

Janne Rautiola

## **LUOKKAKIRJASTON TOTEUTTAMINEN SEPA-MAKSAMISEEN**

## **LUOKKAKIRJASTON TOTEUTTAMINEN SEPA-MAKSAMISEEN**

Janne Rautiola  
Opinnäytetyö  
Kevät 2011  
Tietojenkäsittelyn koulutusohjelma  
Oulun seudun ammattikorkeakoulu

## TIIVISTELMÄ

Oulun seudun ammattikorkeakoulu  
Tietojenkäsittelyn koulutusohjelma

---

Tekijä: Janne Rautiola

Opinnäytetyön nimi: Luokkakirjaston toteuttaminen SEPA-maksamiseen

Työn ohjaaja: Jouni Juntunen

Työn valmistumislukukausi ja -vuosi: Kevät 2011

Sivumäärä: 39 + 4

---

Pankit korvaavat vanhat FTP-yhteyteen perustuvat pankkiyhteysjärjestelmänsä lähitulevaisuudessa uusilla Web Services -pohjaisilla järjestelmillä, ja vanhat Finvoice-verkkolaskut vaihtuvat uusiin SEPA-tilisiirtoihin. Tämän opinnäytetyön tavoitteena oli vastata näihin muutoksiin Nordean osalta. Työn toimeksiantajina olivat oululainen ohjelmistoalan yritys SeBitti Oy ja sen tytäryhtiö BookMaster Oy.

Työn tietoperusta alkaa lyhyellä kuvauksella SEPasta, jonka jälkeen kerrotaan uudesta SEPA-tilisiirrosta ja tilisiirron palautesanomasta. Lopuksi käsitellään Nordean Web Services -palveluita ja niiden tietoturva. Lähteinä on käytetty muun muassa Nordean omia dokumentteja sekä Finanssialan Keskusliiton yhdessä suomalaisten pankkien kanssa tekemiä dokumentteja SEPA-standardien ja Web Services -palvelun käytöstä Suomessa.

Opinnäytetyön tuloksena syntyi luokkakirjasto, jota hyödyntäen voidaan muodostaa SEPA-tilisiirto, ja lähettää se Nordean Web Services -maksuliikennepalveluun. Luokkakirjasto vastaa myös uusiin tietoturva vaatimuksiin, joita Web Services -palvelu asettaa. Kirjasto tuli osaksi BookMaster Oy:n BookMaster Laskutus 2011 -ohjelmistoa.

---

Asiasanat: SEPA, yhtenäinen euromaksualue, ohjelmistokehitys, luokkakirjasto, ISO 20022, Web Services, PKI

## ABSTRACT

Oulu University of Applied Sciences  
Degree Programme in Business Information Systems

---

Author: Janne Rautiola

Title of thesis: Creating Class Library for SEPA payments

Supervisor: Jouni Juntunen

Term and year when the thesis was submitted: Spring 2011

Number of pages: 39 + 4

---

Banks will replace their old FTP based bank connection systems with new Web Services based systems in the near future and obsolete e-invoices (Finvoice) with new SEPA transfers. The aim of this thesis was to respond to these changes in Nordea's case. The clients of this thesis were a software company from Oulu called SeBitti Ltd. and its subsidiary BookMaster Ltd.

The theory begins with a short introduction to SEPA, which is followed by the message description of SEPA transfer, and transfer's feedback message. Finally, it will discuss Nordea's Web Services systems and their security. The sources used in theory consist, among other things, of documents made by Federation of Finnish Financial Services together with Finnish banks about SEPA standards and usage of Web Services in Finland.

Thesis resulted in a class library that can be used to form SEPA transfers and send those formed transfers to the Nordea's Web Services payment system. The class library also covers the new security requirements that the Web Services system impose. The library became part of the BookMaster Ltd's BookMaster Laskutus 2011 billing software.

