jäppiselle rakentavista kommenteista ja ongelmakohtien ymmärtämyksestä työn edetessä. Kiitokset myös LKRT-projektin mainiolle työporukalle.

Neljän ja puolen vuoden tiivistä opiskelutahtia olen kestänyt kavereitteni tukemana. Erityiskiitokset pitkäaikaiselle kämppikselleni Harrille sekä muille harrasteiden kautta tutuiksi tulleille kavereille, joiden kanssa olen päässyt irrottautumaan arjesta. Kiitokset myös itselleni siitä etten vaihtanut TUTA:lle vaikeista hetkistä huolimatta.

Lopuksi vielä kiitokset vanhemmilleni ja koko suvulle, joka on jaksanut tiedustella valmistumisajankohtaani useampaan otteeseen. Se on siis nyt!

Lappeenrannassa 1.3.2004

Sisällysluettelo

Kuvaluettelo

Taulukkoluettelo

Lyhenneluettelo

ACL	Asynchronous ConnectionLess
API	Application Programming Interface
ASN.1	Abstract Syntax Notation #1
BD_ADDR	Bluetooth Device Address
CA	Certificate Authority
CN	Common Name
CRL	Certificate Revocation List
EEPROM	Electrically Erasable Programmable Read Only Memory
FTP	File Transfer Protocol
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HCI	Host Control Interface
HST	Henkilön Sähköinen Tunnistaminen
HTTP	HyperText Transfer Protocol
ICC	Integrated Circuit Card
IEEE	Institute of Electrical and Electronic Engineers
I/O	Input/Output
ISM	Industrial Scientific Medical
ITU-T	International Telecommunications Union, Technical Standards Section
L2CAP	Logical Link Control and Adaption Protocol
LDAP	Lightweight Directory Access Protocol
LMP	Link Manager Protocol
MAC	Message Authentication Code
MeT	Mobile Electronic Transactions
MIT	Massachusetts Institute of Technology
OBEX	Object Exchange
OTA	Over The Air
OU	Organization Unit
PAIN	Privacy, Authentication, Integrity, Non-repudiation
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Digital Assistant

PIN	Personal Identity Number
PKI	Public Key Infrastructure
PPP	Point-to-Point Protocol
PTD	Personal Trusted Device
RA	Registration Authority
RAM	Read Access Memory
RCA	Root Certificate Authority
RFID	Radio Frequency Identification
ROM	Read Only Memory
SCO	Synchronous Connection Oriented
SD	Secure Digital
SDP	Service Discovery Protocol
SE	Security Element
SET	Secure Electronic Transactions
SIG	Special Interest Group
SIM	Subscriber Identity Module
SMS	Short Message Service
SSL	Secure Socket Layer
SWIM	Subscriber Wireless Identity Module
TCP/IP	Transmission Control Protocol / Internet Protocol
TCS	Telecom Control Systems
TLS	Transport Layer Security
TTP	Trusted Third Party
UDP	User Datagram Protocol
URL	Universal Resource Locator
USB	Universal Serial Bus
WAE	Wireless Application Environment
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
WLAN	Wireless Local Area Network
WPKI	Wireless Public Key Infrastructure
WTLS	Wireless Transport Layer Security

1 Johdanto

Sähköinen maksaminen on ollut arkipäivää jo vuosikymmenen ajan. Pankkien verkkopalvelut ja yritysten verkkokaupat ovat saavuttaneet tukevan jalansijan kaupankäynnissä. Internetin käytön kasvu on mahdollistanut uusia liiketoimintamalleja (http://www.amazon.com/) ja samalla ohjannut ostokulttuuria. Viime vuosina on pyritty löytämään sähköisiä vastineita myös käteisostoille.

Yhä useammat ihmiset kantavat mukanaan matkapuhelimia tai muita langattomia päätelaitteita, jotka voisivat toimia viestimisen ja kalenteritoimintojen lisäksi myös maksuvälineinä. Jotta langaton maksaminen olisi mielekästä, pitää maksutapahtuman olla riittävän nopea ja yksinkertainen, mutta siitä huolimatta luotettava ja turvallinen. Vaadittava tietoturvan taso voidaan määritellä käytettävän maksuympäristön ja maksumenetelmän sekä ostosten suuruuden perusteella.

Tässä työssä selvitetään jokapäiväisen työpaikkaruokailun ja automaattimaksamisen edellytyksiä sekä niiden suorittamista langattoman päätelaitteen avulla. Ongelman ratkaisemiseksi tarkastellaan eri maksumenetelmiä ja maksuvälineiksi soveltuvien päätelaitteiden ominaisuuksia. Koska kaupankäynnin osapuolten tunnistaminen ja osapuolten välisen tietoyhteyden suojaaminen ovat maksamisessa tärkeimpiä tehtäviä, työssä tutkitaan erilaisia mahdollisuuksia niiden toteuttamiseksi.

Lopuksi esitellään ratkaisu lähimaksujärjestelmän rakentamiseksi, jossa maksuvälineenä käytetään henkilökohtaista luotettavaa päätelaitetta (PTD, Personal Trusted Device). Ratkaisussa hyödynnetään etukäteen maksettuja tilejä, joiden käyttöoikeuksia hallitaan asiakkaille myönnettyjen varmenteiden avulla. Julkisen avaimen infrastruktuuria (PKI, Public Key Infrastructure) käytetään myös osapuolten tunnistamiseen ja tietoyhteyksien suojaamiseen.

2 Maksujärjestelmät

Sähköisten maksujärjestelmien toimintaa säädetään lailla. Kuluttajansuojalain mukaan asiakkaalla on 14 päivän palautusoikeus kaikille etämyynnin kautta ostetuille tuotteille. Etämyynnillä tarkoitetaan myyjän harjoittamaa toimintaa, jossa ”sopimuksen tekemiseen ja sitä edeltävään markkinointiin käytetään yksinomaan yhtä tai useampaa viestintä”. [SUO78, luku 6 § 4] Käyttäjän yksityisyyden suojaa säädellään EU-maissa direktiivillä [EUR02], jonka mukaan käyttäjän yksityisyyttä julkisissa verkoissa pitää suojella ja mahdollisista julkaistavista tiedoista tiedottaa etukäteen. Tietoverkkojen tietoturvaa pitää myös jatkuvasti mitata ja mahdollisista riskeistä tiedottaa käyttäjiä.

Mobiilit, langattomat maksujärjestelmät eroavat perinteisistä sähköisistä maksujärjestelmistä siten, että maksuvälineenä käytetään langatonta päätelaitetta. Siten palvelut ovat helpommin ja useammassa ympäristössä saatavilla. Valitettavasti myös hyökkäykset maksuvälineeseen ovat mahdollisia useammassa ympäristössä, ja ne tapahtuvat usein huomaamattomasti [SCH02].

Langattoman maksamisen soveltaminen työpaikkaruokailun ja automaattimaksamisen kaltaisiin käyttökohteisiin asettaa käytettävälle järjestelmälle useita vaatimuksia. Maksaminen halutaan suorittaa nopeasti sellaisen maksuvälineen avulla, jota kannetaan joka tapauksessa mukana. Toisaalta maksutapahtuman tulisi olla turvallinen ja luotettava. Maksuvälineen käytön pitäisi olla ilmaista sekä asiakkaalle että kauppiaalle, koska maksettavat ostokset ovat pieniä. Kauppias puolestaan haluaa, että maksun suorittaminen voidaan todeta ostoksen tapahtumahetkellä. Asiakas voi haluta todistuksen maksusta eli sähköisen kuitin. Työpaikkaruokailun maksujärjestelmän suunnittelemiseksi pitää tietää, mitkä ovat ympäristön asettamat vaatimukset, mistä osa-alueista kaupankäynti koostuu ja mikä on käytettävä maksumenetelmä.

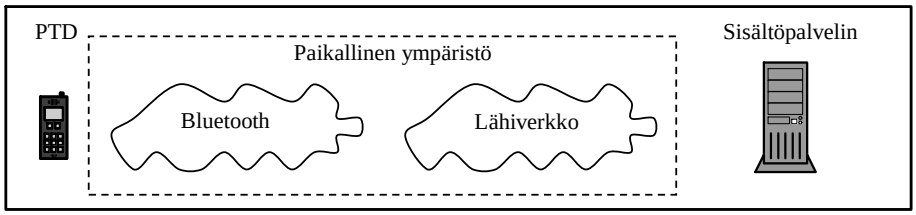
2.1 Maksuympäristöt

Maksujärjestelmät voidaan jaotella niiden käyttöympäristön mukaisesti kolmeen ryhmään: *etäympäristön*, *lähiympäristön* ja *työpöytäympäristön* maksujärjestelmiin. Seuraavat

kappaleet pohjautuvat MeT:n (Mobile Electronic Transactions) määritelmiin. MeT on merkittävimpien telekommunikaatioalan yritysten muodostama instituutio, jonka tarkoituksena on kehittää mobiileja maksutapahtumia tukevaa viitekehystä.

2.1.1 Lähimaksaminen

Lähimaksamisella tarkoitetaan järjestelmää, jossa asiakkaan ja kauppiaan laitteistot sijaitsevat lähekkäin. Maksutapahtuman tiedonsiirtoon käytetään tavallisesti kauppiaan tarjoamaa tiedonsiirtoverkkoa (kuva 1). Lähimaksamisessa yleisesti käytettyjä tiedonsiirtotekniikoita ovat lyhyen kantaman radiotekniikat Bluetooth ja RFID (Radio Frequency Identification) sekä infrapunatiedonsiirto. [MET02a]



Kuva 1. Lähimaksamisen ympäristö

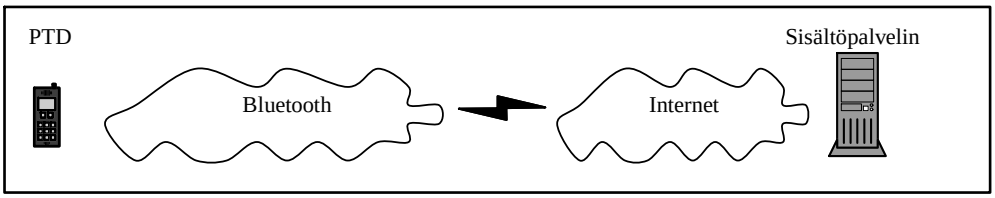
Lähimaksaminen perustuu useimmiten etukäteen maksettujen tilien, lippujen tai erilaisten maksukorttien käyttöön. Ostotapahtumien pitää olla nopeita ja yksinkertaisia, minkä vuoksi myös maksuvälineen käyttöliittymän tulee olla yksinkertainen.

Yksi uusimmista lähimaksamisen sovelluksista on maksaminen matkapuhelimen kuoriin asennetun mikrosirun avulla. Siru sisältää Visa Electron -maksukortin tiedot, jotka voidaan etälukea palvelupisteissä ja kauppojen kassoilla käyttämällä RFID-tekniikkaa [NOR03]. Myös infrapunatekniikalla toteutettuja järjestelmiä on kehitetty. Niissä voidaan matkapuhelimen avulla nostaa rahaa pankkiautomaatista, ostaa lippuja tai asioida automaateilla. Toinen tapa on välittää kauppiaille luottokortin numero, jolta maksu suoritetaan. [VIS03]

2.1.2 Etämaksaminen

Etämaksamisen järjestelmissä asiakas ja kauppias voivat sijaita kaukana toisistaan, ja osapuolten välisessä kommunikoinnissa käytetään hyväksi matkapuhelinverkkoa ja/tai

muuta laajan alueen tiedonsiirtoverkkoa (kuva 2). Näiden verkkojen lisänä voidaan käyttää lyhyen kantaman tiedonsiirtotekniikoita pääsyverkon toteuttamiseksi. [MET02a]



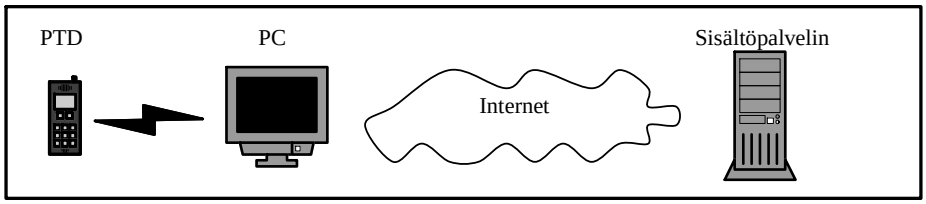
Kuva 2. Etämaksamisen ympäristö

Pankkien verkkopankkipalvelut lukeutuvat etämaksamisen järjestelmiin. Tällöin maksu suoritetaan tililtä, jolle asiakkaalla on verkkopalvelutunnukset. Verkkopalveluissa käytetään käyttäjätunnusta ja salasanaa järjestelmään kirjautumiseen, sekä kertakäyttöisiä salasanoja yhteyden suojaamiseen. [WAR97]

Esimerkkejä etämaksamisesta ovat matkapuhelimien logo-, soittoääni- ja muut tekstiviestien tai puhelinsoiton välityksellä toimivat palvelut, kuten parkkimaksaminen [PAY04], karttapalvelut [POR03b] tai lähiliikenteen matkalippujen ostaminen [LII03]. Tällaisten palveluiden laskutus tapahtuu matkapuhelinliittymän laskutuksen yhteydessä. Joissakin palveluissa laskutus voidaan vaihtoehtoisesti suorittaa luotolliselta tililtä [POR03a]. Tällöin tekstiviestien mukana välitetään joko luottokortin tietoja tai erillistä tunnusta, jotka viittaavat tiettyyn luotolliseen tiliin.

2.1.3 Työpöytämaksaminen

Työpöytämaksamisella tarkoitetaan lähimaksamisen erikoistapausta, jossa henkilökohtaista päätelaitetta käytetään ainoastaan asiakkaan tunnistamiseen ja mahdollisesti salaustoimintoihin tietokoneen välityksellä. Ostaminen ja maksaminen tapahtuvat pöytäkoneen avulla, jolloin hyödynnetään pöytäkoneen tarjoamaa käyttöliittymää. Kommunikointiin voidaan käyttää kiinteää verkkoa pöytäkoneen ja kauppiaan välillä (kuva 3). Päätelaite voi olla yhdistettynä pöytäkoneeseen joko langattomasti tai kiinteästi. [MET02a]



Kuva 3. Työpöytämaksamisen ympäristö

Eräs työpöytämaksamisen sovellus on HST-kortin (Henkilön Sähköinen Tunnistaminen) käyttäminen tunnistukseen ja salaustoimintoihin henkilökohtaisen päätelaitteen avulla. Tällöin HST-kortilla olevan varmenteen avulla voidaan todistaa henkilöllisyys etäpalvelimelle. HST-kortin avainparia voidaan taas käyttää salaustoimintoihin. Käyttökohteena voi olla edellä mainittu pankin verkkopalvelu. Työpöytämaksamisen ympäristössä voidaan käyttää myös GSM-puhelimen (Global System for Mobile Communications) SIM-korttia (Subscriber Identity Module) käyttäjän tunnistukseen ja tietoyhteyden salaamiseen [KHU02].

2.2 Ostotapahtuman kulku

Kaupankäynti jakautuu yleisesti neljään eri osaan. Ensiksi kauppiaat mainostavat tuotteitaan potentiaalisille asiakkaille. Asiakkaat tekevät hankintapäätöksen ja esittävät kauppiaille halukkuutensa palvelun ostamiseksi. Kauppiaat laskuttavat asiakkaita palveluiden mukaisesti, ja lopuksi välittävät heille kaupanteon todistavan tositteen.

2.2.1 Mainostaminen

Kauppiaat pyrkivät mainosten avulla saamaan uusia asiakkaita ja kasvattamaan asiakkaiden ostohalukkuutta. Kun maksuvälineenä käytetään langatonta päätelaitetta, avautuu mainostamiselle uusia mahdollisuuksia: asiakkaiden tunnistaminen mahdollistaa henkilökohtaisten mainosten ja kuponkien lähettämisen suoraan asiakkaille [JÄP01b]. Tällöin asiakkaat voidaan ryhmitellä ja markkinointi suorittaa ryhmäkohtaisesti. Tyypillinen esimerkki asiakasryhmästä on kanta-asiakkaat.

Mainostuksessa voidaan käyttää hyväksi asiakkaiden paikkatietoja. Asiakkaille voidaan mainostaa palveluita tietyn kohdealueen, esimerkiksi kaupan sisällä. [MET02a] [LII03] Myös laajemman alueen palvelut, kuten sääpalvelut, ovat mahdollisia.

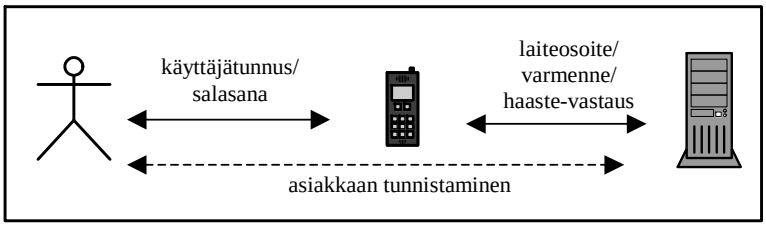
Käytettävyyden kannalta on hyvä, ettei mainosten vastaanottaminen vaadi asiakkailta mitään toimenpiteitä. Toisaalta päätelaitteen näytölle itsestään ilmestyvät mainokset koetaan helposti turhauttaviksi, etenkin jos niiden määrä kasvaa suureksi. Mainostoiminto tulee olla helposti kytkettävissä pois päältä ja mainosten selaaminen siirrettävissä myöhempään ajankohtaan niin haluttaessa. Käyttäjäprofiilien avulla voidaan määrittää minkälaisia mainoksia otetaan vastaan, milloin ja kuinka usein.

Toinen vaihtoehto mainosten vastaanottamiseen on mainoskyselyn tekeminen, jolloin mainoksia vastaanotetaan ainoastaan silloin kun halutaan. Tällöin vastaanottaminen ei ole käytettävyydeltään parasta luokkaa, mutta menetelmän avulla päästään eroon epämiellyttävistä mainosryöpyistä. Käyttäjäprofiilien avulla voidaan edelleen määrittää, minkälaisia mainoksia halutaan vastaanottaa.

2.2.2 Ostaminen

Ostotapahtuman aloittaa yleensä asiakas ilmaisemalla halukkuutensa jonkin hyödykkeen hankkimiseksi. Kaupankäynnissä halutaan usein tietää keneltä ollaan ostamassa, mikä on tuotteen hinta ja mitkä ovat mahdolliset tuotteen mukana saatavat oheispalvelut. Kauppias haluaa usein myös varmistua asiakkaansa henkilöllisyydestä, tämän maksukyvystä ja mahdollisesta kanta-asiakkuudesta. Ostamisvaiheen lopuksi kauppias lähettää laskun asiakkaalle tarkasteltavaksi.

Asiakkaan tunnistaminen suoritetaan yleensä tämän esittäessä ostoaikeensa. Samassa yhteydessä voidaan todeta esimerkiksi kanta-asiakkuudet. Koska langattomassa maksujärjestelmässä maksuvälineenä käytetään langatonta päätelaitetta, on asiakkaan tunnistusketju kaksivaiheinen. Tällöin puhutaan epäsuorasta tunnistamisesta, jossa tunnistetaan erikseen maksuvälineen käyttäjä sekä itse maksuväline (kuva 4).



Kuva 4. Asiakkaan tunnistamisketju

Maksuväline tunnistaa käyttäjän, jolloin aukottoman tunnistusketjun aikaansaamiseksi maksuvälineen pitää olla luotettava. Käyttäjän tunnistus suoritetaan usein käyttäjätunnuksien ja salasanojen avulla. Laitteiden keskinäisessä tunnistuksessa voidaan käyttää hyväksi laiteosoitteita, kertakäyttöisiä salasanoja, varmenteita ja/tai haaste/vastaus-menetelmää.

2.2.3 Maksaminen

Asiakas haluaa useimmiten tarkastella saamaansa laskua ennen sen maksamista. Langattomassa maksujärjestelmässä maksuväline tulostaa laskun tiedot asiakkaalle. Jos lasku näyttää olevan oikein laadittu ja tilattu hyödyke halutaan edelleen ostaa, voidaan lasku hyväksyä maksettavaksi. Tällöin asiakas lähettää kauppiaalle maksuhyväksynnän maksuvälineen avustuksella. Kauppias veloittaa asiakasta käytettävän maksumenetelmän mukaisesti.

Koska sähköisessä maksujärjestelmässä laskun toimittaminen tapahtuu tiedonsiirtoverkkoa pitkin eikä kauppias ole fyysisesti läsnä, pitää asiakkaan pystyä varmistumaan laskun alkuperästä, oikeellisuudesta ja muuttumattomuudesta. Samoin kauppias haluaa varmistaa maksuhyväksynnän alkuperän ja aitouden. Tämän vuoksi ostovaiheessa suoritetun asiakkaan ja kauppiaan tunnistamisen jälkeen täytyy myös suojata maksamiseen käytettävä tietoyhteys.

2.2.4 Maksutosite

Sähköinen kuitti on todistus maksusuorituksesta, jonka avulla voidaan todistaa aikaisemmin suoritetut maksutapahtumat. Kuitista käy ilmi ostotapahtuman ajankohta ja sen yksilöivä tunnistenumero, ostetut hyödykkeet, ostosten loppusumma ja käytetty valuutta sekä kauppiaan tunnistetiedot. Kuitissa voidaan mainita myös käytetty maksumenetelmä sekä mahdollinen tieto kanta-asiakkuuden tunnistamisesta.

Kuitin tietoja ei saa pystyä muuttamaan, eikä sen kopioimisesta saa olla hyötyä. Kuittien siirtämiseen voidaan käyttää suojattua tietoyhteyttä, jolloin ulkopuoliset eivät saa kuittitietoja selville. Turvallisempi tapa on kuitenkin käyttää kuiteissa kauppiaan

allekirjoitusta ja lisätä kuittiin ostajakohtaista tietoa, kuten maksuvälineen laiteosoite ja asiakkaan nimi.

