Petri Lamminaho

Mobiilimaksaminen

Tietotekniikan
kandidaatintutkielma
20. syyskuuta 2011

Jyväskylän yliopisto

Tietotekniikan laitos

Jyväskylä

Tekijä: Petri Lamminaho
Yhteystiedot: petri.lamminaho.jyu.fi
Työn nimi: Mobiilimaksaminen
Title in English: Mobile payment
Työ: Tietotekniikan kandidaatintutkielma
Sivumäärä: 35
Tiivistelmä: Mobiilimaksamisella tarkoitetaan mobiililaitteella, esimerkiksi matkapuhelimella, tapahtuvaa maksamista. Karkeasti se voidaan jakaa etä- ja lähimaksamiseen. Mobiilimaksamista käytetään enimmäkseen pienten ja halpojen tavaroiden tai palveluiden ostoon. Maksamiseen käytetään kaikkia nykyisissä laitteissa olevia tekniikoita: puhelin- ja tietoverkkoa Bluetoothia ja uusimpana NFC-tekniikkaa.

Tietoturva ja varsinkin käyttäjien todentaminen ovat hyvin tärkeitä seikkoja mobiilimaksamisessa. Tietoturva onkin yksi keskenimmistä haasteista mobiilimaksamisessa, varsinkin kun tehdään suuria ja kalliita ostoksia. On käyttäjä pystyttäjä tunnistamaan varmuudella. Nykyisin kännyköissä on älykortit ja sirut joita voidaan myös käyttää maksamisessa käyttäjän tunnistukseen, esimerkiksi NFC käyttää SIM-korttia tunnistukseen.

English abstract: Mobile payment means that user uses mobile device for payment. There are two kind of payment system. Remote system and local payment system. Typically mobile payment is used for small and cheap payments. There are various payment systems and they use a variety of technologies. For example 3G, Bluetooth and NFC, witch is the newest technology.

Security and authentication are very important issues for mobile payment especially when payments are big. Nowadays almost all mobile devices have some kind of a smart card or chip that can be used for identification. For example NFC uses chip and device's SIM-card for authentication.
Avainsanat: tietotekniikka, kandidaatintutkielma, mobiilimaksaminen, Mobiiliteknologiat, NFC
Keywords: information technology, Bachelor's thesis, Mobile payment, Mobile technologies, NFC

Sisältö

1 Johdanto

Matkapuhelimet ja muut mobiililaitteet ovat yleistyneet vauhdilla. Suomessa lähes jokaisella aikuisella on ainakin yksi mobiililaite, joka on yleisimmin matkapuhelin. Toisaalta erilaiset kämmentietokoneet, niin kutsutut tabletit ovat yleistyneet.

Euroopan ja Pohjois-Amerikan lisäksi mobiililaitteiden käyttö lisääntyy myös kehittyvissä maissa, kuten Aasiassa ja Afrikassa. Monelle mobiililaite onkin ensimmäinen internetpäätelaite, joka korvaa perinteisen tietokoneen.

Viime vuosina perinteiset matkapuhelimet ovat lähentyneet perinteisiä tietokoneita. Nykyisin muistia on huomattavasti enemmän ja laitteiden prosessoritehot ovat moninkertaistuneet. Nykyisiin tehokkaimpiin mobiililaitteisiin on saatavilla paljon uusia sovelluksia ja muuta ladattavaa sisältöä esim. musiikkia ja videoita Kuluttaja voi esimerkiksi hankkia uutiset kännykkäänsä videona tai ostaa uusimman mobiilipelin tai radiohitin omalle laitteelleen suoraan verkosta.

Kuluttajan hankkiessa maksullista sisältöä laitteelleen tarvitaan jonkinlainen järjestelmä jonka kautta kuluttaja maksaa tekemänsä ostokset. Koska järjestelmän välityksellä hoidetaan rahaliikennettä, on tieturvaan ja salauksiin on kiinnitettävä huomiota.

Tutkielmassani perehdyn tällaisiin järjestelmiin. Listaan hyvän maksujärjestelmän kriteerejä. Arvioinnin perustana käytän luvussa 3 esittelemiäni hyvän maksamisjärjestelmän kriteerejä. Lisäksi tutkin erilaisia teknisiä ratkaisuja joita mobiilimaksujärjestelmissä käytetään.

Luvussa 2 kerron mobiilimaksamisjärjestelmistä yleisellä tasolla ja pyrin selittämään mikä mobiilimaksamisjärjestelmä itseasiassa on. Luvussa 3 esittelen millaisia kriteerejä hyvälle järjestelmälle asetetaan.

Luvussa 4 esittelen eri järjestelmätyypit. Esittelen niiden yhtenäisyyksiä ja eroja. Ja millaisia ne ovat käyttää. Luvussa 5 esittelen järjestelmissä käytettäviä arkkitehtuureja. Ja selvennän miten käytettävä arkkitehtuuri vaikuttaa järjestelmän toimintaan ja sen käyttöön.

Luvussa 6 esittelen viestintätekniikoita joita mobiilijärjestelmissä käytetään. Selvitän eri tekniikoiden etuja ja haittoja. Lisäksi, kuten edellisessäkin luvussa selvennän miten käytettävä teknologia vaikuttaa järjestelmän toimintaan ja sen käyttöön. Osa luvussa 6 esitellyistä teknologioista ovat käytännössä jo poistuneet käytöstä.

Lopussa luvussa 7 esittelen mobiilijärjestelmien tietoturvaa. Mobiilijärjestelmien asettamista haasteista. Esittelen pikaisesti käytettyjä salaus ja autentikointitekniikoista.

2 Taustaa

Mobiilimaksamisella tarkoitetaan maksamista, joka tapahtuu mobiililaitteiden avulla. Laiteen on oltava pienikokoinen ja helposti liikuteltava. Langattomien laitteiden lisääntyessä myös mobiilimaksamisjärjestelmät tulevat kehittymään ja yleistymään. Maksamiseen voidaan käyttää kännykkää, älypuhelinta tai erilaisia kämmentietokoneita. Helsingissä kuluttaja voi esimerkiksi ostaa bussilipun tai parkkimaksun kännykällä.

Maksaminen tapahtuu yleensä soittamalla tai lähettämällä tekstiviesti palveluntarjoajan puhelinnumeroon. Tällaisissa palveluissa laskutus tapahtuu usein puhelinlaskun yhteydessä. Nykyään on kuitenkin olemassa niin sanottuja lähimaksamisjärjestelmiä, joissa yleensä käytetään muunlaista tekniikkaa. Käytetyistä teknologioista ja protokollista kerron tarkemmin luvussa 6.

Maksutapahtuman perusperiaate on pääosin samanlainen käytetystä järjestelmästä ja teknologiasta riippumatta. Ensimmäiseksi käyttäjä ottaa mobiililaitteellaan yhteyttä palveluun ja kirjautuu sisään. Tämän jälkeen ostaja valitsee halutut tuotteet ja lähettää niistä tiedon palveluntarjoajalle. Tämän jälkeen kauppias varmistaa ostajan henkilöllisyyden ja maksukyvyn ja lähettää kuittauksen onnistuneesta ostotapahtumasta.

Palveluun rekisteröityminen ja myyjän löytäminen vaihtelee tekniikan ja järjestelmän mukaan. Käsittelen aihetta tarkemmin luvuissa 4 ja 6. Asiakkaan ja kauppiaan välinen autentikoinnissa on myös eroja riippuen käytetystä tekniikasta. Autentikointia käsittelen luvussa 7.

Maksaminen voi olla kahden kuluttajan välistä(P2P, Person to Person),Yritysten välistä (B2B, Business to Business) tai yrityksen ja kuluttajan (B2C, Business to Consumer). [1] [10] [14]

Maksaminen voi tapahtua ennakkoon(esimerkiksi sähköinen raha ja pepaid-kortit), jälkikäteen(esimerkiksi luotokortit ja puhelinlaskun yhteydestä) tai reaaliajassa jolloin myyjä saa tiedon maksun suorittamisesta heti(esimerkiksi pankkikortit ja reaaliaikainen tilinsiirto). Moni meistä on tilannut kännykällä palveluita jotka on maksanut ennen kuin on käyttänyt palvelua. Jälkikäteen maksamisessa laskutus tapahtuu erillisellä laskulla tai maksuohjeilla jotka myyjä lähettää ostajalle. [12] [14]

Uusien nopeiden matkapuhelinverkkojen yleistyessä puhelimeen tilattavat palvelut monipuolistuvat. Osa tulevaisuuden palveluista ja sisällöistä tulee olemaan maksullisia, joten tarvitaan jokin luotettava ja nopea tapa maksaa kännykkään tilattavat sisällöt. Kätevimmin tämä käy suoraan puhelimella.

Nykyisin ainoa verkossa maailmanlaajuisesti luotettavasti toimiva maksutapa

on luottokortit. Luottokortin numeron antaminen verkkosivustolle ei kuitenkaan ole täysin ongelmatonta. Väärinkäytöksiä, joissa luottokortin numerot ovat päätyneet vääriin käsiin, on tapahtunut. Mobiilimaksamisesta toivotaan kilpailijaa luottokortille verkkokaupassa. Mobiilimaksamisen toivotaan syrjäyttävän tulevaisuudessa lompakon ja luottokortin. Tavoitteena on, että kuluttajan taskussa olisi kannettava laite jolla puhumisen lisäksi voisi myös maksaa laskuja ja ostoksia helposti ja nopeasti. Nykyisin varsinainen mobiilimaksaminen melko vähäistä muihin sähköisiin maksutapoihin, kuten kuvasta 1 ilmenee. Kasvu on kuitenkin ollut viime vuosina voimakasta. [12]

Mobiilimaksamisen haasteita ovat järjestelmien kankeus ja hitaus, tietoturvaongelmat ja tietyt lailliset ongelmat maksamisessa, eli kuka korvaa jos väärinkäytöksiä tapahtuu. Palvelujen tason odotetaan paranevan tekniikan kehittyessä ja salausmenetelmien kehittyessä tietoturvakin paranee. Näistä asioista lisää luvuissa 6 ja luvussa 7. [1] [14]

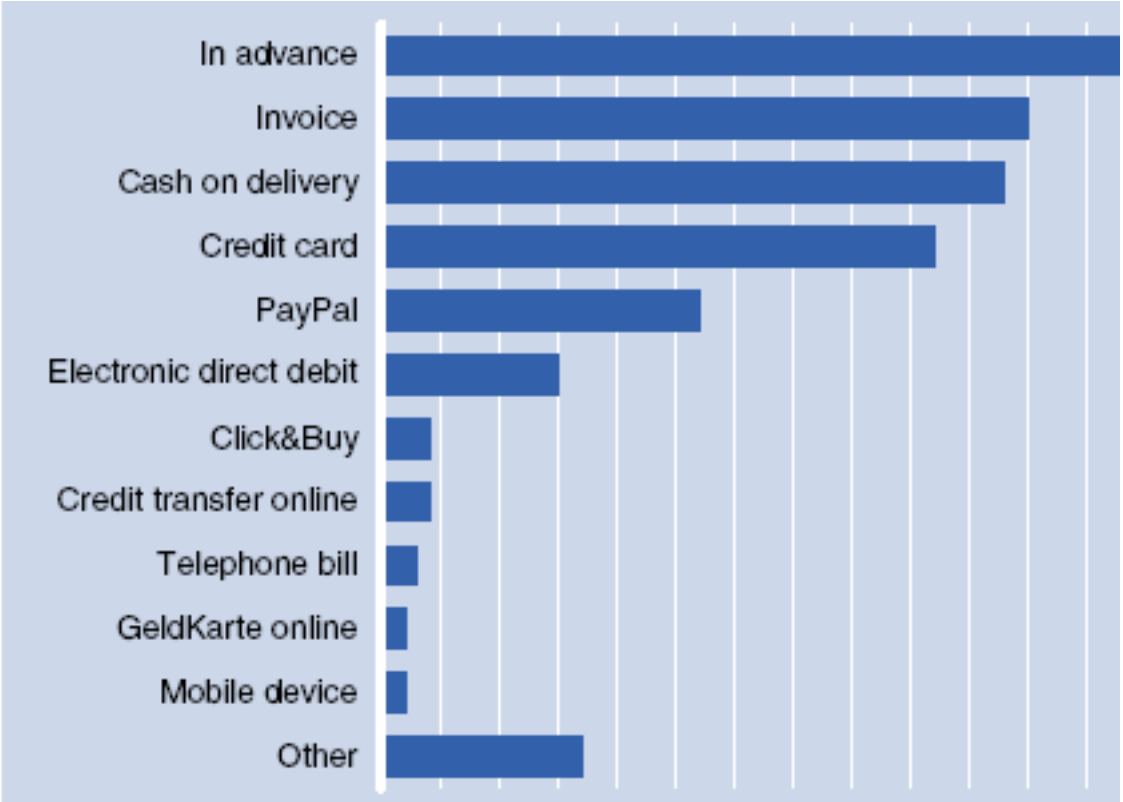
Mikromaksaminen on termi joka esiintyy mobiilimaksamisen yhteydessä. Kuluttajavirasto määritelmän mukaan mikromaksamisen sähköisen rahan käyttämistä pieniin ostoksiin verkon kautta. [16] Sähköistä rahaa kuluttaja voi hankkia palveluntarjoajilta.