---

Keywords: SEPA, Single Euro Payments Area, Software Development, Class Library, ISO 20022, Web Services, PKI

# SISÄLLYS

1 JOHDANTO	6
2 SEPA	8
2.1 Aikataulu	9
2.2 Maksuvälineet	10
2.3 Infrastruktuuri	11
2.4 Tekniset standardit	11
3 SEPA-TILISIIRRON VIESTINVAIHTO	13
3.1 SEPA-tilisiirto	17
3.2 SEPA-tilisiirron palautesanoma	20
3.3 Muut sanomat	21
4 WEB SERVICES -PALVELUT	23
4.1 Maksuliikennepalvelu	23
4.1.1 SOAP-sanoma	24
4.1.2 SOAP-sanoman muodostus ja elinkaari	26
4.2 Tietoturva	28
4.2.1 Julkisen avaimen menetelmä ja digitaalinen allekirjoitus	28
4.2.2 Nordean varmennepalvelu	29
5 TULOKSET	31
5.1 Luokkakirjastojen toteutus	31
5.2 Luokkakirjastojen testaus	34
6 POHDINTA	35
LÄHTEET	38
LIITTEET	40

# 1 JOHDANTO

Pankkien maksujärjestelmät ovat muuttumassa. Suomessa käytössä olleet maksusanomat kuten Finvoice-verkkolasku poistuvat käytöstä ja tilalle tulevat uudet Euroopan keskuspankin määrittelemät maksusanomastandardit. Myös vanha FTP-protokollaan perustunut pankkiyhteysjärjestelmä korvataan uudella Web Services -pohjaisella järjestelmällä. Molemmat muutokset johtuvat SEPAsta. SEPA on hanke, joka uudistaa pankkimaksamisen ja tekee siitä yhtenäisen Euroopan alueella.

Tämän opinnäytetyön tavoitteena oli tehdä luokkakirjasto, jonka avulla voidaan maksaa SEPA-standardien mukaisia tilisiirtoja Nordealle. Kehitystyönä toteutettiin ja testattiin luokkakirjasto, jolla voidaan muodostaa SEPA:n mukanaan tuoman ISO 20022 -sanomastandardin mukaisia maksuaineistoja, ja lähettää nämä maksuaineistot pankille Web Services -määritysten mukaisesti.

Toteutetun ohjelmistokehitystyön kannalta ISO 20022 -sanomastandardit olivat erittäin tärkeässä osassa. Ilman näiden sanomien tuntemista olisi ollut mahdotonta luoda ohjelmisto, jolla voi muodostaa standardoituja maksusanomia. Standardien käyttöönottoa rajattiin laskutusohjelmiston tarpeiden mukaan. Tärkeintä oli, että SEPA-tilisiirrot toimivat, joten opinnäytetyössä toteutettiin vain SEPA-tilisiirron muodostus ja SEPA-tilisiirron palautesanomien purku. Tästä syystä muun muassa SEPA-suoraveloitus jätettiin työn ulkopuolelle.

Web Services -kanavan kanssa kommunikoivaa moduulia rajattiin siten, että työssä toteutettiin kommunikointi vain yhden pankin osalta. Muiden pankkien yhteydet on helppo toteuttaa myöhemmin, kun yksi esimerkki on jo valmiina, ja niiden toteuttaminen ei olisi tuonut juuri mitään teknistä lisäarvoa opinnäytetyölle. Työn aloitushetkellä pankeilla osalla pankeista oli heikot valmiudet siirtyä SEPAan tai valmiuksia ei ollut lainkaan. Tästä syystä pankiksi valittiin se, jonka järjestelmät vaikuttivat selkeimmiltä ja kehittyneimmiltä. Valinnan hetkellä kyseinen pankki oli Nordea, koska se tarjosi automatisoidun testauspalvelun ja selkeän tietoturvaratkaisun.