Asiakkaalla tulee olla mahdollisuus selata ja tarkastella kuitteja jälkeenpäin päätelaitteellaan. Samoin hänellä pitää olla mahdollisuus vanhojen kuittien poistamiseen. Myös kuittien siirtäminen päätelaitteiden välillä tulisi olla mahdollista, jotta sähköisen kuitin toiminta vastaisi käytettävyydeltään paperikuittia. Jotta kuittia voidaan käyttää ostoksen todistuskappaleena jälkeenpäin, täytyy päätelaitteessa olla toiminto, jonka avulla kuitti voidaan lähettää esimerkiksi kauppiaalle tarkastettavaksi. MeTin määrityksen mukaan päätelaitteella tulisi olla mahdollista vastaanottaa sähköinen kuitti, vaikkei itse maksaminen tapahtuisikaan päätelaitetta käyttäen. [MET02e][MET02f]

2.3 Maksumenetelmät

Maksujärjestelmiä voidaan jaotella myös käytettävän maksumenetelmän mukaisesti. Maksu voidaan suorittaa *etukäteen, ostohetkellä* tai *jälkikäteen*. Lippujen hankkiminen on esimerkki maksun etukäteen suorittamisesta, jolloin maksun suuruinen rahasumma on sidottu palveluun ennen sen hankkimista. Etukäteen maksetun tilin käytön voidaan katsoa kuuluvan ostohetkellä maksamiseen, samoin kuin erilaisten maksukorttien käytön. Jälkikäteen suoritettu maksaminen voi perustua asiakkaalle jälkeenpäin lähetettävään laskuun. Esimerkkejä tällaisesta maksutavasta ovat luotollisten tilien käyttö ja matkapuhelinoperaattorin kautta suoritettava laskutus.

2.3.1 Sähköiset liput

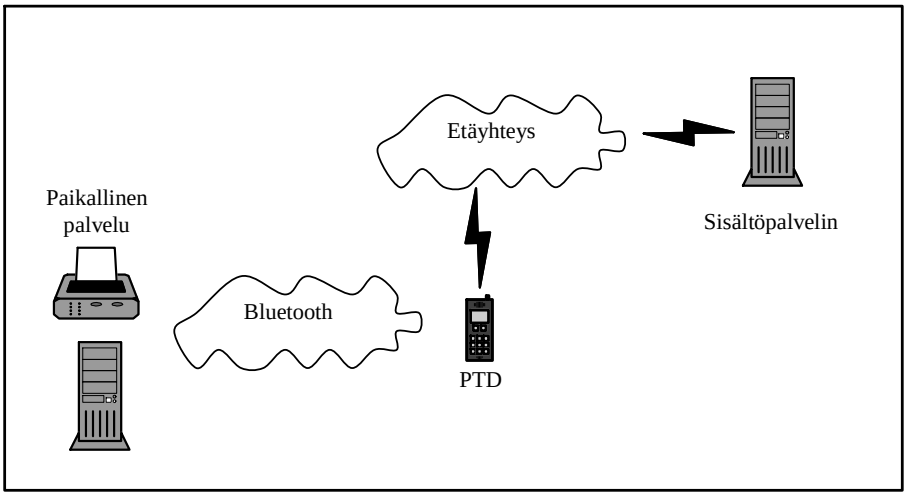
Sähköiset liput ovat maksujärjestelmän osa, jossa sähköisellä objektilla voi lunastaa tiettyjä palveluita tai tavaroita. Näin ollen lippu hankitaan yleensä lähitulevaisuudessa tapahtuvaa ostotapahtumaa varten, jolloin palvelu on maksettu etukäteen. Sähköisten lippujen tarkoitus on toimia vastineena kaikille nykyään käytetyille paperilipuille, kuten pääsylipuille, matkalipuille ja alennuskupongeille. [MET03b]

Lippujen tyypit

Pääsyliput ja alennuskupongit ovat kertakäyttöisiä, kun taas matkaliput ja kausikortit voivat olla myös kestolippuja. Jotkut liput ovat henkilökohtaisia, joitakin taas voidaan

siirtää toisille käyttäjille. Tällöin lipusta ei kuitenkaan saa jäädä kopiota sen vanhalle omistajalle.

Liput voidaan karkeasti jakaa kahteen ryhmään: halpoihin kertalippuihin ja korkeampaa tietoturvaa vaativiin kestolippuihin. Halpoja massatapahtumien pääsylippuja tai julkisen liikenteen matkalippuja käytettäessä suorituskykyvaatimukset ovat korkeat. Tällöin lippujen säilytyksen on tapahduttava itse maksuvälineessä. Kestolippuja ja alhaisemman suorituskyvyn vaativia lippuja voidaan säilyttää myös erillisellä palvelimella, lompakkopalvelimella, mikäli lipuntarkastuspaikoissa on mahdollisuus tietoliikenneyhteyksiin (kuva 5). [TAN02] [LII02]



Kuva 5. Sähköisten lippujen käyttöympäristö

Lippujen tiedot

Lipuissa on tietoja niin myyjästä, ostajasta kuin tuotteesta tai palvelustakin, johon lippu oikeuttaa. Yleisiä, kaikissa lipputyypeissä olevia tietoja ovat lipun otsikko, käyttäjän tunnistetiedot, lipun myöntäjän tunnistetiedot sekä myöntäjän yhteystiedot. Tuotetta tai palvelua koskevat tiedot voivat sisältää tapahtuma- tai tuotetietoja, kuten tapahtuman alkamisajan, keston, loppumisajan ja lipun hinnan.

Tuotteesta voidaan antaa lisäksi tarkempia tietoja, kuten esimerkiksi elokuvateatterin istumapaikan numero ja lipun tyyppi. Jotkut lipun tuottajat haluavat sisällyttää lippuihinsa myös omaa tietoa esimerkiksi tuotemerkistä tai palautusoikeuksista. Tällaisten tietokenttien käyttäminen lipuissa edellyttää, että käyttäjällä on mahdollisuus tarkastella lippujen sisältöä päätelaitteellaan.

Lipun hankkiminen ja käyttäminen

Lipun ostamisessa voidaan käyttää hyväksi lippuautomaatteja tai etäpalvelimia maksuvälineen ominaisuuksista ja maksujärjestelmästä riippuen. Lipun maksamisessa voidaan käyttää mitä tahansa maksumenetelmää. Usein liput hankitaan etäyhteyden avulla, kuten Internetistä, ja käytetään paikallisen tietoyhteyden avulla lippujen tarkastuspaikassa. Tarkastuspaikassa voi olla tulostin, jonka avulla sähköisen lipun saa muutettua paperiseksi, tai ainoastaan indikaattori, joka osoittaa lipun oikeellisuuden. [MET03b] [LII02]

2.3.2 Etukäteen maksetut tilit

Etukäteen maksetut tilit ovat esimerkki maksun suorittamisesta ostohetkellä. Tällöin tietyn maksujärjestelmän käyttöön on sidottu rahaa etukäteen, mutta laskutus tapahtuu vasta ostohetkellä. Menetelmän etuna on se, että asiakkaan maksukyky on helposti todettavissa ja asiakkaan tiedot on saatu talteen jo tilin avaamisen yhteydessä. Toisaalta tilin käyttö edellyttää asiakkaan luotettavaa tunnistamista.

Maksuhyväksynnän saatuaan kauppias velottaa asiakkaan tililtä laskun suuruisen summan. Jos tilillä ei ole katetta, maksusuoritus hylätään ja siitä ilmoitetaan asiakkaalle. Joissakin maksujärjestelmissä tilin ylitys voidaan sallia sakon uhalla.

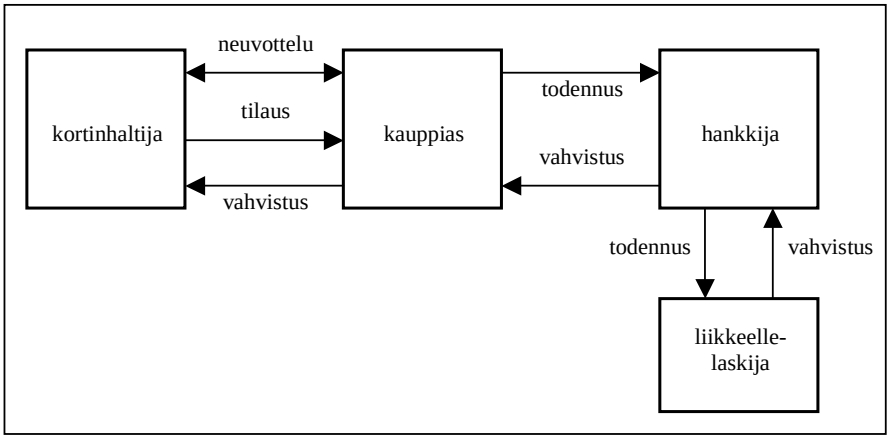
Kun maksamiseen käytetään tilejä, maksutositteiden merkitys kasvaa. Asiakkaalla pitää olla mahdollisuus saada haltuunsa kaikkien tililtä tehtyjen maksujen tositteet. Myös tilin saldo tulee olla vaivattomasti tarkastettavissa. Jotta tilien käyttö maksumenetelmänä olisi sujuvaa, pitää myös talletusten tekemisen olla vaivatonta.

2.3.3 Pankkikortit

Myös pankkikorttien tietoja voidaan käyttää hyväksi sähköisessä maksamisessa. Tällöin asiakas välittää maksuvaiheessa pankkikorttinsa tiedot kauppiaalle, joka tämän jälkeen tiedustelee kortin tietojen oikeellisuutta pankkikortin myöntäjältä. Jos asiakkaan tilillä on katetta, voidaan maksu suorittaa tililtä. MasterCard ja Visa ovat kehittäneet Internetin pankkikorttimaksamiseen määritelmän SET (Secure Electronic Transactions), josta käy ilmi pankkikorttimaksamisen osapuolet ja niiden välinen toiminta.

SET-mallin toimijat

SET-mallissa voidaan erotella neljä eri toimijaa (kuva 6). **Kortinhaltija** on pankkikortin omaava, todennettu järjestelmän asiakas, joka on rekisteröitynyt liikkeellelaskijalle. **Kauppias** myy tarvikkeita tai palveluita, ja hyväksyy sähköisen maksamisen. **Hankkija** (engl. Acquirer) on rahoituksellinen instituutio, joka tukee kauppiaiden toimintaa tarjoamalla heille pankkikorttimaksamispalvelun. **Liikkeellelaskija** (engl. Issuer) on rahoituksellinen instituutio, joka myöntää ihmisille pankkikortteja. Liikkeellelaskijoina toimivat tavallisesti pankit ja luottokunnat.



Kuva 6. SET-malli

Tämän lisäksi SET-mallissa voidaan katsoa olevan toissijaisia toimijoita. **Maksuyhdyskäytävä** on järjestelmä, jonka avulla hankkija tai muu taho tarjoaa kauppiaille jatkuvan yhteyden sähköisen kaupan palveluihin. **Varmentajat** puolestaan varmentavat kortinhaltijoiden ja kauppiaiden tai heidän yhdyskäytäviensä julkisia avaimia. [SET97]

SET-mallin toiminta

Kun kortinhaltija ostaa kauppiaalta hyödykkeen, lähettää hän tilauksen kauppiaalle (kuva 6). Kauppias välittää saamansa tilauksen hankkijalle maksuyhdyskäytävää pitkin todentaakseen kortinhaltijan. Hankkija todentaa kortinhaltijan liikkeellelaskijan avustuksella, ja saadessaan tältä todennusvahvistuksen välittää sen kauppiaalle. Kauppias lähettää ilmoituksen edelleen kortinhaltijalle maksun onnistumisesta.

Julkisen avaimen järjestelmää käytetään SET-mallissa kortinhaltijan tekemän maksumääräyksen salaamiseksi ja allekirjoittamiseksi sekä mallin toimijoiden tunnistamiseksi. Tunnistuksen avulla voidaan eliminoida kauppiaaksi tai hankkijaksi tekeytyminen sekä varastetun pankkikortin käyttö. [WAR97]

2.4 Lähimaksujärjestelmä

Koska työpaikkaruokailun maksaminen ja automaattimaksaminen suoritetaan aina joko ruokalassa tai automaatin läheisyydessä, voidaan maksamiseen käyttää lähiympäristön maksujärjestelmää eli *lähimaksujärjestelmää*. Tällöin maksuvälineenä voidaan käyttää langatonta päätelaitetta, jossa on sopiva tiedonsiirtotekniikka ja muut ominaisuudet maksusovellusten suorittamiseksi.

2.4.1 Ostotapahtuma

Ruokalamaksujärjestelmässä voidaan toimittaa päivän ruokalista asiakkaille päätelaitteeseen mainoksen tavoin. Myös erikoistarjoukset, automaattien tarjonta ja teemaviikkojen tiedot voidaan toimittaa asiakkaille samalla periaatteella.

Ruokalamaksaminen samoin kuin automaattimaksaminenkin vaativat nopeaa maksusuoritusta. Tällöin asiakkaalla täytyy olla nopea tapa suorittaa maksaminen päätelaitteellaan. Tämä vaatii yksinkertaista ja selkeää käyttöliittymää maksuvälineeltä, kuitenkin siten, että päätelaitetta käyttäen voidaan ostaa useammanlaisia hyödykkeitä. Ostohalukkuuden ilmoittamisen, maksun suorittamisen ja kuitin vastaanottamisen pitää tapahtua paitsi nopeasti myös mahdollisimman vähin toimenpitein.

Vaikkakin työpaikkaruokala- ja automaattiostokset ovat yleensä pieniä, ovat ne myös usein toistuvia. Tämän takia työn tarkoituksena on suunnitella luotettava ja turvallinen maksujärjestelmä. Aikakriittisyys luo haasteen asiakkaan tunnistamiselle ja tietoyhteyden suojaamiselle.

2.4.2 Maksumenetelmä

Työpaikkaruokailun laskutus suoritetaan nykyisin monessa paikassa paperisten ruokalippujen avulla. Näin ollen etukäteen hankittavien sähköisten lippujen

hyödyntäminen ruokailun maksamisessa voisi olla toimiva ratkaisu. Lippujen käyttö soveltuu kuitenkin vain tietyn tuotteen tai tietyn arvoisen tuotteen hankkimiseen. Koska maksuvälineellä on tarkoitus maksaa muitakin kahvilaostoksia kuin pelkästään ruokailu, kasvaa erilaisten lippujen määrä suureksi. Toisaalta jokapäiväisen maksutapahtuman suorittamiseksi päätelaitteissa säilytettävien lippujen määrä kasvaa joka tapauksessa suureksi, ellei niitä osteta viikoittain lisää.

Maksukorttien käytön ongelmana on erilaisten maksukorttien suuri määrä. Päästäkseen maksujärjestelmän käyttäjäksi asiakkaan pitää hankkia oikeanlainen pankkikortti omasta pankistaan. Tällöin järjestelmästä tulisi korttiriippuvainen. Jälkeenpäin tapahtuva laskutus esimerkiksi työntekijän palkasta puolestaan tuottaa ongelmia etenkin suuremmissa organisaatioissa, joissa eri työntekijöillä voi olla eri palkanmaksajia.

Kun käytetään kauppiaan hallinnoimia tilejä, joille tehdään talletuksia etukäteen, voivat kaikki työntekijät halutessaan liittyä maksujärjestelmään. Ainoa toimenpide ennen maksamista on tilin avaaminen ja talletuksen tekeminen. Kun tilien ylläpitäjänä toimii työpaikkaruokailun järjestävä ravintoloitsija, on tileiltä laskuttaminen nopeaa maksamisen yhteydessä. Tilien avulla voidaan maksaa mitä tahansa ostoksia, ja lisäksi niitä voidaan tehdä saman ravintoloitsijan ylläpitämistä automaateista ruokalan aukioloaikojen ulkopuolella.

Tilien käyttäminen maksumenetelmänä saa aikaan tarpeen uudelle toiminnolle: tilikyselyjen tekemiselle. Koska asiakas sitoo rahaa järjestelmän käyttöön, eikä maksaminen onnistu ilman riittävää saldoa tilillä, pitää hänen saada halutessaan vaivatta tietoonsa tilin saldo.

3 Tunnistus ja tietoyhteyden suojaus

Koska lähimaksujärjestelmässä on valittu käytettäväksi etukäteen maksettavia tilejä, on asiakkaan tunnistus ostotilanteessa hyvin tärkeää. Kaupankäynnissä myös muiden osapuolten luotettava tunnistaminen ja maksamiseen käytettävän tietoyhteyden suojaaminen ovat tärkeitä tehtäviä. Asiakkaan tunnistaminen jakautuu päätelaitteen suorittamaan käyttäjän tunnistamiseen ja palvelimen suorittamaan päätelaitteen tunnistamiseen. Myös päätelaite tunnistaa palvelun tarjoajan. Tietoyhteyden suojaaminen perustuu lähetettävien viestien salaamiseen.

3.1 Tiedon salaaminen

Tiedon salaamisella pyritään vastaamaan tietoturvan vaatimuksiin, joiden avulla varmistetaan tiedon yksityisyys, todennus, eheys sekä kiistämättömyys. Tätä vaatimusmallia kutsutaan PAIN-malliksi (Privacy, Authentication, Integrity, Non-repudiation). [MEN96]

Salausmenetelmät perustuvat kahteen erilaiseen salaukseen: symmetriseen ja epäsymmetriseen. Menetelmät eroavat toisistaan itse salausmenetelmän, käyttökohteiden sekä avainten hallinnan vuoksi. Salauksen ja salauksen purkamisen suorittavien algoritmien syötteinä käytetään salausavaimia.

Symmetrinen salaus

Symmetrisellä salausalgoritmilla salattaessa ja purettaessa käytetään samaa avainta salausalgoritmin syötteenä. Kyseinen avain tulee olla sekä salaajan että purkajan tiedossa ja toisaalta vain heidän tiedossaan, jotta salauksesta olisi hyötyä. Ongelmaksi muodostuukin avaimen salassa pitäminen. Tämän takia symmetrisessä salauksessa käytettävät avaimet määritelläänkin yleensä lyhytikäisiksi.

Tietoyhteyksiä salattaessa avainten määrä kasvaa nopeasti, kun jokaisen tietoyhteyden salaamiseen joudutaan käyttämään eri avainta. Monissa protokollissa käytetäänkin

kertakäyttöistä avainta. Symmetristä salausta suositummaksi menetelmäksi on monessa käyttökohteessa muodostunut epäsymmetrisen salauksen menetelmät. [MEN96]

Epäsymmetrinen salaus

Epäsymmetrisellä salausalgoritmilla salattaessa ja purettaessa käytetään eri avaimia salausalgoritmin syötteinä. Tarvittavan avainparin muodostavat julkinen ja salainen avain. Salaista avainta vastaava julkinen avain voidaan laskea salaisen avaimen avulla, mutta julkisen avaimen perusteella ei voida päätellä mitään salaisesta avaimesta. Järjestelmän turvallisuus perustuukin siihen, että salaiset avaimet ovat ainoastaan niiden omistajien tiedossa.

Kun tieto salataan julkisella avaimella, voidaan salaus purkaa ainoastaan julkista avainta vastaavalla salaisella avaimella. Jos tieto vastaavasti salataan salaisella avaimella, voidaan salaus purkaa ainoastaan vastaavalla julkisella avaimella. Epäsymmetristen salausmenetelmien avaimet ovat pitkäikäisempiä kuin symmetrisen salauksen avaimet, mikä puolestaan luo tarpeen avainten tehostetulle hallinnoimiselle. [MEN96]

Hybridisalaus

Epäsymmetrinen salaus on huomattavasti hitaampaa kuin symmetrinen salaus, koska sen salausavaimet ovat symmetrisen salauksen avaimia huomattavasti pidempiä. Julkisen avaimen järjestelmät tarjoavat kuitenkin turvallisemman avainten hallinnoinnin. Näiden yhdistelmän, hybridisalauksen avulla pyritään hyödyntämään kummankin menetelmän vahvuudet. [MEN96]

Tiivisteet

Tiivistealgoritmien avulla voidaan mistä tahansa tiedosta muodostaa vakiomittainen, yleensä alkuperäistä tietoa selvästi lyhyempi tiiviste. Tiivistealgoritmi huomioi syötteen kaikki merkit tiivistettä laskettaessa ja luo niiden perusteella yksilöllisen tiivisteen. Usein tiivisteet lasketaan yksisuuntaisilla algoritmeilla, jolloin tiivisteen laatimisessa käytettyä syötettä on käytännössä mahdotonta selvittää tiivisteestä. Yhtenevät tiivisteet voidaan luoda ainoastaan yhtenevistä alkuperäistiedoista. [SMI01]

Käyttäjän tunnistusta suorittavan laitteen muistissa säilytetään usein pelkät salasanojen tiivisteet, ja siten myös salasanojen vertailut suoritetaan kyseisten tiivisteiden avulla. Tiivisteitä voidaan käyttää myös digitaalisessa allekirjoituksessa. [SCH96]

Digitaalinen allekirjoitus

Digitaalinen allekirjoitus luodaan laskemalla tiiviste jollakin tunnetulla yksisuuntaisella tiivistealgoritmilla allekirjoitettavasta tiedosta. Tämä tiiviste salataan allekirjoittajan salaisella avaimella ja liitetään allekirjoitettavan tiedon perään. [SCH96]

Vastaanottaja voi tarkastaa allekirjoituksen purkamalla tiivisteen allekirjoittajan julkisella avaimella, laskemalla itse tiivisteen allekirjoitetusta tiedosta samalla algoritmilla ja vertaamalla tiivisteitä. Jos tiivisteet ovat samanlaiset, on tieto tullut perille muuttumattomana ja sen on laatinut ko. allekirjoittaja. Menetelmällä vastataan PAIN-mallin vaatimuksiin tiedon kiistämättömyydestä ja eheydestä. [RSA99b]

3.1.1 PKI

Julkisen avaimen infrastruktuurin (PKI, Public Key Infrastructure) avulla pyritään ratkaisemaan julkisten avainten hallinnoimisesta aiheutuvia ongelmia. PKI:lla tarkoitetaan organisaatioiden, menetelmien, protokollien ja tapojen joukkoa, jonka avulla luodaan, varmennetaan ja toimitetaan julkisia avaimia [SMI01]. PKI perustuu digitaaliseen allekirjoitukseen sekä kolmannen, luotettavan osapuolen (TTP, Third Trusted Party) myöntämiin varmenteisiin.