Suomalaisen e-Business-verkkosivuston mukaan mikromaksamisella hankitut hyödykkeet saavat maksaa enintään 10 euroa. [6] Esimerkkinä tällaisista hyödykkeistä voidaan mainita soittoäänet ja logot matkapuhelimeen. Koska hyödykkeet joita mikromaksamisella ostetaan ovat pieniä ja halpoja, ei tietoturvan ja kuluttajan tunnistaminen tarvitse olla yhtä vahvaa kuin kalliimmissa ostoksissa.

Maksamisen tapoja ovat esimerkiksi erilaiset tilinsiirrot, prepaid-tilit ja sähköiset shekit. Ehkä kuitenkin tärkein tapa on niin kutsuttu ”maksusuhteen ositus” (payment relationship sharing). Menetelmässä kauppias, jolla on maksusuhde kuluttajan kanssa, tarjoaa palvelua jonka kautta muutkin kauppiaat voivat laskuttaa kuluttajaa sopimuksen kautta. Yksinkertainen esimerkki tällaisesta on soittoäänen tilaaminen kännykkään muualta kuin omalta operaattorilta. Ostoksista syntyneet kustannukset lisätään ostajan puhelinlaskuun. Kuluttaja maksaa ostoksen seuraavassa puhelinlaskussa. [1]

Maksamisessa voidaan myös käyttää sähköistä rahaa, jonka kuluttaja on hankkinut joltain luotettavaksi tunnetulta taholta. Maksutapahtuman aluksi myyjä tarkistaa ostajan henkilöllisyyden ja vähentää käytetyt rahat ostajan sähköisestä lompakosta. Lopuksi palveluntarjoaja siirtää myyjän tilille oikeaa rahaa. Nykyiset sirukortit joihin voidaan tallettaa rahaa toimivat samalla periaatteella. Jotta maksaminen onnistuisi, täytyy kauppiaalla ja palveluntarjoajalla olla keskinäinen sopi-

mus. [1] [10] [16]



Kuva 1: Käytetyimmät maksutavat sähköisessä liiketoiminnassa. [12]

3 Hyvä mobiilimaksamisjärjestelmä

Mobiilimaksaminen on lisääntynyt muutamassa vuodessa merkittävästi. Mobiililaitteiden ja nopeiden tietoverkkojen yleistyessä palvelut ovat kehittyneet. Mobiilimaksusta onkin tullut varteenotettava vaihtoehto muiden maksutapojen rinnalle.

Tärkeä tekijä järjestelmien suosiossa on palvelujen taso. Jos käyttäjät eivät ole kiinnostuneita palveluista, on niitä turha kehittää ja markkinoida. Esimerkkinä voidaan pitää muutaman vuoden takaista WAP-innostusta. Alussa tekniikkaa markkinoitiin palveluilla joita ei vielä ollut. Kun palvelut viimein tulivat kuluttajien saataville, olivat ne kalliita, hitaita ja kömpelöitä käyttää. Samat palvelut voitiin toteuttaa tekstiviestillä kätevämmin ja ennen muuta edullisemmin. WAP toimii mobiiliverkossa ja alkuaikojen GSM-verkot olivat turhan hitaita sujuvaan asiointiin. Verkot olivat hitaita ja yhteydet epävarmoja. Nykyiset 3G-verkot ovat nopeita, eivätkä enää aseta rajoituksia palveluille. [17]

Nykyisin tekniikka ja palvelut ovat kehittyneet parempaan suuntaan, mutta tekniikalla on vieläkin huono maine kuluttajien keskuudessa. Alusta asti WAP-tekniikkaa käytettiin nimenomaan mobiilimaksamispalveluissa. Virvoitusjuoman ostaminen tai parkkimaksun maksaminen kännykällä on ollut mahdollista jo usean vuoden ajan. [17]

WAP-huumasta pitäisi oppia ainakin se, että tekniikan toimivuus ei vielä riitä kuluttajien innostuksen saamiseen. Ennen kuin palvelut tuodaan käyttäjien saataville, käytetty tekniikan kannattaa olla hyvin kehittynyttä ja palvelut sellaisia, että kuluttajat haluavat käyttää niitä.

Agnieszka Zmijewskan määrittelee artikkelissaan hyvän mobiilimaksamisjärjestelmän tunnusmerkit. [32] Toisessa saman tyylisessä artikkelissa, Ljupco Antovski ja Marjan Gusev päätyvät lähes samoihin tekijöihin. [1]

Ensimmäinen, ja ehkä tärkein tekijä on helppokäyttöisyys. Järjestelmän tai palvelun käyttöönotto on oltava helppoa, eikä se saa vaatia työlästä opettelua. Itse käytön pitää olla selkeää ja maksutapahtuma pitäisi hoitua muutaman napin painalluksella. [1] [32]

Koska maksutapahtumassa liikkuu raha, on tietoturva tärkeässä osassa hyvän maksamisjärjestelmässä. Lähetettävän datan oikeellisuudesta ja siitä, että lähetettävät viestit tulevat perille on oltava varma. Viesti on salattava luotettavasti ennen lähetystä, ettei kukaan ulkopuolinen pääse käsiksi tietoihin. Käsittelen tietoturvaa tarkemmin luvussa 7 .

Kolmas kriteeri on kustannukset, joihin lasketaan niin investoinnit, palvelun käyttöönotto ja palvelun varsinaiset käyttökustannukset. Investointeihin lasketaan kustannukset, jotka käyttäjä joutuu tekemään käyttääkseen palvelua(esimerkiksi uuden puhelimen osto). Käyttöönottoon liittyvät kustannukset esimerkiksi palvelun liittymismaksut. Käytöstä aiheutuvat maksut koostuvat puhelinoperaattorin perimistä datansiirtomaksuista ja maksupalvelun veloittamista maksuista, kun palvelua käytetään. [1] [32]

Palvelun hinta on tietysti oltava mahdollisimman pieni, jotta tavalliset keskituloiset kuluttajat saadaan käyttämään palvelua. Keskiverto kuluttaja, joka käyttää matkapuhelintaan ainoastaan puhumiseen, ei todennäköisesti osta uutta kallista puhelinta mobiilimaksamisen takia. Lisäksi varsinkin pieniä ostoksia ostettaessa, maksutapahtumasta perittävä maksut eivät saa olla kalliimpia kuin itse ostos. [1] [32]

Lisäksi Antovski ja Gusev mainitsevat järjestelmän ”yleismaailmallisuutta”, joka käytännössä tarkoittaa, että järjestelmä on standardien mukainen siirrettävä muihin ympäristöihin. Lisäksi he mainitsevat artikkelissaan tekniikan hyväksyttävyyden eli ihmisten on pidettävä tekniikkaa tärkeänä ja sellaisena jota suostuvat käyt-

tämään palvelua säännöllisesti. [1]

Agnieszka Zmijewska listaa kriteeriksi artikkelissaan järjestelmän hyödyllisyyden, joka on käytännössä aika lähellä hyväksyttävyyttä. Ihmisen on, Zmijewskan mukaan, koettava palvelu elämää helpottavaksi asiaksi. Järjestelmän käytön tulisi nopeuttaa asiointia; kuluttajan työteho nousee. [32]

Järjestelmän liikuteltavuus, eli järjestelmä toimi mobiililaitteen avulla missä ja milloin vain on yksi Zmijewskan kriteereistä. Käytännössä tämä on lähes mahdotonta. Rajoituksia tuottaa kännykkäoperaattorin verkko joka ei välttämättä toimi joka paikassa. Toisaalta, vaikka verkko toimisikin, eivät kaikki palvelut toimi joka paikassa. [32]

Viimeisenä kriteerinä Zmijewska mainitsee mielenkiintoisen tekijän. Palvelu voi olla käyttävälle itsensä ilmaisemisen väline. Eli palvelu saattaa olla muotia ja käyttäjälle statussymboli, jonka avulla he erottuvat massasta. Esimerkkinä tällaisista palveluista voidaan pitää yksilöllistä soittoääntä. [32]

4 Erilaiset järjestelmätyypit

Erilaisia maksamisjärjestelmiä on useita erilaisia. Niiden arkkitehtuurit ja käytetyt tekniikat eroavat toisistaan paljonkin. Natali Delić ja Ana Vulkašinović määrittelevät artikkelissaan palvelut kolmeen eri kategoriaan. [4]

- **Tekstiviesteihin perustuvat järjestelmät**
- **POS-järjestelmät**
- **Internetpohjaiset järjestelmät**

Toinen mahdollinen järjestelmien jako, jota alan julkaisuissa käytetään on seuraava: [9]

- **Tilipohjainen systeemi**
- **POS-järjestelmät**
- **Mobiililompakko**

4.1 Tilipohjaiset järjestelmät

Tilipohjainen-järjestelmässä käyttäjä luo ensimmäisellä käyttökerralla tilin. Tili luodaan yleensä palvelun ylläpitäjän verkkosivuilla, mutta on olemassa palveluita joissa käytettävä tili on asiakaan pankki- tai luottotili. Tilin luonnin yhteydessä käyttäjä

antaa omat tietonsa tilin ylläpitäjälle. Jotta järjestelmä toimisi, tarvitaan jokin kolmas luotettavaksi tiedetty taho; esimerkiksi pankki, josta myyjä tietää saavansa rahat. Maksaminen tapahtuu joko ennakkoon tai jälkikäteen luodulta tililtä. [4] [14]

Yksinkertaisimmillaan tilipohjaisessa järjestelmässä laskutus voi tapahtua puhelinlaskun yhteydessä. Maksamiseen voidaan myös käyttää sähköistä rahaa tai älykorttia, jonka myyjä vaihtaa ”oikeaksi” rahaksi. Toinen mahdollisuus on, että ostaja käyttää luottokorttiaan järjestelmässä. Käytännössä kuluttaja antaa luotokorttinsa tiedot rekisteröitymisen yhteydessä. Maksettaessa luottokortin tiedot välitetään myyjälle automaattisesti, eikä käyttäjän tarvitse antaa niitä joka kerta.

Eräs esimerkki tällaisesta maksamisjärjestelmästä on Serbiassa toimiva DinaCard-maksukortti. [4] [5] [10] Asiakas voi hankkia kortin pankista tavallisen luotokortin tapaan. Kortista on olemassa prepaid tai postpaid versio ja sillä voi maksaa POS-terninaalin kautta, internetissä tai tekstiviestillä. Lisäksi kortille voi ladata rahaa automaateista. [5] Kortti toimii vain jos matkapuhelinverkko tukee sitä. Käyttäjien tunnistus hoidetaan puhelinliittymän avulla. [4] [5] [10] Suomessa järjestelmä ei toimi.

Järjestelmän hyvänä puolena on se, etteivät käyttäjän tarvitse lähettää yksityisiä tärkeitä tietojaan joka kerta järjestelmään. Rekisteröitymisen jälkeen maksaminen onkin turvallista ja nopeaa, edellyttäen ettei tilin tiedot joudu vääriin käsiin. Tilin luominen ja palveluun rekisteröityminen ovat kriittisiä kohtia, tällöin esimerkiksi luottokortin numero tai muut tärkeät tiedot eivät saa hukkua tai paljastua .