Opinnäytetyön toimeksiantajina olivat oululainen ohjelmistoalan yritys SeBitti Oy, ja sen taloushallinnon ohjelmistoihin keskittynyt tytäryhtiö BookMaster Oy. Toteutettu ohjelmistorajapinta on otettu käyttöön osana BookMaster Laskutus 2011 -ohjelmistoa. BookMaster Laskutus 2011 on taloushallinnon ohjelmisto, joka sisältää laskutusominaisuuksien lisäksi muun muassa asiakas-

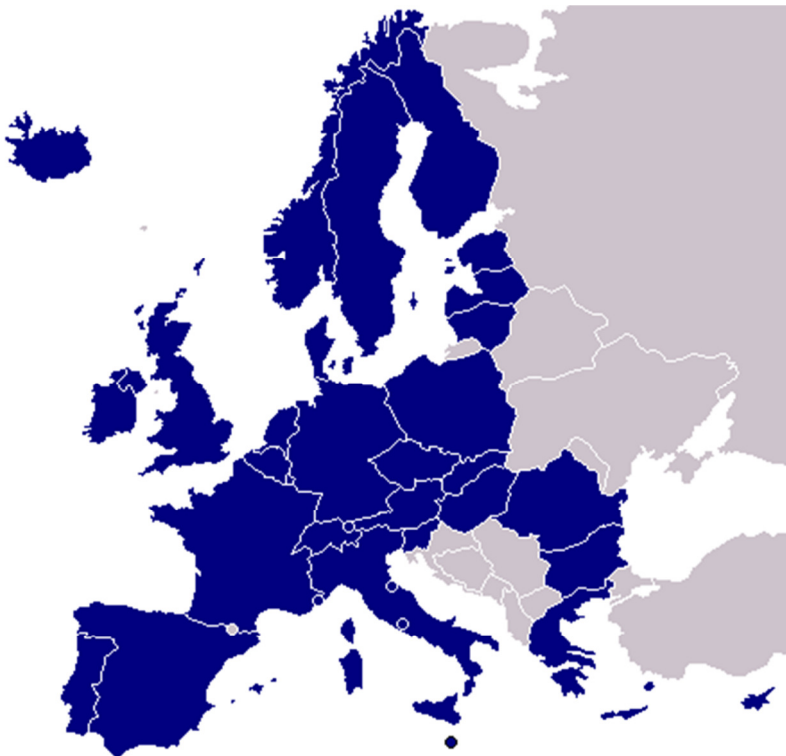
rekisterin, tuoterekisterin sekä osto- ja myyntireskontran. Se myös tukee Finvoice-verkkolaskua, joka korvautuu uudella SEPA-tilisiirrolla.

Raportin toinen luku johdattelee aiheeseen esittelemällä SEPAa. Siinä kuvataan lyhyesti työn kannalta oleellinen SEPA-tilisiirto sekä muut maksuvälineet, infrastruktuuri ja tekniset standardit. Luvussa kolme syvennyttään SEPA-tilisiirron teknisiin standardeihin. Siinä kuvataan tilisiirron toimintatapa ja sanoman XML-muotoinen rakenne menemättä kuitenkaan yksityiskohtaisesti elementtitasolle. Neljännessä luvussa käsitellään pankkien Web Services -rajapintoja ja niihin liittyviä tietoturvatkaisuja. Viidennessä luvussa kerrotaan kehitystehtävän tuloksista eli toteutuneesta luokkakirjastosta ja sen testauksesta. Tietoperustan tärkeimpinä lähteinä käytettiin Euroopan Keskuspankin ja Finanssialan Keskusliiton dokumentteja, joissa kuvataan rajapinnan ja SEPA-tilisiirron toiminta.

## 2 SEPA

SEPA tulee sanoista Single Euro Payments Area, ja suomennettuna se tarkoittaa yhtenäistä euromaksualuetta. Se on alue, jolla kuluttajat, yritykset ja muut talouden toimijat voivat maksaa ja vastaanottaa euromääräisiä maksuja samoin perusehdoin, samoin oikeuksin ja samoin velvollisuuksin riippumatta siitä, missä päin maksualuetta maksaja ja maksun saaja ovat. (Euroopan Keskuspankki 2006, 5, 7.)