Varmenteet

Julkisen avaimen kiistämättömyys varmistetaan sertifikaattien eli varmenteiden avulla. Varmenne on tavallisesti kolmannen, luotettavan osapuolen laatima todistus varmennettavan tahon identiteetistä. Luotettua tahoa, joka toimii varmentajana, kutsutaan varmentajaksi (CA, Certification Authority). [RSA99b]

Varmentajat toimivat hierarkkisesti niin, että juurivarmentaja (RCA, Root Certification Authority) varmentaa muita alemman tason varmentajia, jotka edelleen toimivat yksityisten tahojen varmentajina. Tällaisia julkisia varmentajia on Suomessa muun muassa

väestörekisterikeskus. Juurivarmentajalla on itse luotu varmenne, juurivarmenne, johon kaikkien tahojen tulee voida luottaa.

Varmenteen avulla voidaan osoittaa käyttäjän identiteetin lisäksi tämän hallinnoima julkinen avain. Varmenteen loppuun on liitetty siitä laskettu tiiviste, joka on digitaalisesti allekirjoitettu varmentajan salaisella avaimella. Mikäli kommunikoivat osapuolet eivät tunne toistensa varmentajia allekirjoituksia tarkastaessaan, voivat he tarkastaa varmentajien varmennusketjun, kunnes vastaan tulee tunnettu varmentaja tai juurivarmentaja. [MET02d]

Yleisin varmennestandardi on ITU-T:n (International Telecommunications Union, Technical Standards Section) standardoima X.509-varmenne. Sen tiedot (kuva 7) esitetään ASN.1-määritelmän (Abstract Syntax Notation #1) mukaisesti. **Versio** (engl. Version) ilmaisee varmenteen versionumeron. Uusin versio on X.509v3, joka sallii laajennuskenttien määrittelyn varmenteisiin. Varmentaja, joka luo varmenteen, on velvollinen pitämään yllä juoksevaa **sarjanumerointia** (engl. Serial number) luomilleen varmenteille ja lisäämään sen varmenteeseen tunnisteeksi.

Version
Serial number
Signature Algorithm ID
Issuer
Validity Period
Subject
Subject Public Key Information
Issuer Unique Identifier
Subject Unique Identifier
Extensions
Digital Signature

Kuva 7. X.509-varmenteen sisältö

Allekirjoitusalgoritmi (engl. Signature Algorithm ID) määrittelee algoritmin, jota varmentaja on käyttänyt muodostaessaan digitaalisen allekirjoituksen varmenteesta. **Myöntäjän nimi** (engl. Issuer) on varmenteen myöntäjän eli allekirjoittajan X.500-muotoinen nimitunniste. Tämä nimitunniste sisältää seuraavia komponentteja:

- nimi (CN, Common Name)
- organisaatio (O, Organization)
- yksikkö (OU, Organization Unit)
- valtio (C, Country

Voimassaoloaika (engl. Validity Period) kuvaa varmenteen voimassaoloajan alkamis- ja loppumisajankohdan. **Haltijan nimi** (engl. Subject) kertoo vastaavat tiedot varmenteen haltijasta kuin aiemmin ilmoitettiin varmenteen myöntäjästä.

Julkisen avaimen tiedot (engl. Subject Public Key Information) käsittää varmenteen haltijan julkisen avaimen. Tietokentässä kerrotaan myös, minkä algoritmin mukainen avain on ja mahdollisesti muita avaimeen liittyviä parametreja.

Myöntäjän ja haltijan yksilöiviä tunnisteita (engl. Issuer Unique Identifier, Subject Unique Identifier) käytetään määrittämään varmenteen haltija ja myöntäjä silloin, kun samassa järjestelmässä esiintyy samannimisiä toimijoita. X.509v3 voi sisältää myös **laajennuksia** (engl. Extensions), joissa voidaan esittää jotain muuta käyttäjäkohtaista tietoa. Standardilaajennuksia on esitetty lähteessä [HOU02]. **Allekirjoitus** (engl. Digital Signature) on koko varmenteesta edellä määritellyllä tavalla muodostettu digitaalinen allekirjoitus. [HOU02]

X.509-varmenteet säilytetään ja siirretään yleensä PEM-muodossa (Privacy Enhanced Mail). Tällä tarkoitetaan varmenteen sisällön muokkaamista sellaiseen muotoon, jotta se voidaan tunnistaa varmenteeksi, siirtää kaikissa järjestelmissä muuttumattomana ja muuttaa yksiselitteisesti takaisin alkuperäiseen muotoonsa. Tämä on mahdollistettu Base64-koodauksen avulla. [OPE02]

Peruutuslista ja varmennehakemisto

PKI-mallissa on varmentajien lisäksi rekistereiden ylläpitäjiä (RA, Registration Authority). Peruutuslistan (CRL, Certificate Revocation List) ylläpitäjä pitää listaa kaikista voimassaoloaikana peruutetuista varmenteista. Peruutuslistan avulla mahdollistetaan salausavainten käyttökelvottomaksi saattaminen järjestelmän ylläpitäjän toimesta ja peruutettujen varmenteiden tarkastaminen. Varmenteen luotettavan tarkastuksen mahdollistamiseksi ajanmukaisen peruutuslistan on oltava jatkuvasti kaikkien varmenteiden tarkastajien saatavilla. [SMI01]

Varmennehakemiston ylläpitäjä lisää järjestelmään rekisteröityjen tahojen tiedot varmennehakemistoon ja poistaa sieltä vanhentuneet tiedot. Varmennehakemistosta voi

kuka tahansa järjestelmään rekisteröitynyt tarkastaa tietyn varmenteen olomassaolon ja sen tiedot. Pienemmissä järjestelmissä varmentaja voi itse olla sekä varmennehakemiston että peruutuslistan ylläpitäjä. [RSA99a]

PKI:n riskejä

Mikäli ilkeämielinen taho saa haltuunsa jonkun toisen tahon salaisen avaimen, voi hän käyttää sitä allekirjoittamiseen ja esiintyä näin toisena tahona. Ilkeämielinen taho voi olla käyttäjän laitteessa toimiva ohjelmakoodi, joka voi saada selville salaisen avaimen salasanan, kuten PIN-koodin (Personal Identity Number) tai sormenjälkitunnisteen.

Varmenteiden allekirjoitukset tarkastetaan varmentajien varmenteista saatavien julkisten avainten avulla. Jos ilkeämielinen taho pystyy lisäämään varmenteensa hyväksyttyjen varmentajien listalle, kelpaavat myös hänen allekirjoittamansa varmenteet tarkastajalle. Tarkastajan tulisikin suojata käyttämänsä tarkastusmenetelmät siten, etteivät ulkopuoliset pääsisi niihin käsiksi. [ELL00]

3.1.2 WPKI

WAP-forum (Wireless Application Protocol) on esitellyt WPKI-määrityksen (Wireless Public Key Interface) osana WAP:n turvallisuusstandardeja. WPKI on PKI:hin perustuva määritelmä, jonka avulla PKI:n toiminnallisuudet on optimoitu langattomaan ympäristöön. Määritelmän mukaan langattomassa ympäristössä voidaan X.509-varmenteiden lisäksi hyödyntää WTLS-varmenteita (Wireless Transport Layer Security).

WTLS-varmenteet

WTLS-varmenteet ovat langattomaan ympäristöön tarkoitettuja WAP-forumin määrittelemiä varmenteita. WTLS-varmenteet pohjautuvat X.509-varmenteisiin, mutta ne ovat pienikokoisempia ja soveltuvat siten langattomaan ympäristöön paremmin (kuva 8).

Versio kuvaa varmenteen versionumeron, joka on aina 1 nykyisen määrityksen mukaan. **Allekirjoitusalgoritmi** on WTLS-määritelmässä tuettu allekirjoitusalgoritmi, jolla varmenne on allekirjoitettu. **Myöntäjä** ilmaisee varmenteen allekirjoittajan. **Voimassaoloaika** ilmaisee varmenteen voimassaolon alkamis- ja loppumisajankohdan. **Haltija** kuvaa varmenteen omistajan tiedot. **Julkisen avaimen tiedot** kuvaa algoritmin,

jonka syötteenä avainta voidaan käyttää sekä julkiseen avaimeen liittyviä parametreja. Julkista avainta ei esitetä varmenteessa, vaan ainoastaan palvelimen osoite, josta varmenne ja julkinen avain on saatavissa. **Allekirjoitus** on koko varmenteesta muodostettu digitaalinen allekirjoitus. [WAP01b]

Version
Signature Algorithm ID
Issuer
Validity Period
Subject
Subject Public Key Information
Digital Signature

Kuva 8. WTLS-varmenteen sisältö

Käyttämällä sekä X.509- että WTLS-varmenteita mahdollistetaan WPKI:n liittäminen jo olemassa oleviin PKI-ympäristöihin. Samalla säästetään päätelaitteiden tallennuskapasiteettia sekä suoritustehoa, ja vähennetään verkon liikennettä. WPKI-määritelmä perustuu seuraaviin ohjeistuksiin [WAP01a]:

- päätelaitteilla säilytettävät WTLS-palvelimien (kpl 3.3.2) ja varmentajien varmenteet ovat WTLS-varmenteita
- palvelimilla säilytettävät WTLS-palvelimien ja varmentajien varmenteet ovat X.509-varmenteita
- langattoman tietoyhteyden yli lähetettävät ja/tai päätelaitteissa säilytettävät asiakkaiden ja juurivarmentajien varmenteet ovat X.509-varmenteita
- päätelaitteessa suositellaan säilytettävän URL:ia (Universal Resource Locator) varmennepalvelimella sijaitsevalle varmenteelle, mikäli muutoin pitäisi lähettää X.509-varmenteita langattoman tietoyhteyden yli
- muutoin X.509-varmenteita säilytetään päätelaitteissa ainoastaan tilapäisesti

3.2 Tunnistaminen

Maksujärjestelmässä asiakkaan tunnistaminen on tärkeää. Asiakkaan tunnistaminen langattomissa maksujärjestelmissä vaatii sekä maksuvälineen että maksuvälineen käyttäjän luotettavaa tunnistamista. Tunnistamisketju on siten kaksivaiheinen.

Maksuväline suorittaa käyttäjän tunnistuksen ja kauppiaan laitteiston tunnistuksen. Kauppiaan laitteisto tunnistaa vastaavasti maksuvälineen. Mikäli anonyymimaksaminen hyväksytään, ei asiakkaan tunnistusta vaadita. Tilien käyttöön perustuvassa järjestelmässä asiakas on kuitenkin tunnistettava, jotta voidaan varmistua, että asiakkaalla on oikeus käyttää tiliä.

3.2.1 Käyttäjän tunnistaminen

Maksujärjestelmässä maksuväline suorittaa käyttäjän tunnistuksen. Tarkoituksena on varmistua siitä, että maksuvälineelle kirjautuneella käyttäjällä on oikeus käyttää maksuvälineelle tallennettua salaista tietoa. Maksuvälineen käyttöoikeus voidaan rajata kestämään tietyn aikaa kerrallaan, minkä jälkeen vaaditaan uusi käyttäjän tunnistus. Näin pyritään ehkäisemään mahdollisia väärinkäytöksiä.

Käyttäjän tunnistaminen voidaan toteuttaa monella tavalla. Seuraavat asiat jakavat menetelmät eri ryhmiin [WAR97] [SMI01]:

- käyttäjällä on tiedossa salaisuus
- käyttäjällä on hallussaan esine
- käyttäjällä on yksilöllinen ominaispiirre
- edellisten yhdistelmät

Käyttäjätunnukset, salasanat ja PIN-koodit

Käyttäjätunnusten, salasanojen ja PIN-koodien (Personal Identity Number) käyttö on esimerkki salaisuuden tietämisestä. Käyttäjätunnusten avulla voidaan todeta käyttäjän henkilöllisyys, minkä jälkeen salasanojen avulla voidaan todentaa käyttäjä. [GOL99]

Salasanojen selvittämistä arvaamisen avulla voidaan ehkäistä käyttämällä riittävän laajaa salasana-avaruutta, jota voidaan kasvattaa käyttämällä salasanoissa numeroita, pieniä ja

isoja kirjaimia sekä rajoittamalla salasanojen vähimmäispituutta. Lisäksi salasanan syöttökertoja voidaan rajoittaa lukitsemalla kohde riittävän monen väärän syöttökerran jälkeen.

Usein salasanoja säilytetään sen järjestelmän muistissa, joka käyttäjän tunnistusta suorittaa. Salasanaa kysyttäessä verrataan annettua ja talletettua salasanaa toisiinsa. Turvallisuussyistä salasanat säilytetään aina salatussa muodossa, tiivisteinä. Vaikka salasana siirrettäisiin tietoyhteyden yli salattuna, ei salatun salasanan toistaminen saa johtaa onnistuneeseen tunnistustapahtumaan. [WAR97] [SMI01]

Henkilökohtainen poletti

Poletti on esimerkki henkilökohtaisesta esineestä, jonka avulla käyttäjä on tunnistettavissa. Poletin on siksi oltava pienikokoinen ja jatkuvasti mukana kannettava. Poletteja käytetään usein salasanojen ja PIN-koodien lisänä, jolloin pelkkä salasanojen arvaus ei riitä onnistuneeseen käyttäjän tunnistukseen. [SMI01]

Polettia voidaan käyttää tunnistukseen eri tavoin. Poletti voi olla salausavaimen säilytyspaikka, jolloin avaimeen pääsee käsiksi vasta oikean PIN-koodin antamisen jälkeen. Se voi toimia myös kertakäyttöisen salasanan muodostajana, minkä avulla käyttäjä on tunnistettavissa. Sitä voidaan käyttää myös haaste/vastaus-menetelmän suorittamiseen hyödyntämällä sen säilyttämää salaisuutta. [WAR97]

Polettien täytyy sietää peukalointia, jotta ne pystyvät säilyttämään salaisuutensa eikä niiden kopioiminen ole mahdollista. Henkilökohtaisina poletteina voidaan käyttää toimikortteja, USB-poletteja (Universal Serial Bus) ja PCMCIA-poletteja (Personal Computer Memory Card International Association). [WAR97] [SMI01]

Biometriset tunnistusmenetelmät

Käyttäjien ominaispiirteisiin perustuvissa biometrisissä tunnistusmenetelmissä käytetään hyväksi ihmisen yksilöllisiä sormenjälkiä, silmien iiriksiä, kasvojen muotoja, käsialaa tai ääntä. Menetelmissä mitataan lukijalaitteiden avulla henkilökohtaisia piirteitä tarkasteltavasta ominaisuudesta ja verrataan niitä talletettuihin arvoihin salasanojen tavoin.

Biometriset tunnistusmenetelmät tarjoavat varman tunnistuksen, mutta niiden käytettävyyteen liittyy muutamia ongelmakohtia. Esimerkiksi muutokset käyttäjän

ominaisuuksissa voivat saada aikaan epäonnistuneen käyttäjän tunnistuksen. Myös lukijalaitteiden likaisuus ja muut ympäristön vaikutukset voivat johtaa virheelliseen lopputulokseen. [PHI00][NEG00]

3.2.2 Laitteiden tunnistaminen

Kun maksuväline on tunnistanut käyttäjän, pitää itse maksuväline tunnistaa. Maksuvälineen tunnistamista käyttävät kauppiaiden palvelimet sekä järjestelmän rekisteröijät ja varmentajat. Langattomien päätelaitteiden tunnistamisessa voidaan käyttää laitteiden osoitteisiin, kertakäyttöisiin salasanoihin tai haaste/vastaukseen perustuvia menetelmiä.

Myös maksuvälineen pitää tunnistaa järjestelmän laitteet, joiden kanssa se on tekemisissä. Tähän voidaan käyttää samoja menetelmiä kuin maksuvälineen tunnistamiseenkin. Tunnistusmenetelmän valinnassa on kuitenkin huomioitava maksuvälineen rajoittunut suorituskyky.

Laiteosoitteeseen perustuva tunnistaminen

Laitteet voidaan tunnistaa niiden osoitteiden perusteella. Monilla päätelaitteilla on joko kiinteä laiteosoite tai tiedonsiirtotekniikan tarjoama osoitetunniste. Tunnistusmenetelmä tarkastelee sitä, mistä viestit tulevat, eivätkä sitä keneltä ne tulevat. Lisäksi laiteosoitteet ovat väärennettävissä, eikä niihin perustuva tunnistusmenetelmä siten yksikseen ole riittävän luotettava. Koska osoitetunnistuksen suorittaminen on yleensä yksinkertainen toimenpide, käytetään menetelmää usein muiden tunnistusmenetelmien lisänä. [WAR97] [SMI01]

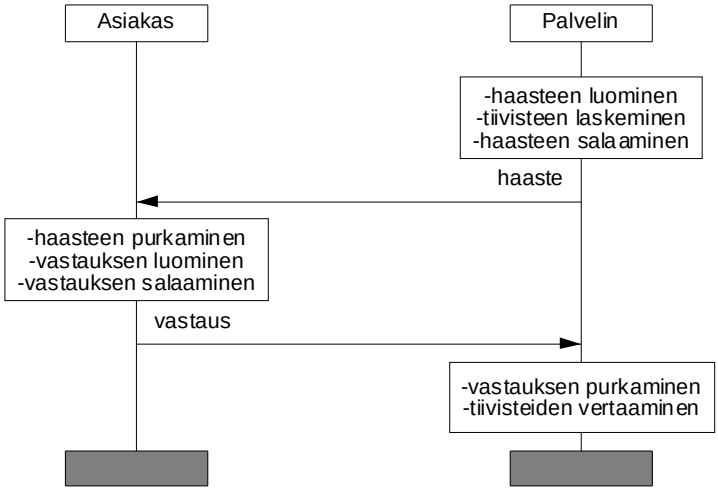
Kertakäyttöiset salasanat

Laite voi tunnistaa toisen laitteen kertakäyttöisen salasanan avulla. Tällöin tunnistava laite lähettää toiselle laitteelle satunnaisesti luodun ja salatun haasteen, jota hyväksikäyttäen tämä voi luoda kertakäyttöisen salasanan. Saatuaan salasanan tunnistava laite tarkastaa sen oikeellisuuden. Tällöin kyseessä on haaste/vastaukseen perustuva salasana. Salasanan määrittämisessä voidaan myös käyttää etukäteen laadittua salasanalistaa tai salaisuuden sisältävää polettia. [WAR97]

Varmenteet ja haaste/vastaus

Varmenteita käyttäen voidaan suorittaa haaste/vastaus-menetelmä, minkä avulla voidaan varmistua laitteen identiteetistä (kuva 9). Laite, joka haluaa tunnistaa toisen laitteen, pyytää ensiksi tunnistettavan laitteen varmennetta. Varmenteen saatuaan tunnistava laite luo haasteen. Haaste on satunnaisluku, josta lasketaan tiiviste. Haaste salataan tunnistettavan laitteen varmenteesta saadulla julkisella avaimella ja lähetetään laitteelle.

Tunnistettavan laitteen pitää vastata haasteeseen. Ensin laite purkaa saamansa haasteen ja laskee siitä tiivisteen sovitulla menetelmällä. Tiiviste lähetetään takaisin tunnistavalle laitteelle, jolloin se vertaa tiivisteitä. Jos tiivisteet ovat samanlaiset, on varmenteen haltijalla hallussaan julkista avainta vastaava salainen avain. [SCH96]



Kuva 9. Haaste/vastaus -menetelmä

Haaste-vastaus menetelmää voidaan hyödyntää myös ilman erillisen haasteen käyttöä. Esimerkki tällaisesta menetelmästä on yhteyden suojaamiseen käytettävän yhteysavaimen luominen ja salaaminen vastapuolen julkisella avaimella. Näin ollen vastapuoli saa yhteysavaimen käyttöönsä ainoastaan, jos hänellä on hallussaan julkista avainta vastaava salainen avain. [SMI01]

3.3 Tietoyhteyden suojaaminen

Maksujärjestelmissä tiedonsiirtoon vaaditaan suojattua tietoyhteyttä. Koska langatonta tiedonsiirtolinkkiä ei voida fyysisesti suojata, on yhteyden suojaamiseksi käytettävä

salaustoimintoja. Tietoyhteyden suojaus voi perustua joko symmetriseen salaukseen, epäsymmetriseen salaukseen tai niiden yhdistelmään. Seuraavassa esitellään suojaamiseen käytettyjä protokollia.

3.3.1 SSL/TLS

SSL (Secure Socket Layer) on alunperin Netscapen (http://www.netscape.com) suunnittelema menetelmä käyttäjien tunnistamiseksi ja tietoyhteyksien suojaamiseksi. Vuonna 1996 valmistui SSL-protokollan versio 3.0 [FRE96], joka on nykyään laajasti käytössä. SSL:n tarkoituksena on estää tietoliikenteen salakuuntelu ja tiedon väärentäminen kommunikoivien osapuolten välillä.