4.2 POS-järjestelmät

Niin kutsuttu POS-järjestelmä (Point Of Service tai Point Of Sale) on lähimaksamisjärjestelmä, jossa ostaja mobiililaitteellaan kytkeytyy POS-maksupäätteeseen ja hoitaa maksutapahtuman. Ostajan laite ja maksupääte ovat siis lähellä toisiaan. Yksinkertaisimmillaan ostaja voi lähettää puhelimensa lompakossa olevan luottokortin numeron myyjän päätteelle. Maksaminen tapahtuu suoraan ostajan ja myyjän välillä eikä välissä ole palvelinta, vaan naksupääte on yhteydessä jonkinlaiseen palvelimeen esimerkiksi pankkiin. [4] [9] [10]

Tällainen järjestelmä voi olla automaattinen tai ihmisen hoitama. Automaattinen järjestelmä on esimerkiksi virvoitusjuoma-automaatti. Ihmisen hoitamasta järjestelmä voi olla kaupan kassa tai taksikuskin ja matkustajan välinen maksutapahtuma. [4] [10]

Koska ostaja ja myyjä ovat POS-järjestelmässä usein sosiaalisessa yhteydessä toisensa kanssa maksettaessa, voidaan maksajan henkilöllisyys tarkistaa esimerkiksi ajokortilla, tämä lisää järjestelmän turvallisuutta. Järjestelmän kriittinen kohta on

tietojen lähettäminen kauppiaan laitteelle. Lähetettävän tiedon täytyykin olla salatussa muodossa ja vietin on mentävä varmuudella oikeaan paikkaan. Enemmän käytetyistä tekniikoista luvussa 6. [4] [10]

POS-järjestelmien suurimana ongelmana on standarttien puute. Esimerkiksi nykyisissä matkapuhelimissa oleva lompakko toiminto, johon käyttäjä voi tallentaa esimerkiksi luottokortin tiedot, tallentaa ja lähettää tiedot hieman eri tavalla riippuen puhelinmallista. Käyttäjien puhelimet tai POS-päätteet eivät siis välttämättä ymmärrä toisiaan vaan pahimmassa tapauksessa jokainen puhelin tarvitsee erilaisen POS-terminaalin. [4] [10]

4.3 Tekstiviesteillä toimivat järjestelmät

Tekstiviesteihin perustuvat järjestelmät ovat yleensä etämaksamisjärjestelmiä, eli ostaja ja myyjä eivät ole läheisessä kontaktissa keskenään. Lisäksi järjestelmät ovat tilipohjaisia. Järjestelmässä ostajan ja kauppiaan välinen kommunikointi hoidetaan tekstiviestien avulla. Maksaminen tapahtuu lähettämällä tekstiviestin maksamisjärjestelmän puhelinnumeroon. Tällaisia järjestelmiä on useita erilaisia, mutta perusidea on kaikissa sama. Ainostaan lähetettävien viestien syntaksit ovat hieman erilaisia. Tekstiviestin avulla kuluttaja voi esimerkiksi tilata soittoääniä kännykkään, jolloin maksu yleensä peritään puhelinlaskun yhteydessä. Koska ostaja ja kauppias eivät ole maksamistilanteessa suorassa yhteydessä toisiinsa vaan kaikki liikennöinti tapahtuu maksamisjärjestelmän palvelimen kautta on kuluttaja tunnistettava koneellisesti. Yleensä tällaisissa järjestelmissä tyydytään PIN-koodin ja puhelimen SIM-kortin tunnistamiseen eikä vahvempia tunnistusmenetelmiä käytetä. Tällaisilla järjestelmillä maksettavat summat ovat kohtuullisen pieniä, ettei raskaammat ja luotettavammat menetelmät kannata. [4] [32]

Järjestelmän maksutapahtuma on kaksivaiheinen, ensin asiakas lähettää viestin jossa hän kertoo summan, oman tilinumeronsa, saajan tilinumeron ja jonkinlaisen viestin. Kun palvelu saa viestin se tarkistaa viestin syntaksin ja tilinumeroiden oikeellisuuden. Tämän jälkeen käyttäjälle lähetetään viesti, jossa pyydetään PIN-koodia. Asiakas vastaa viestiin lähettämällä koodin järjestelmään, joka tarkistaa sen oikeellisuuden ja suorittaa maksun. Lopuksi käyttäjälle lähetetään tieto onnistuneesta maksutapahtumasta. [4]

Tilitiedot ja PIN-koodi lähetetään siis eri viestissä, joka lisää järjestelmän luotettavuutta. Lisäksi järjestelmässä on usein määritelty aika jonka kuluessa käyttäjän on kuitattava järjestelmästä tullut viesti PIN-koodilla. Muutoin maksutapahtuma keskeytetään. Jos käyttäjällä on käytössä DinaCard-maksukortti asiakkaan tunnistus ta-

pahtuu suoraan puhelinverkon kautta. Asiakas antaa tunnistuksessa puhelimensa PIN-koodin, jonka jälkeen järjestelmä lähettää kyselyn suoraan puhelinoperaattorille. Operaattori vahvistaa ostajan henkilöllisyyden. Etuna on, ettei käyttäjän tarvitse muistaa useampia koodeja, vaan yksi riittää. [4] [5]

4.4 Internetpohjaiset järjestelmät

Internetpohjainen järjestelmä on etämaksamis- ja tilipohjainen-järjestelmä. Käyttäjä ottaa mobiililaitteellaan yhteyden kauppapaikan portaaliin joka toimii verkossa. Viestit kulkevat internet-protokollan päällä. [4]

Maksutapahtumassa on kaksi vaihetta jotka muistuttavat suuresti edellä esiteltyä tekstiviesteillä maksamista. Ensimmäisessä vaiheessa käyttäjä ottaa yhteyden palvelimeen ja kirjautuu sisään. Tämän jälkeen käyttäjä valitsee ostettavat tuotteet ja valitsee maksutavan(esim. DinaCard-maksukortti) ja näppäilee oman puhelinnumeron palvelimeen. Palvelin lähettää ensin pyynnön puhelinoperaattorille ja varmentaa henkilötiedot ja luottotiedot pankista. Jos tiedot pitivät paikkansa, järjestelmä pyytää käyttäjältä PIN-koodia jolla ostotapahtuma vahvistetaan. [4] [5]

Jotta tällainen järjestelmä toimisi, on puhelinoperaattorin ja koko maan puhelinverkon tuettava sitä. Kaikissa maissa ja kaikkien operaattoreiden verkoissa tekniikka ei ainakaan vielä toimi. Nopealla verkkoyhteydellä varustetulla kännykällä palvelun käyttäminen on kuitenkin helppoa. Asiakkaan tunnistus toimii useimmiten juuri puhelinoperaattorin kautta SIM-kortin avulla ja asiakkaan PIN-koodilla. DinaCard-järjestelmän lisäksi isot luottokunnat, esimerkiksi Visa, on kehittänyt vastaavan maksujärjestelmän. [1]

Lisäksi on olemassa esimerkiksi mobiililompakoita jotka käyttävät verkkoyhteyttä hyväkseen. Yhteyden kautta kuluttaja voi esimerkiksi ladata sähköistä rahaa laitteelleen. Aiheesta enemmän luvussa 4.5

4.5 Mobiililompakko

Mobiililompakko on maailmanlaajuisesti käytetyin mobiilimaksamisen järjestelmätyyppi. Mobiililompakko on, ainakin yleensä, POS-järjestelmä joka perustuu yleensä tilin käyttöön, johon talletettuja varoja kuluttaja käyttää mobiililompakon avulla. Tilin voi tarjota luottokunta, pankki tai muu luotettavaksi tiedetty taho. Lähes kaikilla suurilla luottokorttiyhtiöillä on oma mobiililompakkojärjestelmänsä. Esimerkiksi Mastecardilla on serveripohjainen järjestelmä. [8] [9] [10]

Lompakoita on kahta päätyyppiä **online-lompakko** ja **offline-lompakko**. Näistä ensimmäisen toiminta perustuu tietoverkon käyttöön. Laite on siis jatkuvasti ver-

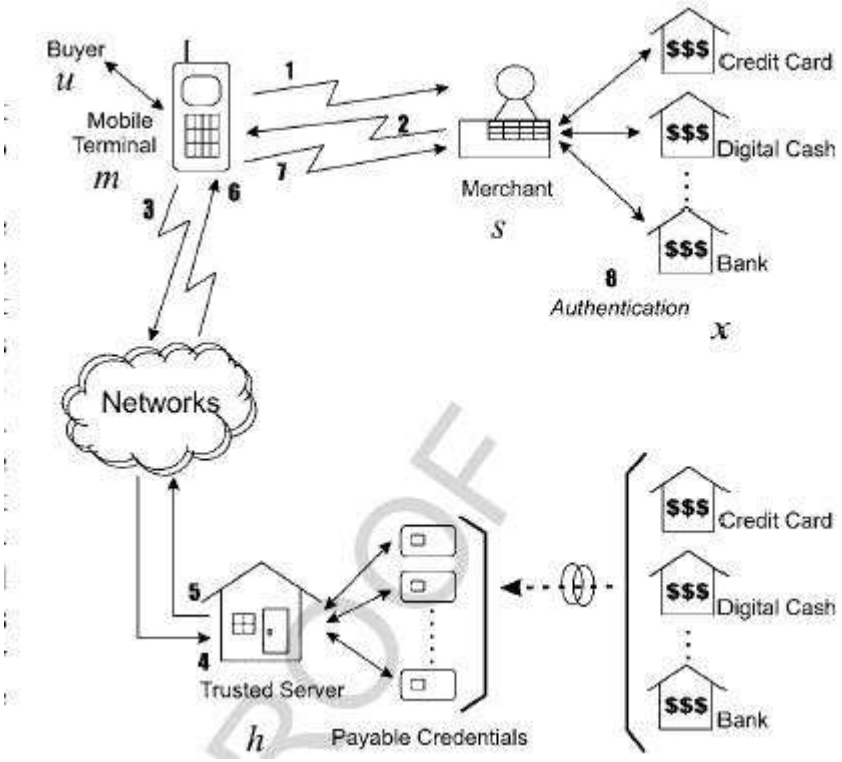
Kuva 2: Sähköisen lompakon prototyyppi. [8]

kon kautta yhteydessä järjestelmän palvelimeen IP-protokollalla. Kauppiaan ja ja kuluttajan välinen liikenne tosin hoidetaan lyhyen kantaman tekniikalla, esimerkiksi IrDA- tai Bluetooth-yhteydellä Tällainen järjestelmä on kuvattu kuvassa 3. [8]

Offline-lompakko toimii jonkin lyhyen kantaman tiedonsiirtoprotokollan päällä ja ottaa sen avulla yhteyden myyjän maksupäätteeseen. Laite ei siis ole jatkuvassa yhteydessä järjestelmän palvelimeen, vaan kuluttaja esimerkiksi käyttää älykortilla varustettua laitetta maksamiseen. Laiteen älykortille on talletettu sähköistä rahaa tai maksamiseen tarvittavat tiedot, esimerkiksi maksukortin tiedot jotka ostaja lähettää myyjälle. [8]

Euroopan yhteisön rahoittama CAFE-projekti kehitti prototyypin mobiililaitteesta, jota voidaan käyttää elektronisena lompakkona. Laite oli offline-lompakko eli siinä ei ollut internetyhteyttä, eli sillä ei voi esimerkiksi ladata sähköistä rahaa suoraan pankin palvelimelta. Laite on esitelty kuvassa 2 Laite oli varustettu älykortinlukijalla, näppäimistöllä ja pienellä näytöllä. Yhteyttä maksupäätteeseen laite piti infrapunayhteyden kautta. [8]

Eräs suosittu tapa toteuttaa järjestelmä on käyttää NFC-teknologiaa. Tekniikan etu on siinä, että se yhdistää maksulaitteen ja puhelimen, eli käyttäjälle riittää yksi