SEPAan kuuluvat kaikki EU-maat sekä EU:n ulkopuoliset ETA-maat, joita ovat muun muassa Islanti, Liechtenstein, Norja ja Sveitsi (kuvio 1). Näiden maiden pankit ovat sitoutuneet yhtenäisen euromaksualueen toteuttamiseen. SEPA-hankkeesta vetovastuussa on Euroopan maksu-neuvosto (European Payment Council, EPC), jonka tavoitteena on pankkitoimialan itsesääteilyllä tukea yhtenäisen, avoimen ja yhteiskäyttöisen maksuliikennemarkkinan saavuttamista. SEPA-hankkeessa EPC:n tulee muun muassa määritellä pankkien yhteinen kanta perusmaksu-palveluihin, antaa strategista neuvontaa standardointiin, määritellä käytännöt ja valvoa tehtyjen päätösten käyttöönottoa. Myös pankit osallistuvat SEPA-palveluiden määrittelyyn, millä pyritään varmistamaan mukana olevien pankkien sitoutuminen hankkeeseen. (Finanssialan keskusliitto 2009, 2, 13.)



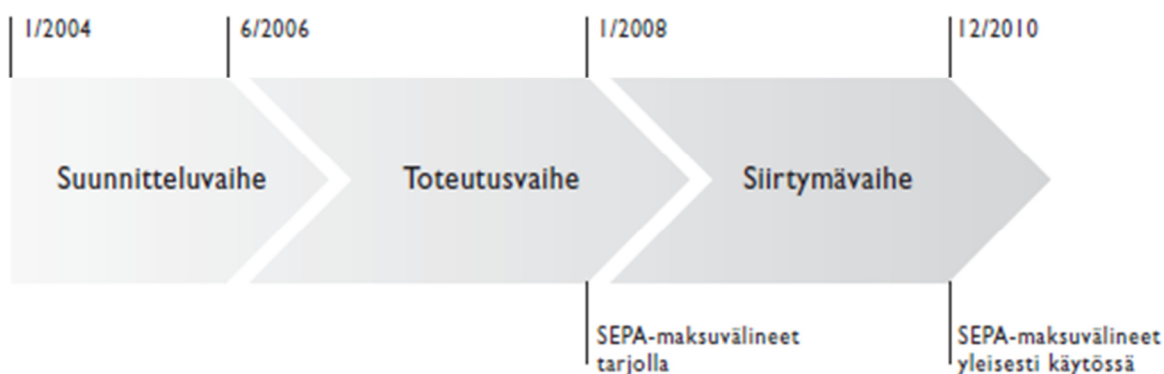
KUVIO 1. SEPA-maat (Wikipedia 2011, hakupäivä 25.4.2011)



SEPAN tavoitteena on edistää eurooppalaisen maksualueen yhdentymistä, ja siten parantaa palvelutasoa sekä tarjota tehokkaita ja edullisia maksutapoja. Yhtenäisen euromaksualueen perustana ja tavoitteina ovat yhteinen raha, euromääräisissä maksuissa käytettävät yhteiset maksuvälineet (tilisiirrot, suoraveloitukset ja korttimaksut), tehokas euromääräisten maksujen käsittelyinfrastruktuuri, yhteiset tekniset standardit, yhteiset liiketoimintakäytännöt, yhdenmukainen lainsäädäntö sekä uusien palveluiden jatkuva asiakaslähtöinen kehittäminen (Euroopan Keskuspankki 2006, 7.)

## 2.1 Aikataulu

Euroopan Keskuspankin vuonna 2006 julkaisema aikataulu koskien SEPAN käyttöönottoa sisältää kolme vaihetta: suunnitteluvaiheen, toteutusvaiheen ja siirtymävaiheen. Nämä vaiheet ja niiden aikataulutus on esitetty kuviossa 2. (Euroopan Keskuspankki 2006, 14.)