SSL on kuljetuskerroksen protokolla, jonka tarkoituksena on toimia pääasiassa yhteydellisten, luotettavien kuljetusprotokollien ja sovellustason protokollien välissä, kuten TCP/IP (Transport Control Protocol / Internet Protocol) ja HTTP (HyperText Transfer Protocol). SSL käyttää hyväksi sekä symmetristä että epäsymmetristä salausta. [FRE96]

SSL:n toiminta

SSL:n toiminta voidaan jakaa kahteen pääosaan: yhteyden muodostukseen ja siirrettävän tiedon salaukseen. Yhteyden muodostukseen, josta käytetään myös nimitystä kättely (engl. Handshake), kuuluvat osapuolten tunnistus, yhteyden avaus ja yhteysparametrien neuvottelu. Yhteysparametreja ovat mm. yhteysavaimen vaihtoon, kommunikoinnin salaukseen ja viestien tiivistykseen käytettävien algoritmien tunnisteet. Siirrettävän tiedon salaukseen käytetään symmetristä yhteysavainta. [FRE96]

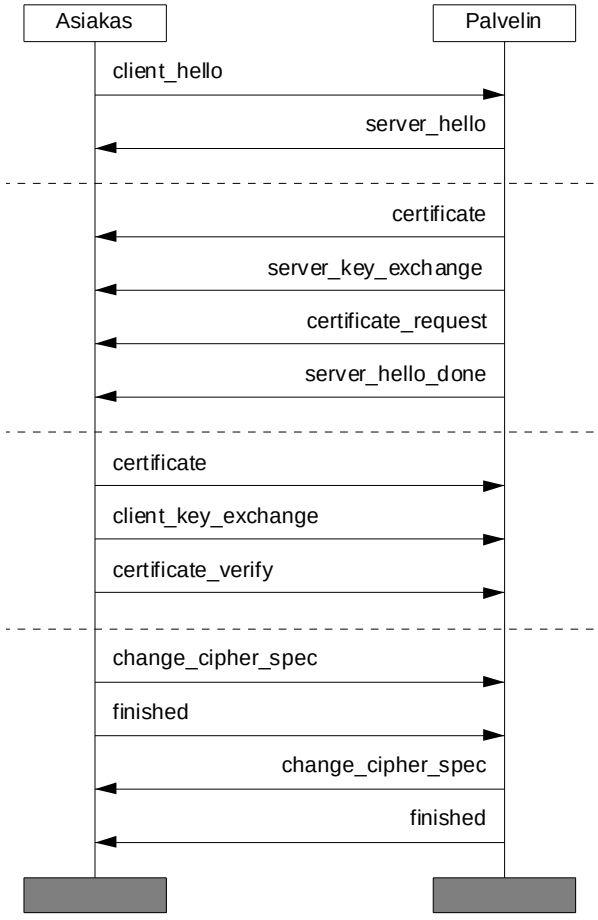
Yhteyden muodostus

Kun käytetään SSL:ää, osapuolten välillä voi olla useampia istuntoja, joista kukin voi käsittää useampia yhteyksiä. Ensimmäisessä vaiheessa neuvotellaan yhteysparametrit, jolloin asiakas voi ilmaista haluavansa käyttää aikaisemmin muodostetun istunnon parametreja (kuva 10). [FRE96]

Seuraavaksi palvelin lähettää oman varmenteensa sekä julkisen avaimensa, joiden avulla asiakas tunnistaa palvelimen. Mikäli palvelin haluaa tunnistaa asiakkaan, pyytää se asiakkaan varmennetta. Asiakas lähettää varmenteensa ja julkisen avaimensa palvelimelle.

Samalla voidaan lähettää varmenteen todentava viesti, jolla varmistetaan, että asiakas hallinnoi myös salaista avainta, jolle varmenne on myönnetty. Viesti perustuu palvelimen lähettämään satunnaislukuhaasteeseen, johon asiakkaan pitää luoda vastaus.

Yhteyden muodostuksen lopuksi hyväksytään ja otetaan käyttöön edellä neuvotellut yhteysparametrit. Lopuksi todennetaan neuvottelun eheys siten, että molemmat osapuolet laskevat hajautusarvot kaikista neuvottelun aikana välitetyistä viesteistä ja vertaavat niitä toistensa saamiin arvoihin. [FRE96]



Kuva 10. SSL-yhteyden muodostus

Tietoyhteyden salaus

Tietoyhteyden salaukseen käytetään symmetristä salaista avainta, yhteysavainta. Se lasketaan sovitulla tavalla satunnaistiedosta yhteyden avausvaiheessa.

Ylemmältä kerrokselta tuleva tieto jaetaan SSL-kerroksella pienempiin osiin, RPU-paketteihin (Record Protocol Unit). Osia tiivistetään ja muuttumattomuuden todentamiseksi niistä lasketaan MAC-tunniste (Message Authentication Code). MAC-tunniste käsittää mm. tiivisteen viestin sisällöstä, järjestysnumerosta ja pituudesta, sekä tiedon protokollasta, joka paketin tietoa käyttää. MAC-tunniste lisätään paketin loppuun, jonka jälkeen paketti salataan sovitulla symmetrisellä algoritmilla yhteysavainta käyttäen. Salatun paketin eteen lisätään vielä otsikkotietoa. [FRE96]

TLS

TLS (Transport Layer Security) versio 1.0 on IETF:n (Internet Engineering Task Force) vuonna 1999 standardoima versio SSL:stä. TLS ei eroa kovin paljoa SSL versiosta 3.0. Suurimmat erot ovat MAC-tunnisteen laskemisessa ja avainmateriaalin luomisessa. TLS sisältää joitakin uusia salausalgoritmivaihtoehtoja sekä virheviestityyppejä virhetilanteiden selvittämiseksi.

TLS:n osat, jotka huolehtivat osapuolten tunnistamisesta ja yhteyden salaamisesta, on toteutettu siten, että jatkossa on mahdollista käyttää myös muita tunnistusmenetelmiä kuin alkuperäisessä SSL:ssä. SSL:ssä jokaisen viestin lähetystä varten avataan ja suljetaan uusi pistoke (engl. Socket), kun taas TLS:ssä voidaan lähettää useita paketteja saman pistokkeen kautta. Tämä parantaa myös tiedonsiirron suorituskykyä. [DIE99] [NIC02]

3.3.2 WTLS

WTLS (Wireless Transport Layer Security) on WAP:n turvallisuuskerroksen protokolla. WTLS perustuu SSL/TLS-protokolliin, mutta se on optimoitu langattomaan ympäristöön. Langaton käyttöympäristö asettaa uusia vaatimuksia tietoyhteyden suojaamiselle. Vaatimukset toiminnallisuuden muuttamiseksi ovat seuraavat:

- tuki myös yhteydettömälle tiedonsiirrolle
- pitkien viiveiden sietokyky
- tiedonsiirron kaistanleveys voi olla rajoite
- päätelaitteiden suoritusteho voi olla rajoite
- päätelaitteiden muistikapasiteetti voi olla rajoite

Vaatimusten seurauksena WAP-forum on pyrkinyt korvaamaan salausalgoritmeja tehokkaammilla algoritmeilla. Yhteydenmuodostuksessa käytettävien WTLS-varmenteiden sisältöjä on pyritty tiivistämään ja viestien tiivistysalgoritmeja kehittämään. Itse varmenteen lähettämisen sijaan voidaan toiselle osapuolelle ilmoittaa pelkästään varmenteen osoite varmennepalvelimella. Käytetty hakemistopalvelu perustuu useimmiten joko LDAP- (Lightweight Directory Access Protocol), HTTP- tai FTP-protokollaan (File Transfer Protocol). Tuki yhteydettömille tietoyhteyksille ja viiveiden sietokyky on toteutettu WAP-protokollan muilla kerroksilla. [NIC02] [WAP01b]

WTLS sisältää kolme eri turvallisuusluokkaa. Turvallisuusluokat eroavat toisistaan tunnistusmenetelmiensä johdosta. Luokkien käytöllä pyritään helpottamaan langattomien päätelaitteiden suorituskykyvaatimuksia.

WTLS luokka 1

WTLS luokka 1 tarjoaa suojatun tietoyhteyden asiakkaan ja palvelimen välillä. Luokassa 1 ei kuitenkaan käytetä varmenteita osapuolten tunnistamiseen. Luokka sopii käyttökohteisiin, joissa siirrettävä tieto pitää pysyä salassa, mutta kommunikoivien osapuolten tunnistaminen ei ole olennaista. [WAP01b]

WTLS luokka 2

WTLS luokassa 2 käytetään varmenteita palvelimien tunnistamiseen. Luokkaa voidaan käyttää sovelluksissa, joissa käyttäjä haluaa varmistua palvelimen oikeellisuudesta, mutta asiakkaan tunnistaminen ei ole oleellista. Jos asiakas halutaan tunnistaa, voidaan lisänä käyttää ulkopuolisia tunnistusmenetelmiä, kuten salasanakyselyjä. [WAP01b]

WTLS luokka 3

WTLS luokassa 3 käytetään varmenteita myös asiakkaan tunnistamiseen. Tällöin asiakkaalla tulee olla päätelaitteessaan salainen avain ja sitä vastaava varmenne. Varmenteen sijasta päätelaitteessa voidaan säilyttää varmennehakemiston URL:ia, josta asiakkaan varmenne on saatavissa. [WAP01b]

3.4 Tunnistus ja tietoyhteyden suojaus lähimaksujärjestelmässä

Lähimaksujärjestelmässä käyttäjän tunnistamista rajoittavat maksuvälineen syöttölaitteistot. Perinteisin menetelmä on käyttää salasanoja, mutta mikäli päätelaitteessa on mahdollisuus biometristen tunnistusmenetelmien käyttöön, voidaan niitä hyödyntää osana käyttäjän tunnistusta. Uusimmissa kämmentietokoneissa ja älypuhelimissa on jo integroituna sormenjäljenlukijoita ja puheohjaustoimintoja.

Laitteiden tunnistamiseen voidaan käyttää laiteosoitteita, mikäli käytetyt tekniikat tarjoavat siihen mahdollisuuden. Menetelmä ei kuitenkaan yksistään ole riittävä korkeaa tietoturvaa vaativassa lähimaksujärjestelmässä. Kertakäyttöiset salasanat eivät huonon käytettävyytensä puolesta sovi nopeaan lähimaksamiseen, ellei salasanoja luotaisi henkilökohtaisen poletin avulla. Erillisten polettien mukana kantaminen ei kuitenkaan palvele tarkoitusta, jossa pyritään vähentämään mukana kannettavia laitteita. Yksi vaihtoehto olisi se, että maksuväline itse muodostaisi etukäteen annetun tiedon perusteella kertakäyttöisen salasanan.

Varmenteiden avulla voidaan sekä tunnistaa laitteet että suojata tietoyhteys. Varmenteiden käyttö on lisäksi nopeaa ja niihin voidaan laajennusten avulla sisällyttää henkilökohtaista tietoa. Laajennusten avulla voidaan myös soveltaa laitteiden osoitetunnistusta. Varmenteiden lisäksi voidaan käyttää haaste-vastausta, jonka avulla varmistutaan varmenteen haltijasta.

Koska lähimaksujärjestelmässä välitettävät viestit ovat pienikokoisia, ei niiden salaaminen epäsymmetrisillä salausmenetelmillä aiheuta merkittäviä viiveitä. Toinen vaihtoehto olisi käyttää jokaisen yhteyden salaamiseen erillistä symmetristä yhteysavainta. Yhteysavaimen luominen ja välittäminen vaatisivat kuitenkin laitteistoilta suoritustehoa ja voisivat siten jopa hidastaa maksutapahtumia.

4 Langaton päätelaite maksuvälineenä

Langattomassa maksujärjestelmässä maksuvälineenä käytetään langatonta päätelaitetta. Tällöin maksuväline muodostuu itse laitteesta ja sen sisältämästä maksuohjelmistosta. Viimeiset vaiheet lähimaksujärjestelmän suunnittelemisessa ovat oikeanlaisen maksuvälineen ja tiedonsiirtotekniikan valinta.

GSM-tekniikan myötä matkapuhelinta alettiin käyttää pienten palveluiden maksamiseen. Nämä palvelut olivat aluksi matkapuhelimessa hyödynnettäviä palveluita, kuten taustakuvien ja soittoäänien lataamista, mutta sittemmin myös monien ulkoisten palveluiden ostaminen on mahdollistettu matkapuhelimen avulla. Matkapuhelimen lisäksi markkinoilla on nykyään muitakin langattomia päätelaitteita, ja niitä varten tuotetaan jatkuvasti uusia palveluita. Kaikkien näiden palveluiden turvallinen hankkiminen ja käyttö asettavat langattomille päätelaitteille vaatimuksia.

4.1 Langattomat päätelaitteet

Maksuvälineeksi soveltuvia langattomia päätelaitteita on useita, vaikka niitä ei voidakaan pitää perusvarustelultaan riittävän luotettavina maksuvälineinä. Laitteiden tietoturvaa voidaan kuitenkin parantaa ulkoisilla menetelmillä, ja toisaalta pienemmän riskin sovelluksissa myös alhaisempi tietoturvan taso on hyväksyttävää. Tähän mennessä lähimaksujärjestelmässä on valittu käytettäväksi etukäteen maksettuja tilejä, epäsymmetrisiä salaustoimintoja, varmenteita ja haaste-vastausta. Kaikki nämä asettavat vaatimuksia myös maksuvälineelle.

4.1.1 Päätelaitteet

Langattomia päätelaitteita ovat *matkapuhelin*, *älypuhelin*, *kämmentietokone* (PDA, Personal Digital Assistant) ja *kannettava tietokone*. Jokaisella näistä päätelaitteista on ominaispiirteitä, jotka vaikuttavat niiden käytettävyyteen ja turvallisuuteen maksuvälineenä. Lähimaksujärjestelmässä ostotapahtuman ja maksusuorituksen on oltava

nopeita ja käteviä suorittaa. Toisaalta maksuvälineen pitää olla myös turvallinen. Maksuvälineen valinnassa tarkastellaan päätelaitteiden seuraavia ominaisuuksia [SCH02]:

- laitteen koko
- näytön koko
- I/O-laitteisto
- valmiusaika
- muistin määrä ja suorittimen teho
- käyttöjärjestelmän ominaisuudet
- toimikortin lukijalaitteen saatavuus

Laitteen koko ja valmiusaika vaikuttavat sen kannettavuuteen ja valmiustilaan. Lähiympäristön maksuvälineen pitää olla nopea käyttää, joten sen valmiustilaan saattaminenkaan ei saa kestää liian kauan. Sopiva näytön koko ja syöttölaitteisto mahdollistavat kaiken oleellisen informaation esittämisen käyttäjälle selkeästi, siten että käyttäjä voi antaa komentoja varmistuen niiden oikeellisuudesta.

Riittävä muistin määrä ja suorittimen teho mahdollistavat kehittyneempien salaustoimintojen käyttämisen. Myös käyttöjärjestelmän ominaisuudet vaikuttavat salaustoimintojen toteuttamismahdollisuuksiin. Toimikorttia puolestaan on yleisesti käytetty maksuvälineenä tai sen osana salaisen tiedon säilyttämiseen [RAD00]. Kortin lukijalaitteen saatavuus tuo lisämahdollisuuksia maksuvälineen toteuttamiseksi.

Matkapuhelin

Matkapuhelimen käyttöä maksuvälineenä puoltaa muita laitteita pidempi valmiusaika sekä sen pieni koko. Uusissa malleissa on myös värinäytöt, joskin niiden koko on edelleen melko pieni kehittyneen käyttöliittymän toteuttamiseksi ja käyttämiseksi. Matkapuhelimien näppäimistö on riittävä yksinkertaisiin maksusovelluksiin, joissa tarvitsee ainoastaan hyväksyä toimintoja nappia painamalla. Muistin määrä ja suorittimen teho ovat matkapuhelimessa kuitenkin hyvin rajalliset.

Toimikortin lukijalaite on GSM-matkapuhelimessa perusvarustus SIM-kortin vuoksi. Ongelmana on se, että matkapuhelimissa on ainoastaan yksi korttipaikka. Ratkaisuna on SIM-kortista ja tietoturvaominaisuuksilla varustetusta WIM-kortista (Wireless Identity Module) koostuva yhdistelmäkortti, SWIM-kortti (Subscriber Wireless Identity Module). Suomessa tällaisia kortteja on tarkoitus ottaa käyttöön vuoden 2004 aikana [MUU03].

Toinen vaihtoehto on käyttää matkapuhelimissa kahta korttipaikkaa (engl. Dual slot), mitä matkapuhelinten valmistajat ovat kuitenkin olleet haluttomia toteuttamaan. Erillisiä kaksoiskortinlukijalaitteita on saatavilla, mutta niiden käytettävyys on toistaiseksi huonoa.

Älypuhelin

Älypuhelimella on kokonsa ja valmiusaikansa puolesta samat mahdollisuudet maksuvälineeksi kuin matkapuhelimellakin. Myös toimikortin käytön mahdollisuudet ovat samanlaiset kuin matkapuhelimissa.

Älypuhelin tarjoaa matkapuhelimeen verrattuna monipuolisemmat syöttölaitteet mahdollisten kosketusnäyttöjen ja ohjauskynien ansiosta. Lisäksi matkapuhelinten näyttöjä suuremmat näytöt mahdollistavat monipuolisempien käyttöliittymien kehittämisen. Älypuhelimien käyttöjärjestelmät ovat myös huomattavasti matkapuhelimia kehittyneempiä, ja niiden muistin määrä sekä suoritinteho mahdollistavat tavallisimpien apuohjelmien käytön.

Jatkuvasti kehitettäviä älypuhelinten käyttöjärjestelmiä edustavat Symbian OS (http://www.symbian.org), Palm OS (http://www.palmsource.com), Linux OS ja Microsoft Pocket PC OS (http://www.microsoft.com/windowsmobile). Älypuhelinten käyttöjärjestelmien kehitysalustat ja niiden ohjelmointirajapinnat (API, Application Programming Interface) tarjonnevat jatkossa myös kattavampia salauskirjastoja tietoturvan parantamiseksi. Näiden menetelmien ansiosta älypuhelimet ovat erittäin potentiaalisia laitteita maksuvälineiksi.

Kämmentietokone

Kämmentietokoneet ovat yleistyneet viime vuosien aikana erityisesti kehittyneiden kalenteri- ja muistiinpanotoimintojen sekä kommunikointiominaisuuksiensa ansiosta. Niiden näytöt ovat huomattavasti suurempia kuin matkapuhelimien näytöt, ja ne mahdollistavat siten monipuolisempien käyttöliittymien kehittämisen ja käytön. Kämmentietokoneet ovat kooltaan hieman suurempia kuin älypuhelimet, mutta ne ovat kuitenkin tarkoitettu mukana kannettaviksi, aina käyttövalmiiksi apuvälineiksi.

Kämmentietokoneiden käyttöjärjestelmät ovat kehittyneitä, ja muistia sekä suoritintehoa on huomattavasti enemmän kuin älypuhelimissa. Omien salaustoimintojen kehittäminen on mahdollista salauskirjastojen avulla. Useimpia nykyisiä kämmentietokoneita on

mahdollista laajentaa PCMCIA-korttien tai SD-laajennuspaikan (Secure Digital) avulla. Valmiusaika on huomattavasti matkapuhelimien valmiusaikoja lyhyempi, mutta selvästi pidempi kuin kannettavilla tietokoneilla.

Kannettava tietokone

Kannettavalla tietokoneella on tarkasteltavista laitteista paras suorituskyky. Koko kuitenkin rajoittaa merkittävästi sen käyttöä maksuvälineenä: vaikka kannettavaa tietokonetta kannettaisiinkin mukana, ei sitä voida pitää jatkuvasti käyttövalmiina lyhyiden valmiusaikojen takia.

4.1.2 Päätelaitteiden vertailua

Langattomien päätelaitteiden vertailun tulokset käyvät ilmi taulukosta (1), jossa esiintyvät arvot on poimittu päätelaite- sekä käyttöjärjestelmävalmistajien kotisivuilta [HEW03] [NOK03b] [SAM04] [PAL04] [APP04]. Vertailun perusteella voidaan todeta, että kämmentietokone ja älypuhelin soveltuvat parhaiten luotettaviksi maksuvälineiksi. Kannettavan tietokoneen koko on merkittävä este sen sujuvalle käytölle nopeassa automaattimaksamisessa. Matkapuhelimen käytön esteenä on puolestaan sen rajoittunut suorituskyky ja puutteelliset tietoturvaominaisuudet.

Taulukko 1. Langattomien päätelaitteiden vertailu

	Matkapuhelin	**Älypuhelin**	**PDA**	**Kannettava tietokone**
paino (g)	<100	>100	>200	>2000
mitat (mm)	~100x40x20	~110x55x25	~135x80x20	~300x270x40
valmiusaika (h)	>300	>100	<15	<5
näytön koko	pieni	pieni	~4”	~14”
muisti (Mb)	~n Kt	~4	~128	~1024
suoritin	pieni	pieni	~400MHz	~2,5GHz
käyttöjärjestelmä	valmistaja-kohtainen	Symbian, Palm, Linux, Pocket PC	Palm, Linux, Pocket PC,	Windows, Linux, Macintosh
toimikorttipaikka	kyllä	kyllä	laajennus	laajennus
hinta	<200€	<500€	>500€	>1000€

Lopullinen valinta älypuhelimen ja kämmentietokoneen välillä voidaan tehdä vaaditun tietoturvatason mukaisesti. Tässä työssä maksumenetelmäksi on valittu etukäteen maksetut tilit, joiden turvallinen käyttäminen vaatii korkeaa tietoturvatasoa, sekä suorituskykyä salaustoimintojen ja osapuolten tunnistuksen suorittamiseksi.

4.2 Tiedonsiirto-ominaisuudet

Maksujärjestelmä ympäristöineen asettaa vaatimuksia maksuvälineissä käytettävälle tiedonsiirtotekniikalle. Tässä työssä suunniteltavassa järjestelmässä voidaan maksuvälineellä paitsi maksaa ostoksia myös tehdä tilikyselyjä ja vastaanottaa mainoksia. Seuraavassa on esitetty järjestelmän vaatimuksia käytettävälle tiedonsiirtotekniikalle.

4.2.1 Vaatimuksia tiedonsiirtotekniikalle

Lähimaksujärjestelmässä siirrettävät tietopaketit ovat usein melko pienikokoisia, eikä niiden siirtäminen laitteiden välillä siten vaadi suuria **tiedonsiirtonopeuksia**. Maksutapahtuman kokonaiskesto sen sijaan täytyy olla mahdollisimman lyhyt, jotta järjestelmän käytettävyys säilyisi. Tästä syystä myös yhteyden alustamiseen kuluvan ajan tulee olla mahdollisimman lyhyt. [VEI02]

Kun lähimaksujärjestelmässä ostetaan fyysisiä tuotteita, tapahtuu maksaminen aina maksupalvelimen välittömässä läheisyydessä: joko automaatin vieressä tai ruokalan kassalla. Siten jopa metrin **kantama** riittää maksamisen suorittamiseksi. Kantaman rajoittamisella voidaan jopa parantaa tietoturvaa, kun tiedetään, että vain tietyn alueen laitteilla on mahdollisuus kommunikoida keskenään.

Tilitietokyselyjen tekeminen ja mainosten vastaanottaminen on puolestaan käytännöllisempää suorittaa silloin, kun niiden suorituspaikkaa ei ole tiukasti rajattu. Koko rakennuksen kattavat kantamat ovat tällöin suositeltavia. Lyhyen kantaman tekniikkaa käytettäessä voidaan kattaa laajempia alueita myös hyvällä tiedonsiirtoverkon suunnittelulla. [JÄP01a]

Koska automaatti- ja ruokalaostokset ovat usein melko pieniä, tiedonsiirtotekniikan **käyttömaksu** tulee pyrkiä minimoimaan. Jotta järjestelmän käyttäminen olisi sekä asiakkaalle että kauppiaalle kannattavaa, tulisi tiedonsiirtoverkon olla maksuton.