Kuva 3: Online lompakon järjestelmäkuva. [8]

laite. Kyseisestä tekniikasta kerron lisää luvussa 6.4.Tekniikan suuri etu, esimerkiksi CAFE-laitteeseen verrattuna, on se ettei käyttäjän tarvitse kantaa useita eri laitteita mukanaan, vaan matkapuhelin hoitaa kaiken. [8]

4.6 P2P-maksamisjärjestelmä

P2P-järjestelmässä (Peer to Peer) asiakas ottaa omalla mobiililaitteellaan suoraan yhteyden myyjän mobiililaiteeseen. Teknisesti yhteys tapahtuu Bluetooth-yhteyden avulla. Ostaja ja myyjä ovat siis suorassa yhteydessä keskenään maksamisjärjestelmän tarjotessa ainoastaan rajapinnan maksamiselle. Järjestelmää voidaan tältä osin pitää POS-järjestelmänä. Kummankin tahon on kuitenkin oltava rekisteröityneenä järjestelmässä, toisin kuin perinteisessä POS-järjestelmässä. [9] [10]

Järjestelmää on tutkittu ja kehitetty San Josen yliopistossa vuodesta 2004 saakka. Tutkimuksen tarkoituksena on ollut kehittää kevyt protokolla, joka mahdollistaa luotettavan rajapinnan maksavan ja myyjän välille Bluetooth-verkon avulla. [9] [10]

Protokolla tarjoaa seuraavat toiminnot: [9] [10]

- P2P osapuolten haku(P2P party discovery)

- P2P istunnon hallinnointi(P2P session management)
- P2P maksutapahtuman hallinnointi(P2P payment management)
- Maksutilien hallinnointi(Acount management)
- Maksutapahtumien vuorottaminen(Payment scheduling)
- Maksunsaajien hallinnointi(Payee management)

Kaikki edellä mainitut toiminnot siis toimivat Bluetooth-verkossa, Bluetooth-protokollapinon päällä. Protokollan toiminnasta ja sen myötä operaatioista tarkemmin luvussa 6.3. [9] [10]

Edellä esiteltyjen ominaisuuksien lisäksi artikkeleissa esitellyssä järjestelmissä käyttäjillä on mahdollisuus muokata ja tarkastella asiakastietojaan tietokoneella verkon kautta. Käyttäjä voi muuttaa tilin käyttörajaa, selailla ostohistoriaansa, muuttaa tunnuksiaan ja tarkastella autentikointi- ja salaustietojaan. Lisäksi maksaminen ja maksutapahtumien vuorottamisen hallinnointi onnistuu myös verkosta käsin. Ostajan lisäksi myös myyjä voi hallinnoida samoja asioita verkon kautta. Eli käyttäjä voi tehdä verkon kautta lähes samat operaatiot, kuin mobiililaiteellaankin. [9] [10]

Ensimmäinen askel järjestelmän käytössä on osapuolten kirjautuminen maksujärjestelmään. Kun kirjautuminen onnistuu asiakas lähettää palvelupyynnön(service request). Järjestelmän tarjoamat palvelut esittelin aiemmin tässä luvussa. [9] [10]

Seuraavaksi asiakkaan laite etsii Bluetooth-protokollan avulla laitteen joka tarjoaa haluttua palvelua. Operaatio tapahtuu Bluetoothin SDP-protokollan avulla. Aiheesta lisää luvussa 6.3. [9] [10]

Seuraava vaihe on autentikointi. Asiakkaan tunnistaminen ja autentikointi on hyvin tärkeää, koska kyse rahaliikenteestä. P2P-järjestelmissä käytetään salausavaimiin perustuvaa autentikointimenetelmää. Osapuolet saavat salausavaimen maksamisjärjestelmästä kirjautumisen yhteydessä avaimen avulla osapuolet tunnistetaan. Samaa avainta voidaan käyttää useampaan kertaan eikä sitä tarvitse joka kerta uusia. Salausavaimiin perustuviin menetelmiin perehdytään hieman tarkemmin luvussa 7.3. [9] [10]

Kun yhteys on muodostettu, haluttu palvelu on löytynyt ja osapuolet on tunnistettu. Maksajan tarvitsee vain näppäillä haluttu summa ja vahvistaa maksutapahtuma. Myyjä tarkistaa maksajan tilin saldon ja jos se on riittävä rahasumma veloitetaan ostajan tililtä, ja maksutapahtuma kuitataan. Jos tilillä ei ole riittävästi käytettävissä olevia varoja, lähetetään siitä viesti ostajalle jolloin hän voi joko näppäillä uuden summan tai lopettaa maksutapahtuman. [9] [10]

5 Maksamisjärjestelmien arkkitehtuurit

Luvussa käsittelen mobiilimaksamisjärjestelmien mahdollisia arkkitehtuureja, eli millaisista komponenteista järjestelmä koostuu ja miten arkkitehtuuri vaikuttaa järjestelmän käyttöön ja toimintaan.

5.1 Perinteinen asiakas-palvelin -järjestelmän arkkitehtuuri

Perinteinen palvelinpohjainen-järjestelmässä maksaja ottaa yhteyden mobiililaiteellaan maksamisjärjestelmään. Kuten verkkopalvelussakin, asiakas lähettää palvelimelle pyyntöjä, joihin palvelin vastaa vasteilla. Asiakas asioi palvelimen kanssa, eikä suoraan toisen asiakkaan kanssa.

Tyypillinen palvelin pohjainen järjestelmä on luvussa 4.5 esitelty mobiililompakko. Asiakas voi ladata esimerkiksi sähköistä rahaa lompakkoonsa. Edellä mainittu arkkitehtuuri on esitelty kuvassa 3

Delić ja Vukašinović esittelevät artikkelissaan [4] erään järjestelmän arkkitehtuurin, joka on esitetty kuvassa 4 Kyseinen arkkitehtuuri käyttää luvussa 4 ja sen aliluvuissa esiteltyä DinaCard-maksukorttia, eikä ole mobiililompakko. Järjestelmä on tilipohjainen, eli asiakkaan on järjestelmään rekisteröitymisen yhteydessä avattava tili, josta ostokset maksetaan. [4]

Järjestelmässä on kaksi osaa: järjestelmän ydin(core) ja maksukorttien keskus, joka lyhennetään NCPC(National center for payment cards). Käyttäjät ottavat mobiililaiteillaan yhteyden järjestelmän ydin-osaan joka on yhteydessä asiakkaiden prepaid-tileihin ja NCPC-yksikköön ISO 8583-rajapinnan välityksellä. [4]

Järjestelmän ydin on järjestelmän ”aivot”. Ytimen tehtävät ovat: [4]

- Hoitaa käyttäjähallinnan
- Hallinnoi rahaliikennettä
- Hallinnoi sovelluksien palveluntarjoajia
- Mahdollistaa kommunikoinnin eri sovelluksien palveluntarjoajien välillä
- Hoitaa käyttäjien autentikoinnin ja tunnistuksen
- Hoitaa kommunikoinnin NCPC:n tai muun rahoituslaitoksen kanssa
- Välittää ja ylläpitää verkosta tulevia pyyntöjä järjestelmän eri kerrosten välillä
- Hoitaa raportoinnin

Mobiililaitteen ja ytimen välinen yhteys on salattu, koska käyttäjä lähettää järjestelmään salasana, käyttäjä- ja tilitietoja. Kuten kuvasta 4 selviää arkkitehtuuri sopii kaikille kolmelle luvussa 4 esittelyille järjestelmätyypeille; tekstiviesti-, internet- ja POS-järjestelmälle. Riippuen järjestelmän tyypistä asiakkaan ja järjestelmän välillä liikkuvat viestit ovat hieman erilaisia, mutta asiakkaan ja ostettavan tuotteen tiedot ovat pakollisia riippumatta järjestelmästä. Lisäksi esimerkiksi POS-järjestelmässä tarvitaan maksupäätteen eli terminaalin tunnus. Lisäksi viestissä voidaan välittää tilin tunnus ja tilin tyyppi, koska asiakkaalla voi olla useita erilaisia tilejä järjestelmässä. [4]

ISO 8583-rajapinnan välityksellä järjestelmä on yhteydessä esimerkiksi johonkin maksukorttijärjestelmään, joka ylläpitää tietoja asiakkaan maksukorteista. Keskus on yhteydessä kauppiaan pankkitilille, johon se siirtää rahat maksun suorittamisen jälkeen asiakkaan maksutililtä. Ytimen ja NCPC:n välillä liikkuva tieto on aina samaa riippumatta siitä millä kommunikointitekniikalla asiakas otti yhteyden järjestelmään. Rajapinnassa välitetään maksukortin tiedot, pankin tunnus, tilauksen määrä ja palvelun ja myyjän määrittävä kauppiaan kategoriakoodi eli MCC(merchant catergory code). [4]

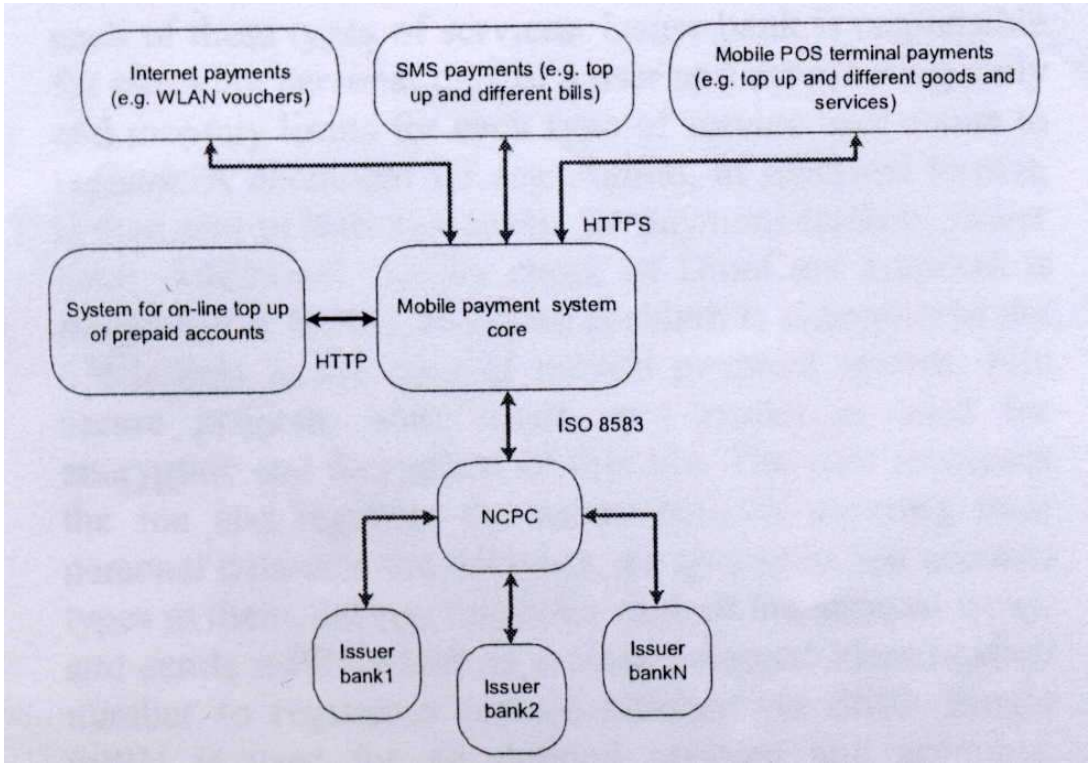
Järjestelmällä on nyt tarvittavat tiedot maksutapahtuman suorittamiseksi. Haluttu summa veloitetaan asiakkaan järjestelmään avatulta tililtä ja siirretään kauppiaan pankkitilille. [4] Käyttäjän tunnistus ja maksutapahtumasta keroin jo luvussa 4, joten siihen en enää palaa.

5.2 P2P-järjestelmän arkkitehtuuri

P2P-järjestelmän arkkitehtuurimalli on esitelty kuvassa 5. Kuvasta selviää, ettei järjestelmä juurikaan poikkea kuvassa 5 esitellystä mallista. Tässäkin järjestelmässä on yksiköt jotka hoitavat käyttäjähallinnan ja käyttäjien tunnistuksen. Ainoa ero luvussa 5.1 esiteltyyn malliin on, että maksaja ja myyjä ovat suorassa yhteydessä toisiinsa Bluetooth- verkon avulla ja kumpikin osapuoli voi olla palvelin tai asiakas. [4] [9] [10]

Järjestelmä koostuu neljästä osasta: [9] [10]

- **Mobiililaite(Mobile client):** Mobiililaiteessa on J2ME pohjainen mobiili P2P-ohjelmisto. Lisäksi laite pystyy ottamaan internetyhteyden HTTPS-protokollan avulla.
- **Väliohjelmisto(Middleware):** Sisältää Apache Tomcat verkkopalvelimen, joka tukee langatonta internettiä ja muita väliohjelmistoja kuten JSP(Java Server page) ja Java servetit



Kuva 4: Perinteinen mobiilimaksamisjärjestelmän arkkitehtuurikuva. [4]

- **Tietokantapalvelin(Payment database server):** Ylläpitää järjestelmän tietokantaa ja kommunikoi tietokantaohjelmiston välityksellä järjestelmän palvelimen ja käyttäjien kanssa. Tietokantaan tallennetaan järjestelmän kannalta kriittiset tiedot esimerkiksi käyttäjien henkilö- ja tilitiedot

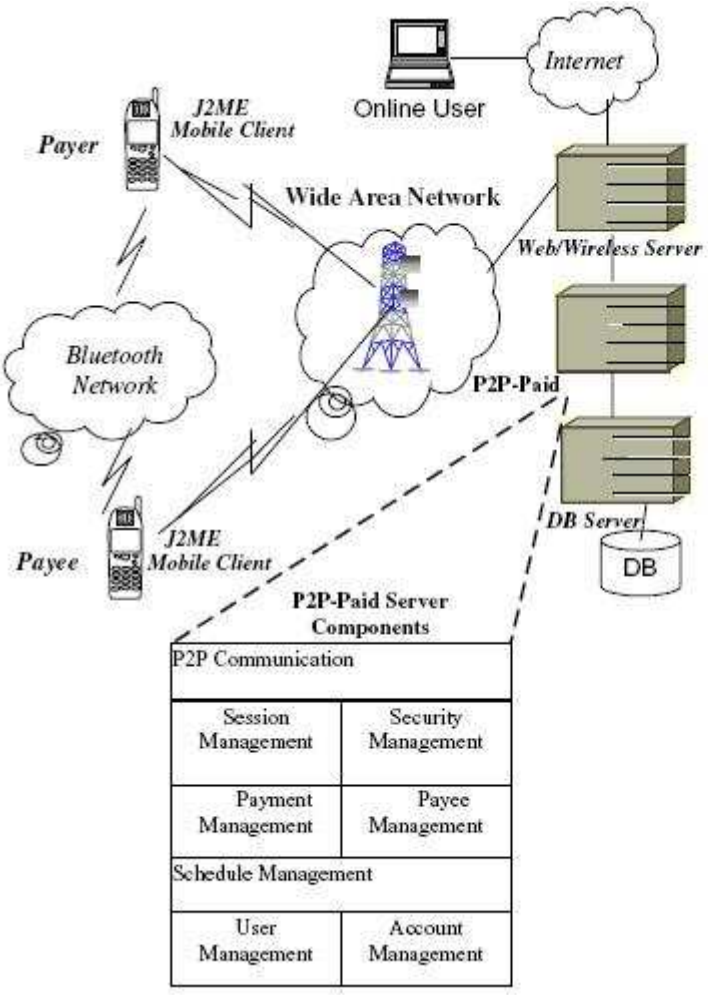
- **Järjestelmän palvelin(P2P-server):** Palvelin on kuten edellä esitellyn järjestelmän ydin-osa. Palvelin hallinnoi järjestelmän toimintoja ja keskustelee middleware-ohjelmiston kautta kautta käyttäjän mobiililaitteen kanssa.

Lisäksi käyttäjän mobiililaiteessa ja järjestelmän palvelimella on muutamia toiminnallisia osia.

Mobiililaiteen ohjelmisto sisältää seuraavat toiminnallisuudet: [9] [10]

- **Käyttöliittymä(User interface):** Tarjoaa käyttäjälle rajapinnan, jonka avulla hän voi lähettää pyyntöjä(request) ja näyttää käyttäjälle järjestelmästä tulleet vastaukset.

- **P2P-palvelumoduuli (P2P service module):** Tarjoaa yhteyden kahden käyttäjän (ostajan ja myyjän) välille yhteyden jonka kautta maksutapahtuma suorite-



Kuva 5: P2P-mobiilimaksamisjärjestelmän arkkitehtuurikuva. [9]

taan. Yhteys toimii Bluetooth-tekniikan päällä. Protokollasta kerroin jo enemmän luvussa 4.6.

- **Tietoturvamoduuli(Mobile security module):** Moduuli tarjoaa perus tietoturvatoiminnot, esimerkiksi autentikoinnin ja äänen tunnistuksen. Tunnistusmenetelmistä enemmän luvussa **??**.

- **Maksamismoduuli(Mobile payment module):** Moduuli pitää yllä yhteyttä asiakkaan mobiililaitteen ja maksupalvelimen välillä, langattoman internetin ylitse.

Järjestelmän palvelimen toiminnalliset osat hoitavat suurelta osin luvussa 4.6 esitellyt järjestelmän tarjoamat palvelut. Järjestelmän palvelimessa on seuraavat moduulit: [9] [10]

- **P2P-viestintä (P2P communication):** Mahdollistaa yhteyden asiakkaan ja palvelimen välillä, alla toimivasta tekniikasta riippumatta.

- **Käyttäjähallinta(User management):** Hallinnoi käyttäjien rekisteröitymistä järjestelmään ja ylläpitää käyttäjärekisteriä. Järjestelmässä voi olla kahdenlaisia käyttäjiä: peruskäyttäjiä ja ylläpitäjiä, joista tämä moduuli pitää kirjaa.

- **Tilihallinta(Account management):** Hallinnoin ja ylläpitää järjestelmässä olevien käyttäjien tilien tietoja.

- **Maksuhallinta(Payment management):** Hallinnoi ja pitää kirjaa kaikista järjestelmässä tapahtuvasta maksuliikenteestä.

- **Maksutapahtumien vuorottamisen hallinta(Schedule management):** Moduuli mahdollistaa useamman kuin yhden yhtäaikaisen maksutapahtuman vuorottamisen ja vuorottamistietojen ylläpitäminen. Moduulin operaatioita ovat vuorottamistietojen lisääminen päivittäminen ja poisto

- **Maksunsaajien hallinta(Payee management):** Hallinnoi ja ylläpitää tietoja kaikista maksunsaajista. Moduuli osaa lisätä tietoja, päivittää tietoja ja tuhota tietoja.

- **Sessioiden hallinta(Session management):** Hallinnoi järjestelmän sessioita

- **Tieturvan hallinta(Security management):** Hallinnoi järjestelmän tietoturvaa. Toiminnot ovat :käyttäjien tunnistus ja autentikointi, salausavainten hallinta ja äänen tunnistus. Aiheesta lisää luvussa 7.

6 Maksamisjärjestelmissä käytettävät viestintäteknologiat

uvussa esitellään erilaisia mobiilimaksamisessa käytettäviä tekniikoita. Jokaisesta tekniikasta on listattu hyviä ja huonoja puolia, nimenomaan käytön ja käyttäjän kannalta.

6.1 Toisen sukupolven kännykkäverkot

Toisen sukupolven matkapuhelinverkot ovat GSM- ja CDMA-verkkoja. GSM-puhelimien käyttämät taajuudet ovat 900 MHz ja 1800 MHz. CDMA-tekniikan käyttämä taajuus on puolestaan 1900 MHz. GSM-verkon tiedonsiirtonopeus on 9.6 kbps ja CDMA-verkon nopeus on 14.4 kbps. Tämä nopeus riittää yleisesti maksamiseen hyvin. Ongelmia saattaa syntyä, jos järjestelmää käyttää tavallista useampi käyttäjä esimerkiksi jokin juhlapäivä jolloin useat ihmiset haluaisivat käyttää järjestelmää samanaikaisesti. [32]

Itse maksutapahtuma tapahtuu soittamalla tai lähettämällä tekstiviesti palveluntarjoajan numeroon. Soitettaessa palveluntarjoajan numeroon laskutus tapahtuu seuraavan puhelinlaskun yhteydessä. Jyväskylän yliopistollakin on virvoitusjuoma-automaatteja jolla juoman voi ostaa soittamalla myyjän numeroon. Järjestelmä on siis helppokäyttöinen. [32]

Jos maksaminen tapahtuu tekstiviestillä, on operaatio hieman edellistä monimutkaisempi. Käyttäjä lähettää tarvittavat tiedot järjestelmään tekstiviestinä. Tekstiviestillä toimiviin järjestelmiin ja niillä maksamiseen paneuduin jo luvussa 4.3, joten tässä en siitä kerro enempää. Esimerkkeinä tekstiviesteillä toimivista järjestelmistä voi mainita Espanjassa toimivan Mobipay-järjestelmän. [32]

Teknologiassa on kuitenkin useita ongelmia, jotka estävät sen yleistymistä. Ensinnäkin maksutapahtuma vie melko pitkään joten ruuhkaisella kaupan kassalla tavan käytettävyys ei ole paras mahdollinen. [32]

Lisäksi kuten jo luvussa 4 selitin järjestelmän toiminta on riippuvainen puhelinoperaattorin kantaverkosta. Käyttäjä tunnistetaan SIM-kortin avulla ja maksujärjestelmä ja operaattorin puhelinverkkoverkko ovat yhteydessä keskenään. Käytännössä tämä tarkoittaa ettei maksujärjestelmä toimi kaikkien operaattorien verkoissa. [32]

Viimeisenä ongelmana on se, että maksutapahtuma maksaa. Yleensä järjestelmällä ostettavat tuotteet ovat kohtuullisen halpoja, tästä syystä maksutapahtumasta peritty maksu saattaa olla suurempi kuin itse ostettavan tuotteen hinta. [32]

Loppuyhteenvetona voidaankin sanoa, että tekniikan tiedonsiirtonopeus riittää maksamisjärjestelmän tarpeisiin kohtuullisesti. Varsinkin puhelulla maksaminen on

helppoa ja maksu hoidetaan tavallisen puhelinlaskun ohessa. [32]

Lisäksi tietoturva on riittävän hyvä pienten ostosten tekemiseen. SIM-kortin ja PIN-koodin yhdistelmä on varma tunnistuskeino. Lisää aiheesta luvussa **??**. Koska palvelun käyttäjä syöttää henkilötietonsa ja esimerkiksi luottokortin tiedot verkossa vain kerran rekisteröityessään järjestelmään, ei tietoja tarvitse lähettää joka kerta maksettaessa, joka pienentää tietoturvariskiä. [32]

Tekniikan ongelmana on maksamisen hitaus, joka huonontaa käytettävyyttä. Lisäksi tekniikka ei toimi kaikkialla, eikä kaikkien operaattoreiden verkoissa. Viimeisenä ongelmana maksutapahtuma itsessään on melko kallis verrattuna ostattavien tuotteiden hintaan. [32]

6.2 2.5G- ja 3G-verkoissa käytetyt tekniikat

Mobiiliteknologian seuraavat sukupolvet ovat 2.5G ja 3G. Teknologioissa käytetään pakettikytkentäisiä verkkoja. Tiedonsiirtonopeus ja verkon kapasiteetti on suurempi kuin GSM-tekniikassa. Suuremman kapasiteetin ansiosta puhelimella voidaan lähettää muitakin viestejä kuin tekstiviestejä(esimerkiksi WAP-viestit).