Koska maksuväline on henkilökohtainen, pitää se olla **tunnistettavissa** jollakin tavalla. Olisi hyvä, jos käytettävä tiedonsiirtotekniikka tarjoaisi menetelmän laitteiden tunnistamiseen, jota voitaisiin käyttää osana asiakkaan tunnistamista. [WAR97]

Mikäli järjestelmässä halutaan lähettää maksupalvelinkohtaisia mainoksia, ei niitä ole järkevää lähettää kaikille asiakkaille, vaan ainoastaan kyseisten palvelimien lähistöllä oleville asiakkaille. Laitteet pitää pystyä tällöin **paikantamaan**. Kantoalueella olevat laitteet voidaan joissakin tekniikoissa selvittää laitehakujen perusteella. [JÄP01b]

Käytettävän tekniikan tulisi olla **yleisesti käytössä** oleva tekniikka. Mitä useampaan päätelaitteeseen kyseinen tekniikka on toteutettu, sitä paremmat ovat edellytykset järjestelmän käytölle.

Bluetooth-tekniikalla on lähimaksujärjestelmän näkökulmasta sopiva kantomatka, tiedonsiirtonopeus ja valmiiden toteutusten määrä langattomissa päätelaitteissa. Kuuluvuusalueella olevien Bluetooth-laitteiden selvittäminen on myös mahdollista laitehakujen ja laiteosoitteiden avulla.

4.2.2 Bluetooth

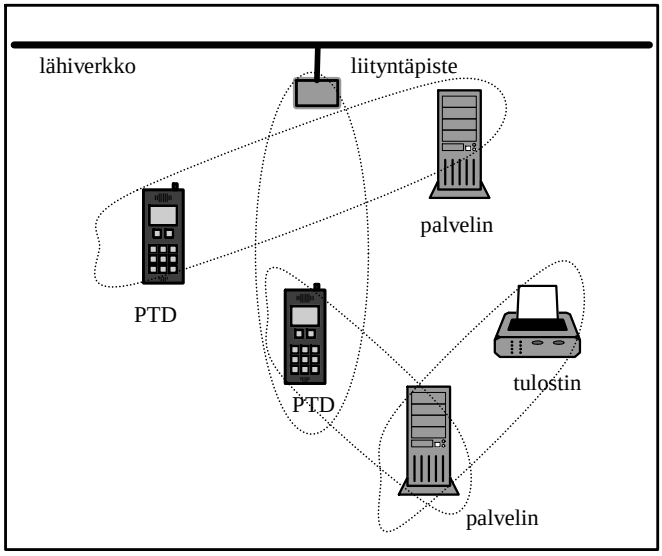
Bluetooth on Bluetooth SIG:n (Special Interest Group) kehittämä lyhyen kantaman radiotekniikka. Bluetooth-tekniikka käyttää maailmanlaajuisesti vapaata 2.4 GHz ISM (Industrial, Scientific, Medical) taajuuskaistaa. Sen maksimitiedonsiirtonopeus on 1Mbps, josta yhdensuuntaisen liikenteen maksiminopeus on 768 kbps.

Bluetooth-lähettimillä on kolme teholuokkaa, jotka vastaavat 1 m, 10 m ja 100 m kantamia. Jokainen Bluetooth-vastaanotin omaa yksilöllisen 48-bittisen IEEE802-standardin (Institute of Electrical and Electronic Engineers) mukaisen laiteosoitteen (BD_ADDR, Bluetooth Device Address), jota käytetään yhteyksien luomiseen. Tätä laiteosoitetta voidaan käyttää lähimaksujärjestelmässä myös laitteiden tunnistamiseen. Laitteiden välistä tiedonsiirtoa on pyritty saamaan luotettavammaksi käyttämällä taajuushyppelyä, joka suoritetaan pikoverkon isäntälaitteen kellon mukaisesti. [BLU01]

Verkkoarkkitehtuuri

Bluetooth-verkot koostuvat isäntä- ja orjalaitteista. Isäntälaite aloittaa yhteydenmuodostuksen orjalaitteelle. Rooleja voidaan vaihtaa yhteyden muodostuksen

jälkeen. Samalla isäntälaitteella voi olla aktiivinen yhteys seitsemään eri orjalaitteeseen ja lisäksi useampaan *park*-tilassa olevaan orjalaitteeseen, jotka ainoastaan seuraavat sivusta tiedonsiirtokanavan taajuushyppelykuviota. Näin muodostunutta verkkoa kutsutaan pikoverkoksi (engl. Piconet).



Kuva 11. Pikoverkko ja hajaverkko

Yksi Bluetooth-laite voi olla isäntänä vain yhdessä pikoverkossa, mutta se voi olla orjana useammassakin pikoverkossa samanaikaisesti. Jos eri pikoverkoilla on yhteisiä laitteita, muodostavat ne yhdessä hajaverkon (engl. Scatternet) (kuva 11). Lähimaksujärjestelmässä käytetään perinteisiä kahdenvälisiä asiakas-palvelin-yhteyksiä, jolloin yhteyden muodostavasta laitteesta tulee isäntälaite ja vastapuolesta orjalaite. Bluetoothin yhteydenmuodostus on riittävän nopea lähimaksujärjestelmän kannalta ja sen käyttö on ilmaista, koska yhteyksien luomiseen ei tarvita kaupallisia kolmansia osapuolia. Fyysisellä tasolla Bluetooth tukee kahta erilaista linkkityyppiä laitteiden välillä:

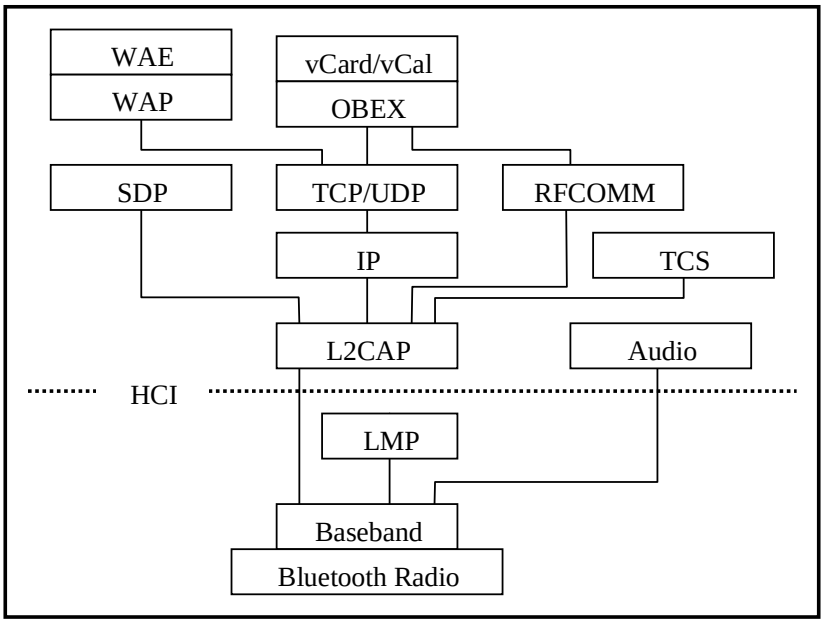
- piirikytkentäinen synkroninen yhteys (SCO, synchronous connection oriented)
- pakettikytkentäinen asynkroninen yhteys (ACL, asynchronous connectionless)

SCO-linkit ovat isännän ja yhden orjan välille muodostettuja point-to-point -linkkejä. SCO-linkkejä käytetään erityisesti aikariippuvaisten palveluiden yhteydessä, kuten äänen siirrossa. ACL-linkit ovat point-to-multipoint -linkkejä isännän ja saman pikoverkon sisällä olevien orjalaitteiden välillä. ACL-linkkejä käytetään uudelleen lähetystä

käyttävien palveluiden yhteydessä varmistamaan siirrettävän tiedon yhtenäisyys. ACL-linkit tarjoavat riittävän luotettavan ja nopean tiedonsiirron lähimaksujärjestelmän viestiliikenteelle. [BLU01]

Protokollapino

Jokaisen Bluetooth-laitteen pitää toteuttaa neljä Bluetooth-protokolla-arkkitehtuurin perusprotokollaa. Nämä ovat Baseband, LMP (Link Manager Protocol), L2CAP (Logical Link Control and Adaptation Protocol) ja SDP (Service Discovery Protocol) (kuva 12). Baseband ja LMP-protokollat sijaitsevat käyttäjäriippumattoman laiterajapinnan (HCI, Host Control Interface) alapuolella ja ne ovat usein laitteistolla toteutettuja. Niiden toiminnallisuutta ohjataan laiterajapinnan läpi laitteen ohjelmistoilla. L2CAP ja SDP ovat Bluetooth-laitteessa ajettavia ohjelmia, jotka optimoivat kaikkien Bluetooth-laitteiden yhteensopivuuden.



Kuva 12. Bluetooth-protokollapino

L2CAP

L2CAP sijaitsee HCI-rajapinnan yläpuolella mukauttaen korkeamman tason protokollia alemman tason protokollien päälle. L2CAP huolehtii yhteyden hallinnasta LMP:n kanssa. Lisäksi L2CAP tarjoaa protokollan kanavoinnin sekä ylempien kerrosten tietopakettien segmentoinnin ja yhteen liittämisen. L2CAP-protokolla tarjoaa kattavan

ohjelmointirajapinnan, jonka avulla voidaan toteuttaa sen päällä toimiva lähimaksuprotokolla. Lähimaksuprotokolla mahdollistaa koko järjestelmän viestiliikenteen toteuttamisen.

SDP

SDP tarjoaa menetelmän, jonka avulla ohjelmat voivat selvittää saatavilla olevat palvelut ja niiden ominaisuudet muissa Bluetooth-laitteissa. SDP ei kuitenkaan tarjoa menetelmää palveluiden käyttämiseksi, vaan sitä varten joudutaan käyttämään muita protokollia. Lähimaksujärjestelmässä voidaan käyttää SDP-kyselyjä kauppiaiden laitteiden selvittämiseksi, minkä jälkeen palvelun käyttäminen tapahtuu L2CAP-protokollan päälle rakennetun lähimaksuprotokollan avulla. [BLU01]

4.3 Henkilökohtainen luotettava päätelaite

Kun ongelman ratkaisemiseksi on valittu käytettävät tekniikat ja välineet, on selvitettävä miten niitä voidaan käyttää hyväksi ja minkälaisia turvallisuusriskejä on edelleen olemassa. Koska työn tavoitteena on saada aikaan luotettava ja turvallinen lähimaksujärjestelmä, pitää myös maksuvälineen olla luotettava. *Henkilökohtainen luotettava päätelaite* (PTD, Personal Trusted Device) on MeTin tekemä määritelmä, jonka mukaan langattomalla päätelaitteella voidaan tietyin edellytyksin käyttää turvallisesti pankkitoimintoja, maksamista, lippujen hallintaa ja muita käyttöoikeuksiin perustuvia sovelluksia [MET02b].

Henkilökohtainen luotettava päätelaite sisältää erityisen *tietoturvaelementin* (SE, Security Element), jonka avulla suoritetaan salaustoiminnot ja jossa säilytetään käyttäjän henkilökohtaista tietoa. Palveluita käytetään järjestelmäkohtaisella maksuohjelmalla, joka myös tunnistaa käyttäjän. Henkilökohtaisen luotettavan päätelaitteen käytössä ja käyttökuntoon saattamisessa voidaan erotella rajapintoja, joille tietoturvariskit voidaan kohdistaa.

4.3.1 Tietoturvaelementti

Tietoturvaelementti suorittaa kaikki tiedon salaamiseen ja osapuolten tunnistukseen liittyvät toiminnot sekä toimii salaisten tietojen tallennuspaikkana. Tällaisia salaisia tietoja

ovat muun muassa salausavaimet, salasanat ja varmenteet. Tietoturvaelementti on mahdollista toteuttaa usealla eri tavalla päätelaitteessa. Vaihtoehtoina ovat laitteisto, ohjelma tai niiden yhdistelmänä toteutettu tietoturvaelementti. Myös toimikorttia käytetään yleisesti tietoturvaelementtinä [MET02c].

Tietoturvaelementti voi olla kiinteä tai irrallinen. Tämä seikka vaikuttaa tietoturvaelementin alustamiseen ja toimittamiseen. Toimikortti on esimerkki irrallisesta tietoturvaelementistä, kun taas sulautettu laitemoduuli sekä ohjelmallisesti toteutettu tietoturvaelementti ovat kiinteitä ratkaisuja. [MET02b]

PIN-koodit

PIN-koodit ovat numeroista koostuvia salasanoja, joita käytetään käyttäjän tunnistamiseen ja salausavainten käyttöoikeuksien hallintaan. Jokaiselle salausavaimelle määritetään oma PIN-koodi, joka käyttäjän pitää tietää salausavainta käytettäessä. [SMI01]

PIN-koodien määrittäminen ja jakelu asiakkaalle voivat olla ongelmallisia. Jos käyttäjä on läsnä salausavaimia luotaessa, voi hän itse määrittää PIN-koodin salausavaimelle. Muutoin PIN-koodien toimittaminen käyttäjälle pitää hoitaa turvallisella tavalla. [MEN96].

Varmenteet

Luotettavan tahon myöntämät varmenteet säilytetään tietoturvaelementissä, samoin kuin varmentajien varmenteetkin, joiden avulla voidaan tarkastaa muiden tahojen varmenteiden oikeellisuus. Omia varmenteita käytetään salaustoimintoihin sekä henkilöllisyyden todistamiseen.[HÄM02]

Salausavaimet

Salausavainten luominen ja turvallinen säilyttäminen ovat tietoturvaelementin keskeisiä tehtäviä. Salausavainten pituudet vaikuttavat salauksen vahvuuteen ja salaukseen kuluvaan aikaan. Mitä pidempi avain sitä vahvempi, mutta toisaalta myös hitaampi salaus. Pituus vaikuttaa myös avainten käyttöaikaan: käyttöajan tulisi aina olla suoraan verrannollinen avainten pituuteen. Käyttöajat voidaan määrittää muun muassa niiden varmenteiden voimassaoloajoilla. [ELL00]

Salausavainten luominen

Salausavainten luomiseen kuuluu käytettävän salausalgoritmin valinta ja salausavainten pituuksien määrittäminen. Olennaista on saada luotua satunnainen avain, jossa ei esiinny toisistaan riippuvia bittejä tai bittisarjoja. Näin ollen avaimen murtamiseksi voidaan käyttää ainoastaan voimakeinoja, kuten eri avaimien kokeilemista järjestelmällisesti. Avaimen tulee olla niin pitkä, ettei avainta ole mahdollista saada selville järkevässä ajassa [SMI01].

Mikäli salausavaimet luodaan tietoturvaelementin ulkopuolella, pitää ne toimittaa turvallisesti tietoturvaelementille. Sen toteutuksesta riippuen salausavaimet voidaan toteuttaa myös elementin sisällä. Julkisen avaimen järjestelmässä salaisen avaimen tarvitsee olla ainoastaan tietoturvaelementin muistissa. Symmetrisen avaimen järjestelmissä salainen avain on saatettava myös vastapuolen tietoon [WAR97].

Salausavainten säilytys

Salausavainten pituuden ohella myös säilytysalustan turvallisuus vaikuttaa avainten käyttöaikaan. Turvallinen säilytysalusta ei kuitenkaan lisää käyttöaikaa, vaan mahdollistaa avaimen pituuteen verrannollisen käyttöajan.

Säilytysalustan tulee olla sekä fyysisesti että ohjelmallisesti suojattu. Olettaen, että säilytysalustaa ei voida aina pitää fyysisesti suojassa, pitää sen myös kestää fyysisiä hyökkäyksiä eli peukalointia. Toisaalta henkilökohtaisen päätelaitteen kadottaminen yleensä huomataan nopeasti, jolloin voidaan olettaa, ettei sen tietoturvaelementtiä pääse peukaloimaan huomaamattomasti. [SCH99]

Mitä enemmän avainta käytetään, sitä mahdollisempaa sen selvittäminen on. Avaimen toimintaa tarkasteltaessa voidaan pystyä päättelemään siinä esiintyviä bittejä. Siksi eri toimintoja varten on suositeltavaa luoda omat avaimet. Julkisen avaimen järjestelmässä suositellaan eri avainten käyttöä digitaaliseen allekirjoittamiseen ja salaamiseen [MEN96].

Salausavainten elinkaaren hallinta

Salausavaimen elinkaaren hallintaan kuuluu avaimen luomisprosessi pituuden määrityksineen, avaimen jakeluprosessi sekä avaimen säilytys. Tämän lisäksi elinkaaren hallintaan kuuluu myös varmentamispolitiikka, varmenteiden säilyttäminen ja

peruutuslistojen käyttö. Kaikkien näiden osien toiminnan arvioinnin pohjalta voidaan määrittää avainten voimassaoloajat [MEN96].

Tietoturvaelementin hallinta

Joissakin tapauksissa kaikki tietoturvaelementin sisältämä tieto voidaan tuhota, jos havaitaan väärinkäyttöyritys esimerkiksi liian monen virheellisen salasanan antamisen jälkeen. Menetelmän käytettävyyttä parantaa varmuuskopioiden ylläpitäminen ulkoisella tallennusmedialla [VEI03].

Päätelaite ja tietoturvaelementti pitää olla lukittavissa myös järjestelmän ylläpitäjän toimesta väärinkäytösten estämiseksi. Julkisen avaimen järjestelmissä tämä on mahdollistettu salausavaimille myönnettyjen varmenteiden peruutustoiminnolla.

4.3.2 Toimikortti tietoturvaelementtinä

Toimikortin (ICC, Integrated Circuit Card, Smart Card) käyttö tietoturvaelementtinä perustuu sen kolmeen perusominaisuuteen: peukaloinnin sietävään rakenteeseen, pieneen kokoon ja sisäiseen laskentakapasiteettiin sekä muistiin. Tässä kappaleessa tarkastelemme toimikorttien soveltumista maksujärjestelmään sekä niiden tuomia mahdollisuuksia ja ongelmia. [RSA99b]

Mahdollisuudet

Toimikortin sisäinen laskentakapasiteetti ja muisti muodostavat toimikortista erillisen mikropiirille toteutetun laskentayksikön. Toimikortilla on oma suoritin, joka suorittaa kortin ROM-muistissa (Read Only Memory) tai haihtumattomassa RAM-muistissa (Read Access Memory) sijaitsevaa ohjelmaa. Toimikortin ja ulkomaailman välinen tiedonsiirto on sarjamuotoista. Se on mahdollista suorittaa sähkömagneettisen induktion avulla kontaktittomissa korteissa tai toimikortin kontaktipintojen välityksellä kontaktillisissa korteissa. [RAD00]

Toimikortin peukaloinninsietokyky on sen tärkeimpiä ominaisuuksia tietoturvan kannalta. Toimikortin rakenne suojaa sen sisältämiä tietoja tehokkaasti ulkopuoliselta hyökkäykseltä. Toimikortin sisältämään tietoon pääsee käsiksi ainoastaan käyttäjän

todentamisen jälkeen. Todentaminen voi tapahtua esimerkiksi PIN-koodin tai sormenjäljen avulla.

Toimikorttien haihtumattomien EEPROM-muistien (Electrically Erasable Programmable Read Only Memory) kapasiteetti on nykyään 16, 32 tai 64 kilotavua. Tämän lisäksi toimikorteilla on ROM-muistia 6-24 kilotavua ja muutamia satoja tavuja tai kilotavuja RAM-muistia. Suorittimet käyttävät RAM-muistia lähinnä laskutoimituksien välituloksien tallennuspaikkana. Suorittimet ovat tavallisesti 8- tai 16-bittisiä. [MIO04]

Toimikortin muistissa voidaan säilyttää henkilökohtaisia salaisia tietoja, kuten salausavaimia ja varmenteita. PKI-toimikorteissa on erillinen salaussuoritin, joka huolehtii salaus- ja allekirjoitustoiminnoista. Suomessa tunnetuin PKI-toimikorttisovellus on HST-kortti. Sen muistiin on tallennettu väestörekisterikeskuksen myöntämä varmenne sekä salausavaimelle että allekirjoitusavaimelle, ja itse avaimet. Väestörekisterikeskuksen varmenteita voi vuodesta 2004 lähtien liittää myös joihinkin pankkikortteihin ja matkapuhelinliittymien SIM-kortteihin. HST-kortin salausavainten käyttöaika on nykyisin 5 vuotta. [POP03][MUU03]

Ongelmat

Merkittävä este toimikortin käytölle tietoturvaelementtinä on sen vaatima kortinlukulaitteisto. Matkapuhelimissa on ainoastaan yksi korttipaikka, joka on varattu SIM-kortille. Matkapuhelinoperaattorien ja varmenneviranomaisten yhteistyö onkin tärkeä seikka tietoturvaelementin toteutuksen kannalta. Kämmentietokoneiden tapauksessa toimikorttia voidaan lukea PCMCIA-kortinlukijalaitteen avulla, joka useimmissa tapauksissa hieman kasvattaa päätelaitteen kokoa ja hintaa.

Toimikortin varkaus- ja katoamistapauksissa ulkopuolinen taho voi hyökätä kortin tietoja vastaan peukalointiyrityksillä. Ne voidaan jaotella neljään ryhmään: *anturointi*, *ohjelmistohyökkäykset*, *signaalien kuuntelu* ja *virheiden generointi*. [KÖM99]

Anturoinnilla tarkoitetaan hyökkäystä, joka suoritetaan erikoistyökalujen avulla laboratorioympäristössä ja jossa kortin sirua manipuloidaan fyysisesti. Sirun arkkitehtuuria voidaan päästä tutkimaan mikroskoopilla ja väylien signaaleja mitata ja muuttaa mikroantureilla. Anturoinnin mahdollistavat erikoislaitteistot ovat kalliita ja uhka pienemmissä sovelluksissa on siten lähes olematon.

Ohjelmistohyökkäykset ovat hyökkäyksiä, jotka eivät vahingoita sirua. Niillä pyritään löytämään toimikorttia käyttävistä protokollista ja salausalgoritmeista heikkouksia, jotka avaavat hyökkääjälle pääsyn kortin sisältämiin tietoihin.