Pakettikytkentäinen mobiilipuhelinverkko toimii hieman kuin tietokoneverkko. Tieto pakataan ennen lähetystä pakettiin ja se löytää perille osoitteen perusteella. Paketin kulkureitti lähettäjältä vastaanottajalle ei ole rajattu kuten vanhoissa piirikytkentäisissä puhelinverkoissa. Lisäksi laskutuksessa huomioidaan lähetetty data, eikä käytetty aika. [32]

2.5G käyttää GPRS- ja EDGE-tekniikkaa. Tekniikoita käytetään perinteisessä GSM-verkossa joten käytetyt taajuudet ovat samoja kuin 2G:sä. Tekniikoiden GPRS-tekniikan tiedonsiirtonopeus on 30-40 kbps. EDGE:n nopeus on parhaimmillaan 150-200 kbps. [32]

Myös jo edellä mainitulla CDMA-tekniikalla on 2.5G-versio(CDMA 2000 1xRTT), joka käyttää pakettikytkentäistä tekniikkaa. Tekniikan maksimi tiedonsiirtonopeus on 144kbps. [32]

Nykyisin vauhdilla yleistyvä 3G-tekniikka puolestaan käyttää UMTS-tekniikkaa ja paranneltua CDMA-tekniikkaa. Tiedonsiirtonopeus UMTS-tekniikassa on 144kbps-2Mbps ja CDMA2000 1xEV-tekniikassa 700kbps-3.09Mbps. [32]

Tekniikoiden etuna on nopeus ja kapasiteetti. Maksamiseen kuitenkaan verkkojen koko kapasiteettia ei tarvita, vaan edellä esitelty 2G-tekniikkakin riittää maksuliikenteen tarpeisiin kohtuullisen hyvin. [32]

3G-tekniikan suurin etu on se, että verkon nopeuden takia käyttäjä pystyy tilaamaan isopakin tiedostoja. Tekniikalla maksettavat palvelut ovatkin yleensä puhelinoperaattorilta tai muilta palveluntarjoajilta tilattavat maksulliset sisällöt, esi-

merkiksi soittoäänet ja videoclipit tai jopa kokonaiset elokuvat ja tv-sarjat. Käyttäjä maksaa tilaamansa lisäpalvelut puhelinlaskunsa ohessa. Palveluntarjoajalla ja puhelinoperaattorilla on oltava keskinäinen sopimus, jotta tämä on mahdollista. [32]

Palvelun käyttö on helppoa: yksinkertaisesti käyttäjä valitsee haluamansa palvelut puhelimensa valikosta. Tunnistus tapahtuu SIM-kortin ja mahdollisesti PIN-koodin avulla. PIN-koodi soveltuu tunnistukseen hyvin, koska usein ostettavat tuotteet ovat halpoja. [32]

Palvelun käyttö on periaatteessa ilmaista, eli käyttäjä maksaa vain tilaamistaan sisällöistä. Tosin osa palveluista ja verkkosivuista saattavat veloittaa ladatusta datasta maksun datan määrän mukaan. [32]

Palvelun käyttöön liittyvät samanlaisia ongelmia kuin edellä esiteltyyn 2G-tekniikkaan. Palvelut eivät välttämättä toimi kaikkialla, vaan tarvitsevat tietyn operaattorin verkon toimiakseen. Katvealueilla ja esimerkiksi vieraan operaattorien verkoissa palvelu ei välttämättä toimi. Lisäksi operaattorilla ja palveluntarjoajalla täyttyy olla keskinäinen sopimus jotta laskutus toimii. [32]

Maailmalla toimii useita järjestelmiä jolla matkapuhelimien käyttäjät voivat tilata lisäpalveluita puhelimeensa. Tärkeimpiä järjestelmät jotka mahdollistavat laskutuksen puhelinlaskun yhteydessä ovat: Vodafone m-Pay, Simpay ja Japanissa toimiva DoCoMo-järjestelmä. Suomessakin operaattorit tarjoavat käyttäjilleen puhelinliittymäänsä erikoispalveluita, jotka käyttäjä maksaa puhelinlaskunsa ohessa. Kuten jo mainitsin lisämaksut ovat kohtuullisen pieniä. Kalliiden tuotteiden ostamiseen tekniikka ei sovellu, koska tämä paisuttaisi puhelinlaskua liikaa ja tietoturvakin asettaa rajoituksia. Halpojen digitaalisien palvelujen ja sisältöjen maksamiseen tekniikka soveltuu hyvin. [32]

6.3 Bluetooth

Bluetooth on infrapunayhteyden ohella toinen nykyisten kännyköiden lyhyen kantaman yhteystekniikka. Toisin kuin edellä esitelty infrapuna, Bluetooth toimii radiosignaalilla, joten puhelimen ja vastaanottimen ei tarvitse olla näköetäisyydellä. Laitteiden ei myöskään tarvitse olla lähekkäin, vaan Bluetoothin kantama on parhaimmillaan jopa sata metriä. Toinen hyvä puoli infrapunaan verrattuna on se, että lähes kaikissa uusissa puhelimissa on Bluetooth-yhteys vakiona. Kuten infrapunaa Bluetoothia käytetään enimmäkseen POS-järjestelmissä reaaliaikaiseen maksamiseen, jonka esittelin luvussa 4.2 ja luvussa 4.6 esitellyssä P2P-järjestelmässä. Järjestelmän arkkitehtuurin esittelin luvussa 5.2 [10]

Käytön kannalta merkittävin ero infrapunaan verrattuna on, että Bluetooth-laite

etsi ympäristöstä kaikki palveluntarjoajat, toisin kuin infrapunassa jossa laite lopettaa haun heti kun on löytänyt yhden infrapuna-laitteen lähistöllä.

Tutkielmassani en keskity juurikaan Bluetoothin teknisempiin seikkoihin, vaan keskityn tekniikkaan tutkielmassa esitellyn P2P- maksujärjestelmän kannalta. Kuten luvussa 5.2 mainitsen järjestelmän toiminnot toimivat Bluetooth-protokollapinon päällä. [9] [10]

Bluetoothin tarkoituksena on ollut kehittää halpa, yksinkertainen ja vähän energiaa tarvitseva lyhyen kantaman kommunikointiteknologia, joka toimii radioaalloilla. Tekniikassa on mahdollista välittää ääntä ja dataa. Teoreettinen tiedonsiirtonopeus on 1Mbps. [2] [3] [30] [29]

Bluetooth toimii taajuudella 2.4 Ghz joka luetaan mikrotaajuusalueelle, aluetta kutsutaan ISM-taajuusalueeksi, joka on vapaasti käytössä. Tämä tarkoittaa etteivät taajuusalueella operoivat laitteet tarvitse erillistä lupaa toimintaan. Lisäksi Bluetooth-laitteet toimivat taajuusalueella jolla esimerkiksi radiolaitteet eivät häiritse laitteiden toimintaa. Toisaalta korkeiden taajuuksien ongelmana on suuri absorboituminen. [2] [3] [30] [29]

Koska Bluetooth-laiteet jaetaan kolmeen luokkaan kantaman ja lähetystehon perusteella. Ensimmäisen luokan laitteiden kantama on noin 100 metriä, toisen noin 20 metriä ja kolmannen luokan laitteiden kantama on noin kymmenen metriä. Toisaalta Bluetooth-laitteille on myös määrätty minimi etäisyys, 10 cm. Tämän lähempänä olevat laitteet häiritsevät toisiaan ja saavat aikaan lähettimien saturoitumisen, eli laite menettää hetkellisesti kykynsä toimia. [2] [3] [30] [29]

Edellä esitetyt luvut ovat vain suuntaa-antavia, todellinen kantama määräytyy ympäristön, olosuhteiden ja laitteiden asennosta toisiaan kohtaan. Kantomatka määritellään aina heikompitehoisen laitteen mukaan. Yleisin laitetyyppi ovat 3-luokan laitteet. Luokaan kuuluvat esimerkiksi perinteiset matkapuhelimet. [2] [3] [30] [29]

Bluetooth-laite voi muodostaa yhteyden yhden palvelinlaiteen kanssa(Point-to-Point), tai verkon useamman laitteen välille(Point-to-Multipoint). Kummassakin tapauksessa yhden laiteen on oltava palveluntarjoaja(master) johon muut laitteet ottavat yhteyttä(slave) Bluetooth-tekniikassa laite joi kommunikoida ainoastaan masterlaitteen kanssa. Huomioitavaa on, kuitenkin että Symbian OS käyttöjärjestelmässä on mahdollista toteuttaa vain Point-to-Point-yhteys. [2] [3] [30] [29]

Bluetooth-laiteet voivat muodostaa maksimissaan kahdeksan laitteen verkon jossa yksi laite toimii masterina ja muut slave-laitteina. Tällaista kahdeksan laitteen verkkoa kutsutaan Piconet-verkoksi. Lisäksi Bluetooth mahdollistaa useamman tällaisen verkon yhdistämisen isommaksi verkoksi, jossa yksi laite toimii palvelimena ja asiakkaana toisessa verkossa(Scatternet). [2] [3] [30] [29]

Seuraavaksi esittelen P2P-maksamisjärjestelmän yhteydenmuodostuksen. Koska järjestelmä käyttää Bluetoothin SDP-protokollaa(Service discovery protocol), ei palvelun haku ja yhteyden muodostus eroa juurikaan perinteisestä Bluetoothin yhteyden muodostuksesta. [2] [3] [30] [29]

Koska tekniikassa laite voi toimia vuorotellen asiakkaana ja palvelimena sopii se hyvin P2P-protokollan tarpeisiin. Jokainen laite joka tarjoaa jotain resursseja on palvelin ja laite joka käyttää resursseja on asiakas. Bluetooth-laitteiden tarjoamat palvelut ja verkon resurssit vaihtelevat jatkuvasti. Tämän takia tekniikassa on oltava jokin tapa jolla asiakas voi löytää uudet lähistöllä olevat palvelut. Tarkoitukseen käytetään SDP-protokollaa. [2] [3] [30] [29]

Bluetooth-laite pitääkin yllä tietokantaa tarjoamistaan palveluista. Palvelua tarjoava laite ”mainostaa” tarjoamiaan palvelujaan lähistöllä oleville asiakaslaitteille. Asiakas suorittaa haun jolla hän etsii lähistöllä olevat Bluetooth-laitteet. Kun haluttu laite löytyy suorittaa asiakas haun palvelimen tarjoamista palveluista. Tämän hoitaa edellä mainittu SDP-protokolla. [2] [3] [30] [29]

Tekniikan huonoimpana puolena on Bluetoothin kankea yhteydenmuodostus. Bluethooth-laite etsii kaikki lähellä olevat Bluetooth-laitteet, hakee niiden palvelut ja kytkeytyy haluttuun palveluun. Toimenpiteeseen saattaa mennä kymmeniä sekunteja, eli ostoksien maksamiseen voi hyvinkin mennä minuutteja. Toinen seikka, mikä arveluttaa, on Bluetooth-signaalin liiankin pitkä kantama. Paketti voidaan, ainakin teoriassa, kaapata ja esimerkiksi luottokortin tiedot joutuvat vääriin käsiin. [2] [3] [30] [32] [29]

6.4 NFC

NFC on Sonyn ja Philipsin yhdessä kehittämä lyhyen kantaman maksamis- ja tunnistustekniikka. Yksinkertaisesti sanottuna sen avulla mobiililaiteeseen voidaan asettaa luottokortti Se toimii taajuudella 13.56 MHz, sen tiedonsiirtonopeus on 212 kbps. Merkittävin ero muihin tekniikoihin on, että tekniikan kantomatka on hyvin lyhyt. NFC-laitteen on siis oltava todella lähellä lukulaitetta. [32]

NFC-laite siis sisältää luottokortin tapaisen sirukortin, joka sisältää samat tiedot kuin maksukortti. Usealla puhelinvalmistajalla on olemassa puhelimiin asennettavia NFC-laitteita. NFC:n avulla puhelimeen voi asettaa perinteisen SIM-kortin rinnalle luottokortin tiedot sisältävän maksukortin, joka hoitaa maksuliikenteen. Käyttäjän tarvitsee ainoastaan heilauttaa puhelimessa olevaa älykorttia lukijan edessä. Lukija rekisteröi maksun reaaliajassa. [32]

Vuonna 2005 käytössä oli kolme merkittävää maksujärjestelmää: PayPass, Fe-

liCa ja Nokian NFC shell-tekniikka. Kaikkien järjestelmien toimintaperiaate on kutakuinkin samanlainen. PayPass on Mastercard-luottokortin kanssa yhteensopiva järjestelmä. PayPass on laajasti käytössä Yhdysvalloissa. Ongelmana järjestelmässä on, että se toimii vain Mastercard-luottokorttien ja Motorolan puhelimien kanssa. Yhdysvalloissa Motorola onkin asentanut Paypass järjestelmän kokeilumielessä puhelimiinsa. [22]

Toinen merkittävä järjestelmä on Sonyn kehittämä FeliCa, joka on käytössä pääasiassa Aasiassa. Ennen järjestelmän käyttöä kuluttajan on ladattava verkosta tarvittava ohjelma laitteeseen. Ohjelman avulla käyttäjä voi myös ladata rahaa älykortilleen verkon kautta. [23]

Nokia julkaisi markkinoiden ensimmäiseisenä NFC Shell lisäyksen joka oli saatavissa vain Nokia 3220 puhelimiin. Uusissa Nokian malleissa N9:ssa ja C7:ssa on NFC-siru. Ongelmana on kuitenkin tietoturva, joka ei riitä maksamiseen. [15] [13]

Nokia, Sony ja Philips perustivat yhdessä NFC foorumin vuonna 2004. Foorumin tehtävänä on edistää tekniikan yleistymistä ja tarjota tietoa markkinoille. [20]

NFC standardoinnista vastaa Ecma International- järjestö, joka lähettää ne hyväksyttäväksi esimerkiksi ISO- järjestöön. NFC:ssä on kaksi erilaista protokollaa. NFCIP-1(Near Field Communication Interface Protocol 1) ja NFCIP-2(Near Field Communication Interface Protocol 2). [15] [20]

NFCIP-1 on määritelty ECMA-340 eli ISO/IEC 18092 standardissa. Protokolla määrittelee signaalirajapinnan, käytettävät tiedonsiirtoprotokollat, yhteyden alustuksen ja törmäysten hallinnan. [15]

NFCIP-1 standardin mukaiset laitteet toimivat taajuudella 13.56MHz. Laitteiden tiedonsiirtonopeus on 106, 212 ja 424 kbit/s. Lisäksi protokolla määrittelee laitteelle kaksi yhteystyyppiä aktiivinen ja passiivinen. [15]

ECMA-352 eli NFCIP-2 on standardoitu ISO/IEC-järjestöjen toimesta NFC:n viralliseksi ISO/IEC 21481 standardiksi. Protokolla edellyttää ettei laitteiden välinen liikenne haittaa muita samalla taajuudella tapahtuvaa liikennettä. Lisäksi ´protokolla määrittelee käytettävän kommunikaatiotilan. Tiloja on kolme erilaista: NCF-, PCD- ja VCD- tila. [15]

NFC-tila tarkoittaa ECMA-340-standardissa määriteltyä NFCIP-1 laitteiden välistä kommunikaatiota. PCD-tila on määritelty ISO/IEC 1443-standardissa. PCD-tilaa käytetään kun laitteet ovat alle 10cm päässä toisistaan. VCD-tila on määritelty ISO/IEC 1593 standardissa ja sitä käytetään kun laitteet ovat 1-1,5 metrin päässä toisistaan. [15]

Kuva 6: Nokia NFC Shell. [7]

7 Tietoturva ja käyttäjien tunnistus

Koska suurin osa mobiilimaksamisesta tapahtuu tietoverkon kautta, on maksajan tunnistaminen tärkeässä osassa, koska ostaja ja myyjä eivät välttämättä ole katsekontaktissa toisiaan kohtaan. Maksutapahtumassa täytyykin jollain tavalla tunnistaa käyttäjät. Nykyään markkinoilla on muutamia varteenotettavia tunnistusmenetelmiä, joista ei kuitenkaan yksikään ole aukoton.

7.1 Mobiilimaksamisen haasteet ja uhat

Mobiilimaksamisen uhat ovat: [18]

- **Langattomuus:** Mobiililaitteiden välissä data kulkee ilmassa. Tapauksissa joissa pakettien salaus on puutteellista voi jokin kolmas osapuoli kaapata tärkeän paketin, joka sisältää esimerkiksi luottokortin tiedot.
- **Virukset:** Virukset ovat nykyaikaisessa tietoliikenteessä suuri ongelma. Mobiilijärjestelmissä ongelma on, ehkä vieläkin suurempi. Monien mobiilijärjestelmien tietoturva ja virustorjunta ovat pöytäkoneita heikompia, tekniikan uutuuden takia.
- **SIM-kortin kopiointi:** SIM-kortista voidaan tehdä kopio ja sen tiedot joutuvat vääriin käsiin. Tällöin joku muu voi esiintyä jonakuna toisena. Järjestelmissä, joissa käyttäjät tunnistetaan SIM-kortin perusteella, tämä on uhka.
- **Laitevarkaudet:** Kännykkä voi kadota tai se voidaan varastaa. Nykyisten kännyköiden tietoturva on osin puutteellista . Tämän takia, varkauden sattues-

sa kännykässä olleet tärkeät tiedot(esim. luottokortin numerot) voivat joutua vääriin käsiin.

- **Tietojen häviäminen:**Laitteen toimintahäiriön takia tärkeät tiedot voivat kadota. Tämän takia onkin tärkeää, että tiedoista tehdään varmuuskopiot.
- **Jatkuva yhteys:** Laite on koko ajan yhteydessä verkkoon, joten käyttäjä ei välttämättä huomaa hyökkäystä.

7.2 PIN-Koodi

Yksinkertaisimmillaan tunnistus voi tapahtua PIN-koodin avulla, jonka käyttäjä näppäilee puhelimella maksettaessa. Tapa on melko yksinkertainen ja helppo, täten se sopiikin pienten ja halpojen ostoksien tekemiseen. Helppouden takia tapa on yleisesti käytössä monissa maksujärjestelmissä. Koodin ongelmana on lyhyys: Esimerkiksi nelinumeroinen koodi mahdollistaa ainoastaan kymmenentuhatta erilaista vaihtoehtoa. Koodi on siis helppo murtaa nykyajan tietokoneilla. Yleisen käytettävyyden takia on kuitenkin helpompaa käyttää melko lyhyitä tunnisteita, jotka ovat helpommin muistettavia. [32]

7.3 Salausavaimet ja digitaalinen allekirjoitus

PKI(Public Key Infrastructure) on tapa salata lähetettävää tietoa epäsymmetrisillä menetelmillä, jotka perustuvat johonkin matemaattiseen algoritmiin, esimerkiksi RSA-algoritmiin. Menetelmässä käytetään kahta avainta: julkista ja yksityistä avainta. Yksityisellä avaimella salatun viestin voi purkaa vain julkisella avaimella ja päinvastoin. Salaisen avaimen haltia voi jakaa julkista avainta yleisesti, esimerkiksi verkossa, haluamilleen osapuolille, mutta yksityinen avain pysyy ainoastaan avaimen haltijalla. [25]

PKI-menetelmän avulla lähettäjä voi varmistua kenen hallussa julkista avainta vastaava yksityinen avain on. Tällä tavalla voidaan olla varmoja lähettävän aitoudesta. Avaimen aitouden ja sen haltijan henkilöllisyyden varmistaa jokin luotettavaksi tiedetty taho niin kutsutulla varmenteella. [25]

Epäsymmetrisen menetelmän lisäksi on olemassa symmetrisiä salausmenetelmiä. Menetelmässä viestin salaukseen ja purkuun käytetään samaa avainta. Menetelmä ei ole yhtä turvallinen kuin kahteen avaimeen perustuva menetelmä. [25]

Toinen salausavaimiin liittyvä termi on digitaalinen allekirjoitus. Se kuuluu sähköisiin allekirjoituksiin ja se on toteutettu salausavaimella. Sen avulla voidaan varmistua viestin oikeellisuudesta ja lähettäjän henkilöllisyydestä. Digitaalisen allekirjoituksen on oltava myös juridisesti pätevä. [25]

Esimerkiksi Kuopion yliopistossa on kehitelty tekniikkaa jonka avulla käyttäjät tunnistetaan digitaalisella allekirjoituksella. Yksinkertaistaen käyttäjät lähettävät tekstiviestin toisilleen, jonka avulla osapuolet tunnistetaan. Viesteissä olevaa digitaalista allekirjoitusta verrataan luotettavan osapuolen ylläpitämään tietokantaan, joka ylläpitää varmenteita. Järjestelmästä lisää hieman myöhemmin. [11]

Mobiiliympäristössä käytetään PKI:n hieman mukautettua WPKI(Wireless Public Key Infrastructure) versiota . WPKI:sa käytetään salausalgoritmina RSA-menetelmää ja ECC(Elliptic Curve Cryptosystems)-algoritmia joka vaatii vähemmän muistia ja kapasiteettia kuin RSA ja soveltuu paremmin mobiilimaailmaan jossa laiteen ja sen akun kapasiteetti on usein rajallinen. [18]

WPKI:in on taattava neljä seikkaa maksamisjärjestelmissä, jotta se olisi käyttökelpoinen: [18]

- **Käyttäjien luotettava autentikointi:** Yhteyttä muodostaessa on oltava varma vastapuolen henkilöllisyydestä.
- **Turvallinen tiedonsiirto(Confidentiality):** Yhteys osapuolten välillä on pysyttävä salattuna koko ajan.
- **Tiedon eheys ja oikeellisuus:** Tieto ei saa muuttua eikä korruptoitua lähetyksessä osapuolten välillä
- **Kiistämättömyys(None repudiation):** Mekanismin on taattava, että ostaja ei voi tulevaisuudesta kiistää ostosta ja jättää ostosta maksamatta.

PKI ja digitaalinen allekirjoitus ovat varmoja salausmenetelmä, jotka toimii hyvin ilman suuria ongelmia. RSA-algoritmia pidetään yleisesti murtamattomana menetelmänä, kunhan salausavaimet valitaan hyvin.

7.4 Älykortti

Älykortit ovat mobiililaitteissa käytetyin tunnistustapa. Jokaisessa matkapuhelimessa on SIM-kortti, joka yksilöi laitteen käyttäjän. Usein älykortin lisäksi käyttäjän tunnistukseen tarvitaan PIN-koodi Kortin sirulla on esimerkiksi käyttäjän digitaalinen allekirjoitus. [18]

Älykortin hyvä puoli on että nykyisissä matkapuhelimissa on SIM-kortti jo valmiina. Kortille voidaan lisätä ominaisuuksia jonka jälkeen puhelin korvaa esimerkiksi lompakon. Kuten luvussa 6.4 kerroin voidaan kännykkään lisätä toinen kortti joka sisältäisi esimerkiksi rahaliikenteen operaatiot. [18] [27]

Mobiilimaksamisälykortit perustuvat ISO 7816-X- ja ISO/IEC 1443-1-standardeihin. Standardit esimerkiksi määräävät, että kortit pitävät sisällään ja hallinnoivat yksityisiä salausavaimia, eristää salaukseen käytettävät menetelmät muista järjestelmän osista ja että kortti on siirrettävissä koti-, työ- ja kannettavan laitteen välillä.[18]

Suomessa kehitetty ja käytetty avoin HST-arkkitehtuuri, jota tarjotaan eri yrityksille ja yhteisöille henkilökorttia. Väestörekisterikeskus tarjoaa sähköistä HST-henkilökortin sirulla on FINEID-sovellus hallinnoi sähköisen henkilökortin tietoja ja tarjoaa alustan salausavainten hallinnointiin.[27]

Kortti on saatavissa myös Osuuspankin Visa Electron -kortille sekä Soneran ja Elisan liittymällä varustetun matkapuhelimen SIM-kortille. Salaukseen kortti käyttää RSA-algoritmia. Aiemmin mainitsemani Kuopion yliopistossa toteutettu projekti käytti Suomen väestörekisteriä ja FINEID-järjestelmää hyväkseen digitaalisen allekirjoituksien lisäämiseksi tekstiviesteihin.[27] [11]

Älykortti on ihmisille tuttu. Jokaisessa kännykässä on sellainen, joten se on käytössä todettu hyväksi. Ihmisten puhelimeen on helppoa toinen kortti joka sisältää tunnisteet, eikä puhelimen käyttö sinänsä muutu.