Signaalien kuuntelun avulla tarkastellaan muun muassa toimikortin kontaktipintojen signaalien analogisia ominaisuuksia. Toimikortin virrankulutuksesta ja sen vaihteluista voidaan tietyissä olosuhteissa tehdä johtopäätöksiä kortin sisäisestä rakenteesta ja sen toiminnasta. Myös signaalien kuuntelu vaatii erikoislaitteistoa.

Virheiden generoinnissa pyritään virhetilanteita tuottamalla saamaan selville kortin sisältöä. Virheitä voidaan generoida esimerkiksi muuttamalla kontaktipintojen signaaleja nopeaan tahtiin.

Tehokkaimmat hyökkäykset saadaan aikaan yhdistelemällä edellä mainittuja hyökkäysyrityksiä. Koska toimikorttia säilytetään päätelaitteessa, on kortinhaltija yleensä tietoinen korttiin kohdistuvista väärinkäytöksistä. Korttiin voi tällöin kohdistua vain päätelaitteen ohjelmiston hyökkäysyritys tai kortinomistajan oma hyökkäysyritys. Jos kortin tiedolla ei itsessään ole taloudellista arvoa, jota muuttamalla kortin haltija voisi hyötyä, jäävät jäljelle ainoastaan ohjelmistohyökkäykset. [KÖM99]

4.3.3 Maksuohjelma

Maksuohjelman avulla suoritetaan maksaminen sekä kuittien, lippujen ja mainosten vastaanotto ja hallinta. Maksuohjelmasta käytetään toisinaan nimitystä lompakko-ohjelma, mikä kuvastaa sen toimintoja: maksuohjelmalla suoritetaan kaikki vastaavat toiminnot kuin fyysisellä lompakollakin. Maksuohjelma toimii käyttäjän rajapintana tietoturvaelementtiin ja koko järjestelmään.

Maksuohjelman avulla säilytetään lompakon tavoin myös henkilökohtaista tietoa. Varmenteet ovat verrattavissa luotettavan tahon myöntämiin henkilöllisyystodistuksiin. Maksuohjelma säilyttää myös maksamisessa hyödynnettäviä salaisia tietoja, kuten pankkikorttien tietoja, tilinumeroita ja salasanoja. Se tunnistaa käyttäjän sovellusta käynnistettäessä.

Jotta maksuohjelman avulla voidaan vakuuttaa käyttäjälle sovelluksen käytön turvallisuus ja luotettavuus, on maksuohjelman käyttöliittymän tarjottava riittävästi informaatiota

jokaisessa tilanteessa. Käyttäjä tekee päätöksensä käyttöliittymän informaation mukaisesti ja antaa käskyjä maksuohjelmalle käyttöliittymän nappien avulla.

Nokia Wallet

Lompakko (engl. Wallet) on Nokian matkapuhelimissa käytettävä ohjelma [NOK03a], jonka avulla käyttäjät voivat tallettaa henkilökohtaisia tietoja matkapuhelimeen. Näitä tietoja voidaan käyttää kaupankäynnissä lomakekenttien automaattiseen täyttämiseen. Lompakon sisältämä tieto on suojattu erillisellä PIN-koodilla, jonka avulla lompakko-ohjelma tunnistaa käyttäjän. Lompakon tehtävänä on yksinkertaistaa aikaavievien maksutoimintojen suorittamista. Nokian Walletia käytetään erityisesti etämaksamisessa, jossa usein joudutaan käyttämään valikkopohjaisia käyttöliittymiä.

Nokia Wallet 2.0 tarjoaa viisi eri moduulia henkilökohtaisten tietojen hallintaan. **Korttimoduulia** käytetään *maksukorttien* ja *kanta-asiakkuuskorttien* tietojen hallinnoimiseen. Myös käyttäjäprofiilin sisältäviä kortteja voidaan sisällyttää moduuliin. Käyttäjätunnuksen ja salasanan sisältävien *valtuuskorttien* luominen on myös mahdollista lompakko-ohjelman avulla.

Korttien tietoja voidaan ottaa vastaan ilmateitse (OTA, Over The Air). Tällöin etukorttien käyttö helpottuu entisestään ja vastaavasti kauppiaan tietoja sisältäviä kortteja voidaan ladata matkapuhelimeen maksutapahtumien helpottamiseksi.

Käyttäjät voivat luoda **lompakkoprofiileita** langattomille palveluille. Profiilien avulla kuvataan mitä kortteja tai tietoja tietyn palvelun hankkimisessa käytetään. Vastaavasti voidaan kuvata myös sähköisten kuittien ja lippujen vastaanottotapa, sekä talletuspaikka. Profiilien käytöllä nopeutetaan maksutapahtumia, joissa vaaditaan useiden erilaisten tietojen syöttämistä.

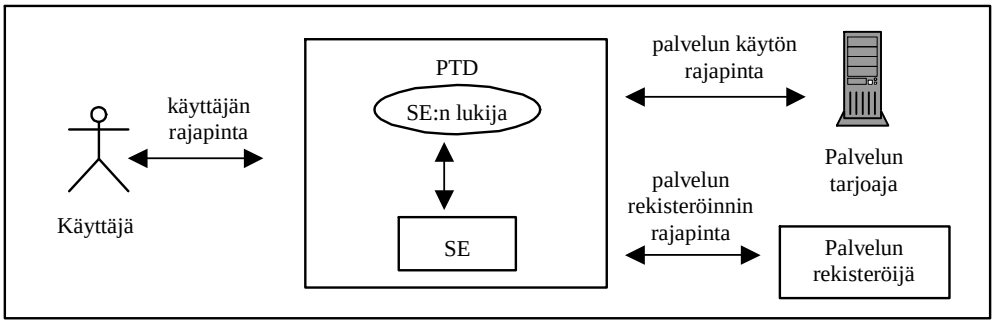
Henkilökohtaisiin muistioihin voidaan tallettaa erilaisia yksityisiä tietoja, jotka halutaan pitää salassa. Tällaisia tietoja voivat olla tilinumerot, maksukorttien numerot, käyttäjätunnukset ja salasanat. Muistioiden tiedot suojataan lompakon PIN-koodilla. Lompakon kopiointitoiminnon avulla tiedot voidaan kopioida esimerkiksi tekstiviestiin tai matkapuhelimen kalenteriin.

Kuittimoduulin avulla hallitaan kuitteja ja lippuja. Nokian lompakossa niiden vastaanotto perustuu RFID-tekniikkaan. Moduuli tarjoaa myös lippujen ja kuittien selaustoiminnon.

Asetustoimintojen avulla käyttäjä voi esimerkiksi vaihtaa lompakon PIN-koodia ja valita, haluaako hän ylipäätään käyttää lompakon PIN-koodi-toimintoa.

4.3.4 Rajapinnat

Maksuvälineen toimintakuntoon saattaminen ja turvallinen käyttäminen tapahtuu tiettyjen rajapintojen kautta. Tietoturvariskit ja menetelmät niiden pienentämiseksi voidaan siten kohdistaa yksittäisille rajapinnoille (kuva 13). Rajapintojen määritykset mukailevat lähdettä [MET02b].



Kuva 13. Henkilökohtaisen luotettavan laitteen rajapinnat

Käyttäjän rajapinta

Käyttäjän rajapinta muodostuu päätelaitteen syöttö- ja tulostuslaitteistosta. Näkyvän osan rajapinnasta muodostavat päätelaitteen näyttö, kosketusnäyttö, näppäimistö, sormenjäljen lukija, kamera, mikrofoni, kaiuttimet ja erilaiset ohjaustyökalut.

Käyttäjän rajapinta käsittää käyttäjän ja päätelaitteen väliset toiminnot. Sen tehtävänä on kuvata käytettävä palvelu siten, että käyttäjä voi aina olla varma, mitä palvelua hän käyttää ja että palvelun käyttö on turvallista. Rajapinnan kautta myös syötetään tietoja päätelaitteelle sekä annetaan käskyjä esimerkiksi nappien painalluksilla. Kaikki tieto maksun onnistumisesta, digitaalisen allekirjoituksen suorittamisesta sekä kuittien ja lippujen selaamisesta esitetään käyttäjälle kyseisen rajapinnan avulla.

Palvelun käytön rajapinta

Palvelun käytön rajapinta kuvaa, miten päätelaite voi käyttää palvelua, kommunikoida maksu-, mainos- tai lompakkopalvelimen kanssa. Suojatun tietoyhteyden luominen

päätelaitteen ja palvelun tuottajan välillä kuuluu rajapinnan tehtäviin. Palvelun tarjoajan identiteetin varmistaminen ja salattuun yhteyteen liittyvien parametrien sopiminen on olennainen osa suojatun tietoyhteyden luomista. Palvelun tarjoaja puolestaan vaatii käyttäjän tai oikeammin sanottuna päätelaitteen tunnistamista.

Maksutapahtuma suoritetaan palvelun käytön rajapinnan kautta. Tuotelistat, laskut, maksuhyväksynnät, kuitit, tilitiedot ja mainokset välitetään palvelun käytön rajapinnan avulla. Siten myös maksamiseen käytettävä tiedonsiirtotekniikka sekä maksuprotokolla ovat osa palvelun käytön rajapintaa.

Palvelun rekisteröinnin rajapinta

Palvelun rekisteröinnin rajapinta kuvaa, miten maksuväline ja sen omistaja rekisteröidään tietyn järjestelmän asiakkaaksi. Rajapinnan kautta tapahtuu maksuohjelmiston lataaminen päätelaitteeseen. Mikäli järjestelmässä käytetään asiakkaan tunnistukseen tai salaustoimenpiteisiin julkisen avaimen järjestelmää, suoritetaan varmenteiden myöntäminen tämän rajapinnan avulla. Mikäli salausavaimia ei ole luotu tietoturvaelementissä, luo palvelun rekisteröijä ne ja siirtää varmentamisen lopuksi päätelaitteeseen rajapinnan avulla.

Käyttäjän varmentamiseksi tarvittavat henkilöllisyystiedot voidaan välittää palvelun rekisteröijälle varmennepyynnön muodossa, mikäli salausavaimet on luotu tietoturvaelementissä. Muutoin henkilöllisyystiedot voidaan antaa kirjallisena. Palvelun rekisteröijä toimittaa käyttäjän varmenteet, sekä oman ja juurivarmentajan varmenteet päätelaitteelle varmennustapahtuman lopuksi.

4.3.5 Uhkakuvia

Mikäli maksuväline katoaa tai tuhoutuu, voidaan sen mukana menettää henkilökohtaista tietoa. Jos maksuväline sisältää salaista tietoa, jonka omaamisella on taloudellista hyötyä, syntyy ilkeämielisille tahoille houkuttimia murtautua maksuvälineeseen. Henkilökohtaisen päätelaitteen yksityiseen tietoon kohdistuvia uhkia voidaan luokitella taulukon (2) mukaisesti [VEI03].

Taulukko 2. Päätelaitteen yksityisyyteen kohdistuvat uhat

Uhka	Riski	Suojautuminen
PTD tuhoutuu	Henkilökohtaisen tiedon menetys	PTD-tiedon minimointi/ hajautus/varmuuskopiot
PTD katoaa	Mahdollinen henkilökohtaisen tiedon väärinkäyttö	Käyttöoikeuksien määritys/PTD:n fyysinen suojaus
PTD varastetaan	Henkilökohtaisen tiedon väärinkäyttö	PTD-tiedon salaus
PTD-tiedon tunnistettu väärinkäyttö	Mahdollinen taloudellinen menetys/järjestelmän toiminnan häirintä	Maksuvälineen peruutus/PTD-tiedon itse-tuhoutuminen
PTD-tiedon tunnistamaton väärinkäyttö	Taloudellinen menetys/järjestelmän toiminnan häirintä	PTD:stä kulkevan tiedon tarkkailu/ tiedonsiirron salaus

Jos päätelaite joutuu vääriin käsiin, voidaan päätelaite lukita ja sen sisältämä tieto tuhota. Jos tiedoista on olemassa varmuuskopiot erillisellä palvelimella, kynnys **tietojen tuhoamiselle** on pienempi. [MET03a]

Päätelaitteen **tietojen kahdentuminen** voi häiritä järjestelmän toimintaa ja joissain tapauksissa jopa murtaa koko järjestelmän. Kriittisten tietojen, kuten kuittien, kahdentuminen tulisi estää esimerkiksi käyttämällä digitaalista allekirjoitusta ja aikaleimoja. Myös tietojen personointi pienentää niiden kahdentumisesta aiheutuvia riskejä. Esimerkki tällaisesta on maksuvälineen laiteosoitteen sisällyttäminen allekirjoitettuun kuittiin (kpl 5.1).

Käyttöoikeuksien avulla määritetään, mitä kullakin käyttäjällä on lupa tehdä järjestelmässä. Oikeiden käyttöoikeuksien luovuttamiseksi käyttäjä pitää tunnistaa. Sen avulla varmistutaan, kuka päätelaitetta milloinkin käyttää ja kenen hallussa päätelaite milloinkin on. [GOL99]

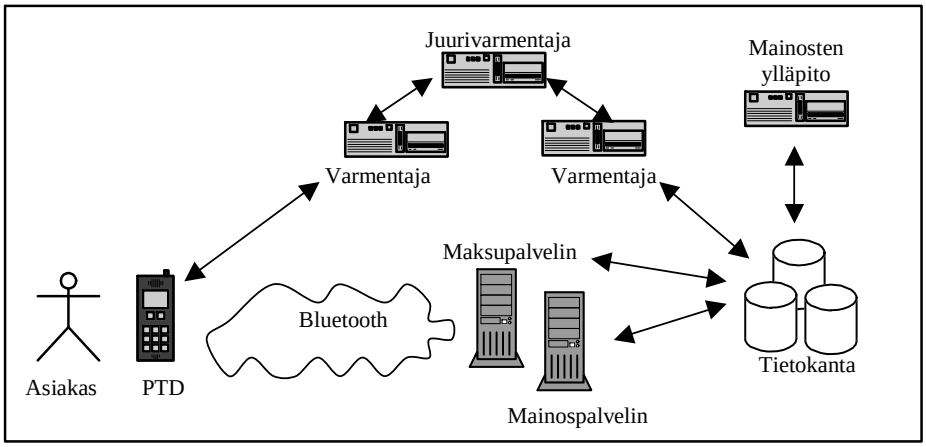
5 Lähimaksujärjestelmä

Tässä kappaleessa esitellään ratkaisu lähimaksujärjestelmän toteuttamiseksi. Järjestelmässä käytetään maksuvälineenä kämmentietokonetta ja maksaminen perustuu etukäteen maksetun tilin käyttöön. Ratkaisu soveltuu työpaikoilla tehtävien automaattiostosten ja ruokailun maksamiseen, missä maksun nopea suorittaminen on tärkeää. Järjestelmän asiakkaat voivat myös vastaanottaa mainoksia ja tehdä tilikyselyitä maksuvälineillään.

Tunnistamisessa ja tietoyhteyden suojaamisessa käytetään hyväksi julkisen avaimen järjestelmää ja varmenteita. Tiedonsiirtoon käytetään Bluetooth-tekniikkaa. Järjestelmässä käytetään hyväksi päätelaitteiden paikannusta ja esitetään ratkaisu myös paikallisten mainosten ja ruokalistojen lähettämiseksi asiakkaille.

5.1 Järjestelmän rakenne

Maksujärjestelmän rakenne ja toimijat käyvät ilmi kuvasta (14). **Juurivarmentaja** varmentaa muita järjestelmää hallinnoivia laitteita myöntämällä näille varmenteita. Juurivarmentaja ei koskaan varmenna järjestelmään käyttäjiä, mutta se varmentaa kaikki maksupalvelimet ja toisen asteen varmentajat. Juurivarmentajalla on kiinteä yhteys tietokantaan.



Kuva 14. Lähimaksujärjestelmän rakenne

Varmentaja on juurivarmentajan varmentama taho, joka varmentaa ja rekisteröi käyttäjiä järjestelmään. Se tarkastaa varmennuksen yhteydessä käyttäjän tiedot, jotka lisätään varmenteeseen, ja luo tälle tilin. Se suorittaa myös rahan tallettamisen käyttäjän tilille talletusta tehtäessä. Varmentajalla on kiinteä yhteys tietokantaan, sekä mahdollisesti Bluetooth-ominaisuus rekisteröintivaihetta varten.

Järjestelmän **asiakas** on järjestelmään rekisteröitynyt käyttäjä, jolle on myönnetty varmenne ja oma tili maksamista varten.

Maksuvälineenä toimii henkilökohtainen luotettava päätelaite. Käyttäjä liittyy päätelaitteen avulla järjestelmään. Maksuväline suorittaa käyttäjän tunnistuksen sekä maksupalvelimen tunnistuksen. Se sisältää lisäksi tietoturvaelementin, jossa suoritetaan salaus- ja allekirjoitustoiminnot ja säilytetään henkilökohtaiset tiedot. Maksuväline kommunikoi järjestelmän kanssa Bluetoothin avulla.

Maksupalvelin on juurivarmentajan varmentama kauppiaan laite, joka suorittaa tililtä laskuttamisen ja maksutapahtuman läpiviemisen. Maksupalvelin on osa automaattia tai ruokalan kassajärjestelmää, ja sillä pyörii SDP-palvelin, jonka avulla kuvataan maksupalvelimen tarjoavan maksupalvelua. Maksupalvelin suorittaa maksuvälineen tunnistamisen. Maksupalvelimessa on Bluetooth-ominaisuus sekä kiinteä yhteys tietokantaan.

Maksupalvelin pystyy käytännön syistä johtuen suorittamaan ainoastaan yhden maksutapahtuman kerrallaan. Sen sijaan tilikyselyjä tehtäessä se pystyy palvelemaan useampaa asiakasta kerrallaan.

Mainospalvelin välittää kauppiaiden mainoksia järjestelmän asiakkaille tiettyjen sääntöjen mukaisesti. Mainosten välityksessä hyödynnetään asiakkaiden paikkatietoja, jolloin automaatin mainokset lähetetään ainoastaan lähiympäristön laitteille. Fyysisesti mainospalvelimet voivat olla osa maksupalvelimia. Myös mainospalvelinten palvelut kuvataan SDP-palvelimen avulla. Mainospalvelimella on Bluetooth-ominaisuus sekä kiinteä yhteys tietokantaan.

Mainostenhallintaohjelman avulla kauppiaat voivat lisätä mainoksia tietokantaan asiakkaille välitettäväksi sekä muokata mainosryhmien käyttösääntöjä. Myös mainoksien voimassaoloajan määrittäminen ja mainosten poistaminen järjestelmästä suoritetaan mainoksenhallintaohjelmistolla. Ohjelmalla on kiinteä yhteys tietokantaan.

Lähetettävät mainokset talletetaan **tietokantaan**, samoin kuin mainosryhmien käyttösäännöt. Tietokannassa pidetään yllä myös peruutuslistaa ja varmennehakemistoa. Myös maksutapahtumatiedot ja tilin talletustiedot ovat tietokannassa.

Varmenteet

Järjestelmässä käytetään X.509v3-varmenteita, joihin on tehty muutamia laajennuksia. Asiakkaiden varmenteihin on lisätty kämmentietokoneen Bluetooth-laiteosoite ja tilin numero, johon varmenteen haltijalla on käyttöoikeus. Näin varmenne ei pelkästään todenna asiakasta, vaan myös määrittää asiakkaan maksuvälineen ja käytettävän tilin.

Myös palvelimien varmenteet sisältävät Bluetooth-laiteosoitteen. Varmentajien varmenteet puolestaan sisältävät tiedon, joka osoittaa niiden olevan varmentajia. Maksupalvelimilla on samat avaimet ja varmenteet salausta ja allekirjoitusta varten. Maksuvälineen ei tarvitse allekirjoittaa mitään, joten sillekkin riittää pelkkä salausavaimen varmenne. Kaikkien varmentajien varmenteet tulee toimittaa maksupalvelimille, koska ne käyttävät niitä asiakkaidensa varmentamiseen.

Sähköiset kuitit

Asiakkaan on mahdollista tallettaa kuitti jokaisesta tekemästään ostoksesta päätelaitteeseensa. Kuitti talletetaan jokaisen ostoksen yhteydessä myös järjestelmän tietokantaan. Kuitit on digitaalisesti allekirjoitettu maksupalvelimen salaisella avaimella, jolloin niiden oikeellisuus voidaan todeta niin vastaanottovaiheessa kuin myöhemminkin. Näin ollen kuitin voi kopioida, mutta sitä ei voi väärentää eikä sen sisältöä voi muuttaa. Kuittien sisältö käy ilmi kuvasta (15).

Wed Dec 10 12:36:31 2003
ID: 419
P: opiskelijalounas 2.05 P: kahvi 0.70
M: LUT pääruokala #1
D: 00:02:C7:0C:40:15
A: 25222
S: 2.75 eur

Kuva 15. Lähimaksujärjestelmän kuittien tiedot

Kuitissa ilmoitetaan ostotapahtuman ajankohta ja sen yksilöivä tunniste. Tuotteista kuvataan niiden nimet ja laskun loppusumma. Kauppiaasta kuvataan ainoastaan nimi, kun taas asiakkaasta kuvataan maksuvälineen laiteosoite sekä maksamiseen käytetty tili.

5.2 Järjestelmän maksuväline

Järjestelmän maksuvälineenä käytetään Linux-käyttöjärjestelmällä varustettua kämmentietokonetta. Sen suorituskyky mahdollistaa kehittyneiden salaustoimintojen ja käytettävyydeltään hyvän käyttöliittymän hyödyntämisen. Maksuohjelman ja laiteosoitteen sisältävän varmenteen avulla kämmentietokoneesta muodostetaan henkilökohtainen ja luotettava maksuväline, jonka tietoturvaelementti on ohjelmallisesti toteutettu komponentti.

Maksuohjelma

Maksuohjelman avulla luodaan salausavaimet sekä varmennepyynnöt rekisteröitymisvaiheessa. Rekisteröitymisen lopuksi vastaanotetaan salausavaimen varmenne sekä juurivarmentajan varmenne. Avaimet ja niiden salasanat sekä varmenteet talletetaan tietoturvaelementille.

Maksusuorituksessa maksuohjelma tulostaa asiakkaalle ohjeet ja tiedotteet, joiden avulla maksaminen suoritetaan. Maksuohjelma suorittaa maksamisen asiakkaan antamien komentojen mukaisesti. Komentoja annetaan kämmentietokoneelle kosketusnäytön avulla ohjauskynää käyttäen.