Tekniikan suurimman ongelman nykyisin muodostaa sirukorttien ja mobiililaitteiden kohtuullisen pieni kapasiteetti, isoihin koneisiin verrattuna. Tyypillisesti mobiilimaksamisälykortin sirulla on jonkinlainen mikroprosessori ja muistia jotka hoitaa salauksen, mutta esimerkiksi RSA-menetelmä on melko vaativa va tarvitsee kohtuullisen paljon muistia ja tehokkaan prosessorin, joten tämä nostaa kortin hintaa ja vaikeuttaa sen toteutusta.[18]

7.5 Biometriset menetelmät

Biometriikalla tarkoitetaan, melko uusia, tunnistusmenetelmiä, jolla mitataan ihmisen fyysisiä ominaisuuksia, (esimerkiksi ääni tai sormenjälki) tai käyttäytymiseen liittyvää(esim. Kävelytyyli). Toinen keskeinen käsite on multimodaalinen autentikaatio, jossa useampi biometrinen-menetelmä yhdistetään. Yleensä kuitenkin yksi tunnistustapa riittää ihmisen luotettavaan tunnistukseen.[26]

Biometriikan etuna on, ettei käyttäjän tarvitse kortteja tai muita tunnisteita. Lisäksi tapa tunnistaa nimenomaan käyttäjän, eikä esimerkiksi laitetta tai älykorttia. Laiteen katoaminen ei ole niin vakavaa kuin perinteisissä salausmenetelmissä.[26]

Eräässä tutustumassani tutkimuksessa ihmisen ääntä käytettiin niin kutsutun äänishekin(Voice Cheque) allekirjoitukseen. Maksajan äänestä luodaan digitaalinen vesileima, joka lisätään shekkiin.[28]

Menetelmä perustuu jonkin luotettavaksi tiedetyn tahon keräämään tietokantaan jossa kaikkien palvelun käyttäjien äänistä on näyte johon digitaalista vesileimaa verrataan. Jokaisella shekillä on kaksi ominaisuutta, jotka pitää tarkistaa : Ensimmäiseksi pitää varmistua asiakkaan henkilöllisyydestä ja toiseksi varmistua siitä ettei kukaan ulkopuolinen ole muuttanut shekkiä lähetyksen aikana.[28]

Jo nykyisinkin äänishekki on hyvin tietoturvallinen, koska ihmisen ääni on riittävän yksilöllinen, jotta henkilön tunnistus on varmaa. Kaikkien palvelun käyttäjien äänitunnisteet on tallennettu varmaksi tiedettyyn tietokantaan. Jotta shekin oikeellisuudesta varmistuttaisiin se salataan ennen lähetystä RSA-algoritmilla ja salausavainten avulla.[28]

Tulevaisuudessa biometriikka voi olla erittäin tärkeä tunnistusmenetelmä, kunhan pienet ongelmat saadaan korjattua . Nykyisin kyseiset menetelmät eivät ole tarpeeksi tehokkaita laajaan käyttöön. Esimerkiksi esittelemäni P2P-maksujärjestelmässä on tavoitteena kehittää äänentunnistus, muta ainakaan artikkeleissa joihin tutustuin ei menetelmä ole vielä käytössä. [9] [10]

8 Yhteenveto

Mobiililaitteiden kehityksen myötä yhä suurempi joukko kuluttajista käyttää matkapuhelintaan muuhunkin kuin puheluihin. Yksi lisääntyvistä palveluista on erilaiset maksamissovellukset, jotka muuttavat mobiililaitteen maksuvälineeksi.

Palvelut ovatkin kehittyneet huomattavasti muutaman vuoden aikana. Palveluista on tullut entistä halvempia, helppokäyttöisempiä ja sujuvampia, joten suurempi osa keskivertokuluttajista ovat halukkaitta käyttämään niitä.

Tulevaisuudessa matkapuhelin voikin korvata kuluttajan luotto- ja muut maksukortit päivittäisten ostoksien ostamisessa. Jotta tämä tapahtuisi, on palvelun kuitenkin oltava yhtä helppokäyttöinen ja sujuva käyttää kuin nykyiset maksukortit ja tai käteinen. Myöskin palvelun kustannukset eivät saa olla, ainakaan kovin paljon, suuremmat kuin perinteisten maksutapojen käyttö.

Toinen käyttökohde jossa mobiilimaksamista käytetään on erilaisten palveluiden, sisältöjen ja pienten sovelluksien hankkiminen mobiililaitteiseen. Yleensä tilattu sisältö maksetaan puhelinlaskun yhteydessä, mutta luottokorteillakin toimivia järjestelmiä on olemassa.

Tutkielmassani loin nopean katsauksen mobiilimaksamiseen. Tutkin olemassa

olevia järjestelmiä ja erilaisia käytettäviä teknologioita. Niiden välisiä eroja, hyviä ja huonoja puolia.

Eräs varteenotettava teknologia on NFC., jonka yleistymistä on uumoiltu jo usean vuoden ajan. Nyt moni iso valmistaja on tuonut NFC-sirun laitteisiinsa. Joten tekniikka voi yleistyä nopeasti. Kunhan pienistä lapsentaudeista päästään eroon. Maksamisen ohella NFC:tä voidaan käyttää kulunvalvontaan ja henkilöiden tunnistamiseen. Tekniikan oikeastaan suurin ongelma onkin se että harva laite tukee sitä. Tulevaisuudessa tämä voi kuitenkin muuttua ja tekniikka yleistyy. Arkikäytössä NFC on nopea, käytössä vaivaton ja helppokäyttöinen, joten se voi tosiaankin yhdistää maksukortit ja matkapuhelimen.

Lähteet

[1] Ljupco Antovski ja Marjan Gusev, *M-Payments*,

Proceedings of the 25th International Conference on Information Technology Interfaces (ITI 2003), 16-19 June, 2003, sivut 95 - 100.

[2] *Bluetooth-tekniikan virallinen kotisivu*, <URL:`http://www.bluetooth.com`>.

[3] *Bluetooth-tekniikan virallinen jäsensivu*, <URL:`http://www.bluetooth.org`>.

[4] Natali Delić ja Ana Vukašinović *Mobile Payment Solution - Symbiosis between banks, application service providers and mobile network operators* Proceedings of the Third International Conference on Information Technology: New Generations, (ITNG'06), ISBN:0-7695-2497-4, sivut 346 - 350

[5] *DinaCard-maksukortin kotisivu*,

<URL:`http://www.dinacard.nbs.yu/en/index.html`>. 25.5.2007

[6] *E-business.fi-e-Business Suomessa-sähköisen liiketoiminnan sanasto*,

<URL:`http://www.e-business.fi/fi/default.aspx?tocID=1`>.
viitattu 20.5.2007

[7] *Esato 2005 Nokia Launches NFC Shell for Mobile Payments.* Saatavana verkosta osoitteesta:

<URL: `http://www.esato.com/news/article.php/id=436`>.

[8] Stig Frode Mjølsnes ja Chunming Rong *On-Line E-Wallet System with Decentralized Credential Keepers* Stavanger University College, Norja Volume 8, Number 1 / February, 2003, ISSN:1383-469X (Print) 1572-8153 (Online), Sivut 87-99

[9] Jerry Gao, Krishnaveni Edunuru, Jacky Cai ja Simon Shim *P2P-Paid: A Peer-to-Peer Wireless Payment System* Proceedings of the 2005 Second IEEE International Workshop on Mobile Commerce and Services (WMCS 05), San Jose State University, Computer Engineering, San Jose, USA, 2005.

19-19 July 2005, ISBN: 0-7695-2391-9, sivut 102 - 111

[10] Jerry Gao, Jacky Gai ja Simon Shim , *A Wireless Payment System*, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS 05) San Jose State University, Computer Engineering, San Jose, USA 2005, 16-18 Dec. 2005, ISBN: 0-7695-2512-1

[11] Marko Hassinen ja Konstantin Hyppönen *Strong Mobile Authentication*, Kuopion Yliopisto, Wireless Communication Systems, 2005. 2nd International Symposium, 5-7 Sept. 2005, ISBN: 0-7803-9206-X, sivut 96-100

[12] Stefan Heng *E-Commerce settles for established payment systems Limited market potential for innovative payment systems* Deutsche Bank Research, Frankfurt am Main, Germany, May 14, 2007, ISSN Print: 1619-3245, ISSN Internet: 1619-3253, ISSN e-mail: 1619-4756

[13] *'Nokian nfc-siru ei sovi maksamiseen'* IT-Viikko uutinen 26.10.2011

[14] Stamatis Karnouskos, Fraunhofer Fokus

Mobile Payment: A Journey through Existing Procedures And Standardization Initiatives, IEEE Communications Surveys and Tutorials, Fourth Quarter 2004, Volume 6, No. 4, Sivut 44-66

[15] Mikko Kivioja

Mobiilimaksaminen lähimaksamisen näkökulmasta Tampereen Ammattikorkeakoulu

[16] *Kuluttajaviraston verkkosivusto - Maksaminen sähköisissä palveluissa*

<URL:`http://www.kuluttajavirasto.fi`>. viitattu 15.8.2007

[17] Vijay Kumar, Srinivas Parimi ja Dharma P. Agrawal *WAP: Present and Future* Published by the IEEE CS and IEEE Communications Society,January-March 2003, ISSN: 1536-1268, sivut 79-83

[18] Gianluigi Me *Security overview for m-payed virtual ticketing* appears in: Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings, 7-10 Sept. 2003, Volume:1, ISBN: 0-7803-7822-9, sivut 844- 848

[19] Seema Nambiar, Chang-Tien Lu ja Lily R. Liang, *Analysis of Payment Transaction Security in Mobile Commerce*, 2004 IEEE, sivut 475-480

[20] *NFC-forum.org*, URL: `http://www.nfc-forum.org`>, viitattu 20.11.2007.

[21] *Nokian kotisivu*, <URL: `http://www.nokia.com/nfc`>, viitattu 20.11.2007.

[22] Michael Pastore, *MasterCard Puts PayPass in Mobile Phones*, 13.10 (2004).

Saatavana verkosta osoitteesta:

<URL: `http://www.insideid.com/ecommerce/article.php/3421401`>,

viitattu 6.3.2008.

[23] *Sonyn kotisivut*, <URL: `http://www.sony.net/`>, viitattu 20.11.2006.

[24] Ramesh Subramania ja Brian D. Goodman *Peer-to-Peer Computing: The Evolution of a Disruptive Technology*,

2005, ISBN: 159140-4312

[25] *Viestintävirasto* <URL: `http://www.ficora.fi/`>, viitattu 2.2.2008.

[26] VTT-Biometriikka ja multimodaalinen tunnistus

Verkko-osoitteesta: <URL:`http://www2.vtt.fi/`>, viitattu 5.2.2008

[27] *Väestörekisterikeskus-Sähköinen henkilökortti*, verkko-osoitteet:

<URL:`http://vrk.fineid.fi/`> ja <URL:`http://www.fineid.fi`>,

viitattu 4.2.2008.

[28] Jiehua Wang, Song Yuan *A Novel Security Mobile Payment System Based On Watermarked Voice Cheque* Nantong University, Nantong, China, Darmstadt University of Technology, Darmstadt, Germany, appears in: Mobile Technology, Applications and Systems, 2005 2nd International Conference, 15-17 Nov. 2005, ISBN: 981-05-4573-8.

[29] William H. Tranter, Brian D. Woerner, Jeffrey H. Reed, Theodore S. Rappaport, Max Robert *'Wireless Personal Communications: Bluetooth Tutorial and Other Technologies*, 2002, eBook ISBN: 0-306-46986-3.

[30] Patricia McDermott-Wells *What is Bluetooth?*, December 2004 - January 2005, sivut 33-35

[31] *Wikipedia*, <URL: `http://www.wikipedia.org`>,viitattu 20.2.2008.

[32] Agnieszka Zmijewska, *Evaluating Wireless Technologies in Mobile Payments - A Customer Centric Approach*, Proceedings of the International Conference on Mobile Business (ICMB05), 11-13 July 2005, ISBN: 0-7695-2367-6, sivut 354-362, University of Technology, Sydney, 2005.