Maksuohjelman avulla asiakas voi myös tehdä tilikyselyitä ja vastaanottaa mainoksia. Myös maksutapahtumista saatavien kuittien hallinta tapahtuu maksuohjelman avulla: asiakas voi tarkastella, poistaa ja käyttää kuitteja maksujen todistuskappaleina kuittien välitystoiminnon avulla. Välitystoiminnon avulla kuitti voidaan siirtää kauppiaan laitteiston tarkasteltavaksi.

Käyttäjän tunnistus

Maksuohjelmaa käynnistettäessä maksuohjelma kysyy käyttäjältä salasanaa, jonka avulla käyttäjä saa käyttöoikeuden salausavaimeen. Kolmen peräkkäisen virheellisen salasanan syötön jälkeen ohjelma lukittuu ja kysyy purkukoodia. Onnistuneen käyttäjän tunnistuksen

jälkeen maksuohjelmaa voi käyttää vain tietyn aikaa, minkä jälkeen ohjelma vaatii käyttäjän tunnistuksen uusimista. Salausavaimeen ei päästä käsiksi ilman onnistunutta käyttäjän tunnistusta.

Tietoturvaelementti

Tietoturvaelementti on toteutettu ohjelmallisesti salauskirjaston avulla. Täten järjestelmän käyttämiseksi ei tarvitse hankkia erillistä toimikorttia. Elementille on talletettu salausavaimet, salasanat ja oma sekä juurivarmentajan varmenne. Salaisen avaimen säilytys on kriittisin kohta koko järjestelmässä.

Tietoturvaelementin avulla suoritetaan myös viestien salaus ja purkaminen. Asiakkaan salausavainten lisäksi salaus- ja purkutoimintoihin käytetään maksupalvelimen varmennetta. Elementti tarkastaa maksupalvelimen varmenteen allekirjoituksen juurivarmentajan varmenteen avulla.

5.3 Järjestelmän tietoyhteys

Järjestelmässä käytetään Bluetoothia paitsi maksuvälineen ja maksupalvelimien myös maksuvälineen ja mainospalvelimien välisiin tietoyhteyksiin. Tietoyhteyden suojaaminen toteutetaan salaamalla yksittäisiä viestejä eri menetelmillä. Viestien salaamiseen käytetään sekä asiakkaan että maksupalvelimen julkista ja salaista avainta. Osa viesteistä lähetetään salaamattomina niihin kohdistuvien uhkien vähyydestä johtuen. Samalla nopeutetaan maksutapahtuman kulkua.

Kun kummankin kommunikoivan osapuolen julkista ja salaista avainta käytetään viestien salaamiseen, saadaan aikaan myös luotettava osapuolten tunnistus. Tällöin voidaan todeta, että toisella osapuolella on hallussaan myös salainen avain, jota vastaava julkinen avain on varmenteessa kuvattu.

Viestiliikenne ja viestityypit

Järjestelmässä välitettävissä viesteissä on otsakekenttä, joka määrittää viestin tyypin. Viestityypistä riippuen viesti voi sisältää otsakekentän lisäksi tietokentän. Tietokenttä voi olla moniosainen, ja jokainen osa koostuu joko selkokielisestä tai salatusta tiedosta.

Taulukossa (3) on esitetty järjestelmässä välitettävät viestit, niiden kulkusuunnat ja tietokenttien pituudet sekä mahdolliset salaukset.

Taulukko 3. Lähimaksujärjestelmän viestityypit

Kulku	**Viesti**	**Otsake**	**Tietokenttä**	**Koko (tavua)**	**Salaus**
A -> V	cert_q	CERT_Q	certreq	800	**
V -> A	cert_r	CERT_R	cert	1500	*
			rootcert	1500	*
A -> P	init_q	INIT_Q	cert	1500	*
P -> A	init_r	INIT_R	cert	1500	*
			prlist	115	-
A -> P	product	PRODUCT	product_id	32	-
P -> A	challenge	CHALLENGE	chall	128	J(a)
A -> P	response	RESPONSE	resp	128	J(p)
P -> A	pay_q	PAY_Q	payment_id	128	S(p)
			sum		
			resp		
A -> P	pay_r	PAY_R	payment_id	128	S(a)
			sum		
			receipt		
P -> A	receipt	RECEIPT	receipt	128	-
			signature	128	S(p)
A -> P	account_q	ACCOUNT_Q	cert	1500	*
P -> A	account_r	ACCOUNT_R	accountState	128	J(a)
A -> P	cancel	CANCEL	-	-	-
P -> A	err	ERR	errcode	4	-
P -> A	ack	ACK	-	-	-
A -> P	advert_q	ADVERT_Q	-	-	-
P -> A	advert_r	ADVERT_R	advertData	256	-
P – palvelin A – asiakas V – varmentaja		** – sisältää PEM-koodatun varmennepyynnön * – sisältää PEM-koodatun varmenteen J – julkisella avaimella salaaminen S – salaisella avaimella salaaminen			

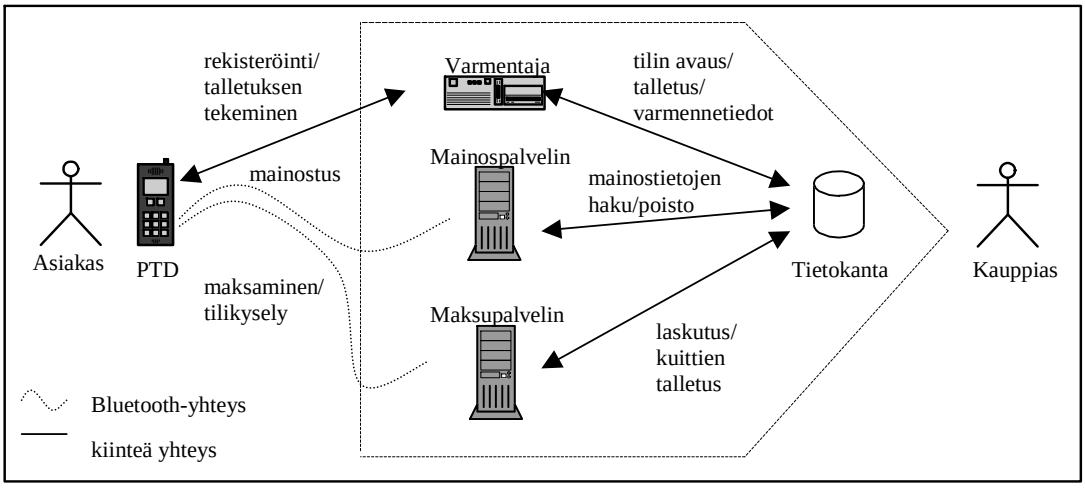
Viestit *init_q*, *init_r* ja *account_q* sisältävät otsakkeen lisäksi pem-koodatun varmenteen. *init_r* sisältää lisäksi salaamattoman tietokentän, jossa kuvataan tuotetarjonta hintoineen.

Ostettavat tuotteet ilmoitetaan palvelimelle selkokielisellä *product*-viestillä, joka sisältää valittujen tuotteiden yksilölliset tunnistenumerot. *challenge* käsittää asiakkaan julkisella avaimella salatun 112 tavua pitkän satunnaisluvun. *response* sisältää haasteesta lasketun 16 tavua pitkän tiivisteen, joka on salattu palvelimen julkisella avaimella.

pay_q sisältää laskun summan ja haasteesta lasketun tiivisteen. Koko viesti on salattu palvelimen salaisella avaimella. *pay_r* sisältää maksettavan summan sekä osoittimen siitä, halutaanko maksusta kuittia. Koko viesti on salattu asiakkaan salaisella avaimella. *receipt* sisältää palvelimen allekirjoittaman kuitin. *account_r* sisältää tilitiedot, jotka on salattu palvelimen julkisella avaimella.
err-viesti sisältää virhetunnisteen, joka kertoo päätelaitteelle, mistä järjestelmän virheellinen toiminta aiheutui. *advert* sisältää selkokielisen mainostekstin.

5.4 Järjestelmän toiminta

Asiakas voi maksaa langattomalla päätelaitteellaan automaatti- tai ruokalaostoksia, tehdä tilikyselyitä, vastaanottaa ja hallita mainoksia sekä ostotositteita (kuva 16). Tätä varten asiakkaalla täytyy olla sopiva päätelaite ja hänen pitää rekisteröityä järjestelmään. Rekisteröityminen tapahtuu varmentajan avustuksella, ja hänen luonaan tilille voi myös tallettaa rahaa.



Kuva 16. Lähimaksujärjestelmän toiminta

Mainosten vastaanotto ei ole välttämätöntä maksamisen suorittamiseksi, mutta järjestelmään rekisteröitynyt asiakas voi vastaanottaa paikallisia mainoksia milloin tahansa ollessaan mainospalvelimen kuuluvuusalueella. Asiakas voi tehdä tilikyselyjä maksupalvelimen läheisyydessä sekä maksaa ostoksia maksuvälineellään, mikäli hänen tilillään on rahaa. Maksamisen päätteeksi saatavia kuitteja voidaan käyttää todistusaineistona jälkikäteen. Seuraavassa on kuvattu edellä mainitut toiminnot yksityiskohtaisemmin.

5.4.1 Järjestelmään rekisteröityminen

Käyttäjän rekisteröiminen järjestelmään suoritetaan varmentajan luona. Varmentajana voi toimia esimerkiksi vahtimestari tai ruokalan kassan henkilökunta. Käyttäjän laitteeseen ladataan ensin maksuohjelma, jonka avulla hän voi luoda salausavaimet ja varmennepyynnön. Pyyntöön lisätään seuraavia käyttäjän tietoja:

- nimi
- sähköpostiosoite
- organisaatiotiedot
- päätelaitteen laiteosoite

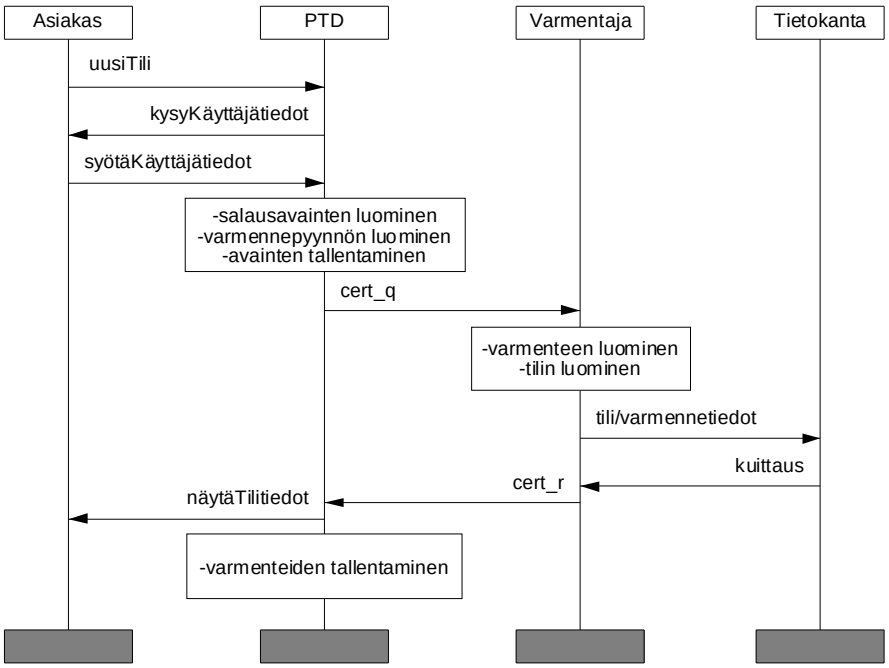
Varmentaja varmistaa käyttäjän henkilöllisyyden. Maksuohjelma lähettää varmennepyynnön varmentajalle, joka generoi tilinumeron käyttäjälle ja luo varmenteen pyynnön tietojen perusteella (kuva 17). Samalla varmentaja tarkastaa laiteosoitteen oikeellisuuden ja luo asiakkaalle tilin. Sekä tilinumero että laiteosoite lisätään varmenteen laajennuskenttiin.

Onnistuneen rekisteröitymisen jälkeen varmentaja siirtää varmenteen käyttäjän päätelaitteelle ja kopion varmenteesta varmennehakemistoon. Samalla lähetetään juurivarmentajan varmenne päätelaitteelle.

Tietoyhteys langattoman päätelaitteen ja varmentajan laitteiston välillä voidaan toteuttaa kiinteästi USB- tai sarjaporttiyhteyden avulla. Tällöin maksuohjelman oikeellisuutta ei tarvitse tarkastaa erikseen. Bluetooth-yhteyden yli siirrettäessä maksuohjelma voidaan todentaa varmentajan allekirjoituksen avulla.

Talletuksen tekeminen

Rekisteröidyttyään maksujärjestelmään asiakas voi tallettaa tililleen rahaa joko varmentajan tai ruokalan kassahenkilökunnan avulla. Sekä varmentajalla että ruokalan kassalla on ohjelmistot, joiden avulla talletukset voidaan tehdä. Talletukset voidaan maksaa millä tahansa menetelmillä, jotka ovat kyseisissä paikoissa mahdollisia. Talletusten tekemistä varten tarvitsee tietää ainoastaan tilin numero, jolle talletus halutaan tehdä.



Kuva 17. Käyttäjän varmentamisen viestiliikenne

Maksuvälineen peruuttaminen

Lähimaksujärjestelmässä maksuväline voidaan tehdä maksukelvottomaksi peruuttamalla asiakkaan varmenne. Tällöin maksuvälineen katoamis- ja varkaustapauksissa voidaan ilmoittaa varmentajalle asiasta, joka lisää asiakkaan varmenteen peruutuslistalle. Maksupalvelin tarkastaa maksuvaiheessa ettei asiakkaan varmenne ole peruutettu, koska peruutettua varmennetta ei hyväksytä asiakkaan tunnistamisessa. Mikäli asiakas haluaa myöhemmin uudelleen liittyä järjestelmään, vaatii se uutta rekisteröitymistä.

5.4.2 Mainostaminen

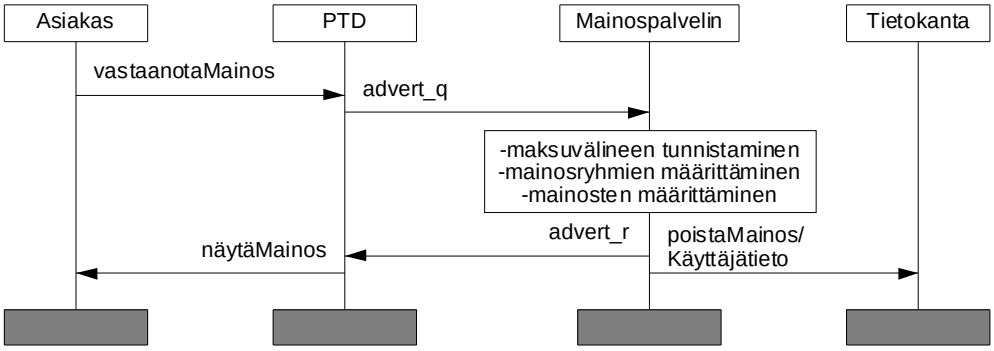
Ruokalan tarjoukset ja ruokalistojen sisällöt voidaan lähettää mainoksina suoraan asiakkaille. Kauppiaalla on ohjelmisto, jonka avulla henkilökunta voi lisätä mainoksia lähetettäväksi. Mainoksille voidaan määrittää mainosryhmät ja voimassaoloajat, joiden avulla mahdollistetaan mainosten ajankohtaisuus.

Käyttäjä voi valita järjestelmään liittyessään, haluaako hän saada mainoksia päätelaitteeseensa. Mainosryhmien avulla voidaan määritellä minkälaisia mainoksia halutaan vastaanottaa: pelkästään tarjouksia, pelkästään ruokalistoja vai kumpiakin. Mainosryhmiä voidaan myöhemmin muokata ruokalan henkilökunnan avustuksella.

Mainospalvelimen selvittäminen

Mainoksen vastaanottaminen suoritetaan asiakkaan aloitteesta (kuva 18). Maksuohjelma selvittää laitehaun avulla lähistöllä olevat Bluetooth-laitteet, jonka lisäksi mainospalvelimien selvittämiseksi käytetään SDP-kyselyjä. Asiakkaalle tulostetaan tiedot löydetyistä mainospalvelimista, joiden perusteella valitaan käytettävä palvelin.

Palvelimien selvittäminen Bluetooth-tekniikan laitehaun avulla vie paljon aikaa. Siksi tunnettujen mainospalvelimien osoite- ja nimitiedot voidaan tallettaa päätelaitteen muistiin, jolloin käytettävä palvelin voidaan suoraan valita listasta ilman laitehakuja.



Kuva 18. Mainosten 98 0 Td (e)Tj 4.m 4838.39 2122.4 l 4763.99 2141.6 l 4763.99 20Td (s)Tj 3.6

mainoksia, tehdään lähetys selkokielisenä. Kun päätelaite on saanut mainoksen, se tulostaa sen asiakkaalle.

Samaa mainosta ei lähetetä useampaan kertaan samalle käyttäjälle: kun mainos on kertaalleen lähetetty, poistetaan tietokannasta tieto, jonka mukaan kyseinen mainos tulisi käyttäjälle lähettää. Bluetooth mahdollistaa paikallisten mainosten lähettämisen lähistöllä oleville laitteille. Näin järjestelmässä voidaan lähettää asiakkaille esimerkiksi automaattikohtaisia mainoksia.

5.4.3 Maksaminen

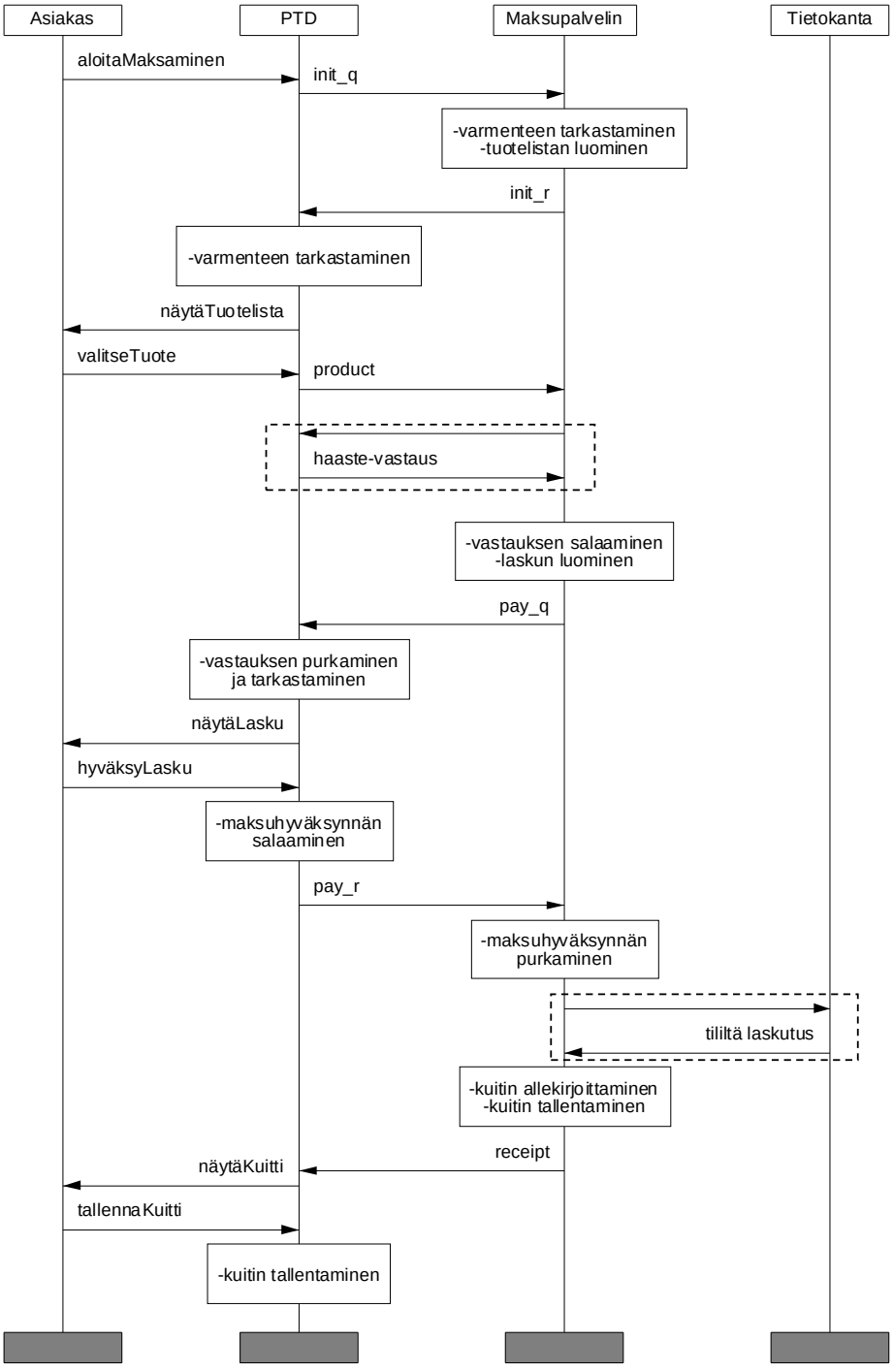
Maksaminen jakaantuu viiteen eri vaiheeseen: *maksupalvelimen selvittämiseen, osapuolten tunnistamiseen, ostamiseen, maksamiseen* ja *maksutositteen toimittamiseen.* Mallissamme osapuolten tunnistus ja tietoyhteyden salaus liittyvät läheisesti toisiinsa.

Maksupalvelimen selvittäminen

Maksuohjelma selvittää maksupalvelimet samalla tavoin kuin mainospalvelimetkin. Jos tuloksena on useampi maksupalvelin, voidaan valinta tehdä listauksesta esimerkiksi automaatin nimen ja sen kyljessä olevan tunnistetarran perusteella. Myös maksupalvelimien tiedot voidaan tallentaa päätelaitteen muistiin, jotta maksutapahtumaa voidaan jatkossa nopeuttaa.

Osapuolten tunnistaminen ja ostaminen

Maksutapahtuma aloitetaan lähettämällä varmenteen sisältävä maksunaloitusviesti maksupalvelimelle (kuva 19). Palvelin tarkastaa varmenteen varmentajien varmenteiden ja peruutuslistan avulla, ja mikäli asiakkaan varmenne on aito, sidottu kyseiseen maksuvälineeseen sekä voimassaoleva, lähettää palvelin oman varmenteensa sekä tuotelistauksen päätelaitteelle. Päätelaite tarkastaa palvelimen varmenteen juurivarmentajan varmenteen avulla. Jos palvelimen varmenne on oikea, tulostetaan tuotelistaus asiakkaalle.



Kuva 19. Maksutapahtuman viestiliikenne

Asiakas voi ostaa useampia tuotteita samalla kertaa. Valittuaan tuotteet listasta, muodostaa päätelaite viestin, joka sisältää ostettavien tuotteiden tunnistenumerot, ja lähettää sen maksupalvelimelle.

Maksupalvelin vastaa tilaukseen luomalla 128 tavua pitkän satunnaisluvun, josta lasketaan 16 tavua pitkä tiiviste. Haaste salataan asiakkaan julkisella avaimella ja lähetetään asiakkaan päätelaitteelle. Päätelaite purkaa haasteen salaisella avaimellaan ja laskee sovitulla menetelmällä haasteesta tiivisteen. Tiiviste salataan maksupalvelimen julkisella avaimella ja lähetetään maksupalvelimelle.

Maksupalvelin purkaa saamansa tiivisteen salaisella avaimellaan. Jos tiivisteet ovat yhtenevät, luo maksupalvelin laskun, joka salataan yhdessä tiivisteen kanssa maksupalvelimen salaisella avaimella ja lähetetään päätelaitteelle. Päätelaite purkaa laskun ja tiivisteen maksupalvelimen julkisella avaimella ja vertaa tiivisteitä. Mikäli tiivisteet ovat yhtenevät, tulostaa päätelaite laskun tiedot asiakkaalle.

Maksaminen ja maksutosite

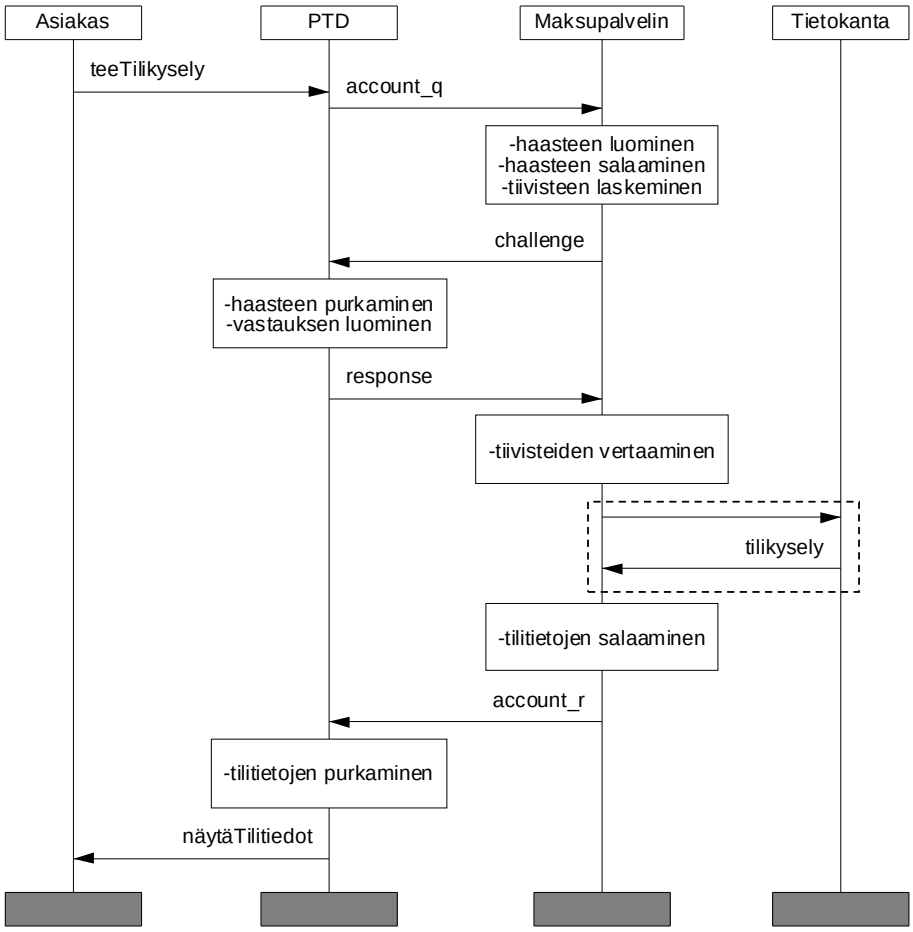
Asiakkaalla on tässä vaiheessa mahdollisuus valita, haluaako hän kuitin ostoksestaan. Kun asiakas on hyväksynyt laskun, luo päätelaite maksuhyväksynnän, salaa sen salaisella avaimellaan ja lähettää palvelimelle. Maksuhyväksyntä sisältää tiedon siitä, haluaako asiakas kuitin.

Maksupalvelin purkaa viestin asiakkaan julkisella avaimella ja laskuttaa asiakkaan tililtä laskun summan. Maksupalvelin luo tapahtumasta kuitin ja allekirjoittaa sen. Kuitti talletetaan tietokantaan ja lähetetään käyttäjälle, mikäli hän on kuitin tilannut. Muuten lähetetään pelkkä kuittaus maksun onnistumisesta. Jos tilillä ei ole katetta, lähetetään virheviesti. Ruokalan kassalla voi olla indikaattori, joka osoittaa henkilökunnalle maksun onnistumisen.

Päätelaite tarkastaa kuitin allekirjoituksen maksupalvelimen julkisella avaimella ja näyttää kuitin asiakkaalle. Asiakas voi joko tallettaa kuitin myöhempää tarkastelua varten tai tuhota sen.

5.4.4 Tilikyselyn tekeminen

Asiakas voi tehdä tilikyselyn maksupalvelimien läheisyydessä. Sen avulla asiakas saa selville kaikki tiliä koskevat tiedot, kuten tilin haltijan tiedot, tilinumeron ja tilin saldon. Asiakkaan tunnistus toteutetaan samalla tavalla kuin maksutapahtuman yhteydessäkin.



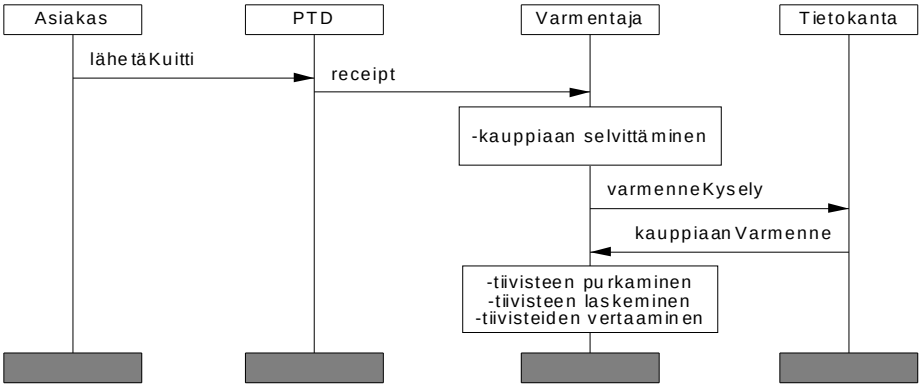
Kuva 20. Tilikyselyn viestiliikenne

Maksupalvelin tunnistetaan ainoastaan laiteosoitteen avulla. Tämä ei takaa täysin aukotonta palvelimen tunnistusta, mutta toisaalta palvelimeksi tekeytyminen tilikyselyä tehtäessä ei myöskään vahingoita järjestelmän toimintaa. Suurin haitta, jonka palvelimeksi tekeytyminen voi saada aikaan, on asiakkaan saama virheellinen tilitieto.

Tilikyselyn aloitusviestissä varmenne lähetetään palvelimelle, joka tarkastaa varmenteen oikeellisuuden ja suorittaa haaste/vastaus-menetelmän aiemmin kuvatulla tavalla (kuva 20). Onnistuneen asiakkaan tunnistuksen jälkeen palvelin tekee tilikyselyn tietokannasta ja muodostaa tilitietoviestin. Viesti salataan asiakkaan julkisella avaimella ja lähetetään tämän päätelaitteelle, joka purkaa viestin asiakkaan salaisella avaimella ja tulostaa tilitiedot.

5.4.5 Kuittien todisteena käyttö

Asiakas voi käyttää ostotapahtumista saamiaan kuitteja todisteena, jos järjestelmässä ilmenee virhetoimintaa. Tällöin asiakas voi välittää kuitin varmentajalle, joka tarkistaa sen oikeellisuuden (kuva 21).



Kuva 21. Kuittien todisteena käytön viestiliikenne

Saatuaan kuitin varmentaja tarkastaa kuitista kauppiaan palvelimen, jonka kanssa maksutapahtuma on suoritettu. Sen jälkeen varmentaja hakee tietokannasta kyseisen maksupalvelimen varmenteen ja purkaa kuitin tiivisteen siitä saadulla julkisella avaimella. Lopuksi varmentaja laskee itse tiivisteen kuitista ja vertaa maksupalvelimen luomaa tiivistettä omaansa. Mikäli tiivisteet ovat samanlaiset, on kuitti alkuperäinen ja sitä voidaan käyttää todistuskappaleena. Jos asiakasta on laskutettu väärin, voidaan menetys hyvittää esimerkiksi lisäämälle hänen tilille vastaava summa rahaa.

6 Johtopäätökset

Lähimaksujärjestelmässä voidaan vastaanottaa mainoksia, maksaa pieniä ostoksia, tehdä tilikyselyitä ja hallita kuitteja langattoman päätelaitteen avulla. Päivittäisiin ostoksiin sopivimmat maksumenetelmät ovat erilaiset liput ja tilit. Langattoman lähimaksamisen sovelluksissa tarvitaan korkeaa tietoturvaa, johon pystytään vastaamaan henkilökohtaisen luotettavan päätelaitteen ominaisuuksilla.

Tarpeelliset salaustoiminnot ja käytettävyys pystytään takaamaan kämmentietokoneen tarjoaman suorituskyvyn ja koon avulla. Tulevaisuudessa potentiaalinen maksuväline on älypuhelin, kunhan niiden suorituskyky ja käyttöjärjestelmien ominaisuudet paranevat. Toimikortin tai muun erillisen tietoturvaelementin käyttö mahdollistaisi henkilökohtaisten tietojen siirrettävyyden siten, että järjestelmässä maksaminen olisi mahdollista useammalla päätelaitteella. Ellei toimikortille ole saatavilla sisäistä lukijalaitetta, laskee käytettävyys kuitenkin liikaa.

Kaupankäynnin osapuolten tunnistaminen ja tietoyhteyden suojaaminen on mahdollista suorittaa julkisen avaimen infrastruktuurin avulla. Kun osapuolten tunnistamiseen käytetään kolmannen luotettavan osapuolen myöntämiä varmenteita, jotka varmentavat käytettävän maksuvälineen ja tilin sekä maksuvälineen omistajan, saadaan aikaan luotettava tunnistus. Samalla voidaan todeta käyttäjän oikeus tilin käyttöön. Koska maksamisen viestiliikenne muodostuu pienikokoisista viesteistä, epäsymmetrisen avaimen salaus on toimiva ratkaisu myös tietoyhteyden suojaamisessa, eikä erillisen yhteysavaimen käytölle siten ole tarvetta.

Lähteet

[APP04] Apple: Introducing the new iBook G4, 01/2004. Saatavissa: http://www.apple.com/ibook/ (tarkastettu 15.1.2004)

[BLU01] Bluetooth SIG: Bluetooth Core 1.1 vol 1 specification, 2001. Saatavissa: http://www.bluetooth.org/ (tarkastettu 12.1.2004)

[DIE99] Dierks, Allen: The TLS Protocol Version 1.0, RFC 2246 1/1999, Internet Society. Saatavissa: http://www.ietf.org/rfc/rfc2246.txt (tarkastettu 12.1.2004)

[ELL00] Ellison, Schneier: Ten Risks of PKI: What You're not Being Told about Public Key Infrastructure, Computer Security Journal Volume XVI Number 1, 2000.

[EUR02] European Union: Directive on Privacy and electronic communications, Official Journal of the European Communities L201/37 12.7.2002

[FRE96] Freier, Karlton, Kocher: The SSL Protocol Version 3.0, Internet-draft 11/1996. Saatavissa: http://wp.netscape.com/eng/ssl3/draft302.txt (tarkastettu 12.1.2004)

[GOL99] Gollman: Computer Security, 1999, England. ISBN 0-471-97844-2

[HOU02] Housley, Polk, Ford, Solo: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280 4/2002, Internet Society. Saatavissa: http://www.ietf.org/rfc/rfc3280.txt (tarkastettu 12.1.2004)

[HEW03] Hewlett-Packard: Busines products, tuotekuvaukset 12/2003. Saatavissa: http://www.hp.com/sbso/busproducts.html (tarkastettu 12.1.2004)

[HÄM02] Hämetvaara: Certificate Managament in Mobile Devices, Master's Thesis, university of Tampere 2002.

[JÄP01a] Jäppinen: Bluetooth wireless technology based guidance system, Master's Thesis, Lappeenranta university of technology 2001.

[JÄP01b] Jäppinen, Porras: Flash Notes over Bluetooth Wireless Technology, International Conference on Wireless LANs and Home Networks, 2001.

[KHU02] Khu-Smith, Mitchell: Using GSM to Enhance E-Commerce Security, WMC'02, September 28, 2002, USA.

[KÖM99] Kömmerling, Kuhn: Design Principles for Tamper-Resistant Smartcard Processors. Proceedings of the USENIX Workshop on Smartcard Technology, 1999, USA.

[LII02] Liikenne- ja viestintäministeriö: Sähköinen tapahtumalippu 08/2002. Saatavissa: http://www.mona-ohjelma.net/julkaisut/korpisalo-raportti.pdf

[LII03] Liikenne- ja viestintäministeriö: Mobiili lähimaksaminen - nykykäyttö ja tulevaisuus, Liikenne- ja viestintäministeriön julkaisuja 22/2003. Saatavissa: http://www.mintc.fi/www/sivut/dokumentit/julkaisu/julkaisusarja/2003/a222003.pdf (tarkastettu 12.1.2004)

[MEN96] Menezes, Oorschot and Vanstone: Handbook of Applied Cryptography, 1996. ISBN 0-8493-8523-7

[MET02a] MeT: MeT Core Specification 1.2, 11/2002. Saatavissa: http://mobiletransaction.org/pdf/R200/specifications/MeT_CoreSpec_v120.pdf (tarkastettu 12.1.2004)

[MET02b] MeT: PTD Definition Version 2.0 15-10-2002. Saatavissa: http://www.mobiletransaction.org/pdf/R200/specifications/MeT_PTDdef_v200.pdf (tarkastettu 12.1.2004)

[MET02c] MeT: PTD Security Requirements Version 2.0 15-10-2002. Saatavissa: http://www.mobiletransaction.org/pdf/R200/specifications/MeT_SecReq_v200.pdf (tarkastettu 12.1.2004)

[MET02d] MeT: Financial Certificates V 1.0, 01-11-2002. Saatavissa: http://www.mobiletransaction.org/pdf/R200/guidelines/MeT_Financial_Certificates_100.pdf (tarkastettu 12.1.2004)

[MET02e] MeT: Receipts Specification V 1.0, 05/2002. Saatavissa: http://www.mobiletransaction.org/pdf/R200/specifications/MeT_ReceipSpec_v100.pdf (tarkastettu 12.1.2004)

[MET02f] MeT: Receipts Requirements V 2.0, 09/2002. Saatavissa: http://www.mobiletransaction.org/pdf/R200/specifications/MeT_ReceipReq_v200.pdf (tarkastettu 12.1.2004)

[MET03a] MeT: MeT Wallet Concept Description Version 1.0, 09/2003. Saatavissa: http://www.mobiletransaction.org/pdf/met_wallet_documents/MeT_Wallet_Concept_Description_20030922.pdf (tarkastettu 12.1.2004)

[MET03b] MeT: MeT White Paper on Mobile Ticketing 1.0, 01/2003. Saatavissa: http://www.mobiletransaction.org/pdf/R200/white_papers/MeT_White_paper_ on_mobile_ticketing_v1.pdf (tarkastettu 12.1.2004)

[MIO04] Miotec: Esittelymateriaalit - Esitteet ja datasivut, 2004. Saatavissa: http://www.miotec.fi/suomi/viestinta/esittelymateriaali/esitteet.html (tarkastettu 17.2.2004)

[MUU03] Muukkonen: Puhelimella voi tehdä sopimuksen, Tietoviikko 4.12.2003

[NEG00] Negin, Chmielewski Jr, Salganicoff, Camus, von Seelen, Venetianer, Zhang: An Iris Biometric System for Public and Personal Use, Computer IEEE 2002.

[NIC02] Nichols, Lekkas: Wireless Security: Models, Threats and Solutions, 2002. ISBN 0-07-138038-8.

[NOK03a] Forum Nokia: Introduction to the Nokia Wallet Application, version 1.0; April 16, 2003. Saatavissa: http://www.forum.nokia.fi (tarkastettu 13.1.2004)

[NOK03b] Nokia: Puhelinmallit, 12/2003. Saatavissa: http://www.nokia.fi/puhelimet/puhelinmallit/ (tarkastettu 12.1.2004)

[NOR03] Nordea: Nordea kokeilee uutta tapaa maksaa kännykällä. Saatavissa: http://www.nordea.fi/fin/info/news/20030912.ASP?navi=yritys info&item=yritysinfo (tarkastettu 12.1.2004)

[OPE02] OpenSSL Project: Documents, pem(3), 2002. Saatavissa: http://www.openssl.org/docs/crypto/pem.html

[PAY04] Payway Ltd: Parkit – Service description, 2004. Saatavissa: http://www.payway.fi/en_description.html, (tarkastettu 12.1.2004)

[PAL04] Palmsource: Handhelds & Smartphones 01/2004. Saatavissa: http://www.palmsource.com/ (tarkastettu 15.1.2004)

[PHI00] Phillips, Martin, Wilson, Przybocki: An Introduction to Evaluating Biometric Systems, Computer IEEE2000.

[POP03] Population Register Centre (VRK): FINEID S4-1, Implementation Profile 1 for Finnish Electronic ID Card v 2.0, 2003. Saatavissa: http://www.fineid.fi/download/S4-1v20.pdf (tarkastettu 12.1.2004)

[POR03a] Poropudas: Visa and Telenor provide m-commerce to Norwegians, lehdistötiedote 13.2.2003. Saatavissa: http://www.mobile.commerce.net/story.php?story_id=2761 (tarkastettu 12.1.2004)

[POR03b] Portalify: Coinlet Mobile Payment Solution, white paper 2001. Saatavissa: http://www.portalify.com/files/Coinlet_WhitePaper.pdf (tarkastettu 12.1.2004)

[RAD00] Radicchio: Choosing a smart card for secure wireless e-commerce, 2000. Saatavissa: http://www.radicchio.org/member_center/download/bpwg/bpr_001.pdf (tarkastettu 12.1.2004)

[RSA99a] RSA Laboratories: PKCS#15 - A Cryptographic- Token Information Format Standard 11/1999. Saatavissa: http://www.usenix.org/publications/library/proceedings/smartcard99/full_papers/nystrom/nystrom.pdf (tarkastettu 12.1.2004)

[RSA99b] RSA Security Inc: Understanding Public Key Infrastructure (PKI), 1999. Saatavissa: http://www.computel.com.lb/Downloads/PKI.pdf (tarkastettu 12.1.2004)

[SAM04] Samsung: Mobile Phone Products, 01/2004. Saatavissa: http://www.samsung.com/Products/MobilePhone/CDMA/index.htm (tarkastettu 15.1.2004)

[SCH96] Schneier: Applied Cryptography: Protocols, Algorithms and Source Code in C, 2. edition, John Wiley & Sons, Inc. 1996. ISBN 0-471-12845-7

[SCH99] Schneier, Shostack: Breaking Up Is Hard To Do: Modelling Security Threats for Smart Cards, 19.10.1999. Saatavissa: http://www.counterpane.com/smart-card-threats.pdf (tarkastettu 12.1.2004)

[SCH02] Schwiderski-Grosche, Knospe: Secure Mobile Commerce, Electronics & Communication Engineering Journal, Volume: 14 Issue: 5 , Oct. 2002.

[SET97] SET: Secure Electronic Transaction Specification, Book2: Programmer's Guide version 1.0, 1997. Saatavissa: http://www.setco.org/download.html#spec (tarkastettu 12.1.2004)

[SMI01] Smith: Authentication From Passwords to Public Keys, 2001. ISBN 0-201-61599-1

[SUO78] Suomen eduskunta: Kuluttajansuojalaki (38/1978), muutokset 5.6.2002/460 ja 15.12.2002/1072

[TAN02] Tanila, Teemu: Sähköiset liput: Tietoturvaa julkisen avaimen teknologiasta, Pro gradu –tutkielma, Tampereen yliopisto 2002.

[VEI02] Veijalainen, Terziyan, Tirri: Transaction Management for M-Commerce at a Mobile Terminal, Proceedings of the 36th Hawaii international Conference on System Sciences, IEEE 2002.

[VEI03] Veijalainen, Haq, Matsumoto: Privacy and Security Considerations for PTD, 2003. Saatavissa: http://www.dicomo.org/2003/dicomo-papers/140.pdf (tarkastettu 12.1.2004)

[VIS03] VISA: NTT Docomo, Visa International, Nippon Shinpan & co. Test Payments via Mobile Phone IrDA Ports, 7.4.2003. Saatavissa: http://www.corporate.visa.com/mc/press/press143.html (tarkastettu 12.1.2004)

[WAP01a] WAP Forum: Wireless Application Protocol Public Key infrastructure Definition Version 24-Apr-2001.

[WAP01b] WAP Forum: Wireless Transport Layer Security Version 06-Apr-2001.

[WAR97] Warwick Ford, Michael S. Baum: Secure Electronic Commerce, Prentice Hall PTR, 1997. ISBN 0-13-027276-0