KUVIO 2. SEPAN käyttöönoton aikataulu (Euroopan Keskuspankki 2006, 14)

*Suunnitteluvaihe* kesti vuoden 2004 alusta vuoden 2006 puoliväliin, ja sen aikana suunniteltiin uudet tilisiirto- ja suoraveloitusjärjestelyt, pankkikorttiohjeisto sekä selvitys- ja toimitusinfrastruktuurien ohjeisto. Vaiheen aikana myös kehitettiin vaadittavat tekniset standardit ja määriteltiin turvallisuusvaatimukset. (Euroopan Keskuspankki 2006, 14.)

Suunnitteluvaiheen jälkeen alkaneessa *toteutusvaiheessa* keskityttiin uusien SEPA-maksuvälineiden, standardien ja infrastruktuurien käyttöönoton valmisteluun. Toteutusvaiheeseen kuului myös näiden valmisteltujen komponenttien testaus. Jokaiseen euroalueen maahan perustettiin kansallinen seurantayksikkö, jonka tehtävänä on ollut tarkkailla pankkien, infrastruktuurioperaattorien, julkishallinnon, yritysten sekä lukuisten muiden käyttäjien valmistautumista SEPAN käyttöönottoon. (Euroopan Keskuspankki 2006, 14.)

*Siirtymävaihe* alkoi toteutusvaiheen päätyttyä vuoden 2008 alussa ja se päättyi vuoden 2010 lopussa. Siirtymävaiheen aikana asiakkaat pystyivät käyttämään kansallisia maksujärjestelmiä rinnakkain SEPA-järjestelmien kanssa. Yksi vaiheen tavoitteista oli, että markkinoilla siirrytään SEPA-järjestelyjen käyttöön vähitellen oma-aloitteisesti siten, että vuoden 2010 loppuun mennessä merkittävä osa maksuista suoritetaan jo SEPA-maksuvälineillä. (Euroopan Keskuspankki 2006, 14.)

## **2.2 Maksuvälineet**

Euroopan maksuneuvosto on kehittänyt SEPAa varten uudet maksutavat: SEPA-tilisiirrot sekä SEPA-suoraveloituksen. Näiden lisäksi se on kehittänyt toimintaohjeiston SEPA-korttimaksuja varten. SEPA:n siirtymävaiheen tavoitteena on, että kansallisessa käytössä olevat maksuvälineet korvataan SEPA-maksuvälineillä, joiden taustalla ovat yhteiset SEPA-järjestelyt ja -toimintaohjeisto. Molemmissa uusissa maksutavoissa tilinumerot annetaan IBAN-muotoisina tilinumeroina ja pankkitunnukset BIC-tunnuksina. (Euroopan Keskuspankki 2006, 19–21.) IBAN (International Bank Account Number) on kansainvälinen tilinumeron esittämismuoto ja BIC (Bank Identifier Code) on kansainvälinen pankin yksilöintitieto (Finanssialan Keskusliitto 2009, 10).

SEPA-tilisiirto (SEPA Credit Transfer, SCT) on pankkien väliseen rahansiirtoon tarkoitettu maksujärjestely, jossa määritellään yhteiset säännöt ja toimintatavat euromääräisiä tilisiirtoja varten. SCT:n vaatimuksena on muun muassa, että summan on siirryttävä kokonaisuudessaan maksun saajan tilille, maksun suuruutta ei saa rajoittaa ja maksun on oltava perillä saajan tilillä kolmessa pankkipäivässä. Lisäksi sen on oltava kaikkien käytettävissä yhtenäisellä euromaksualueella. (Euroopan Keskuspankki 2006, 20.)

SEPA-suoraveloitus (SEPA Direct Debit, SDD) on SEPA-tilisiirron tavoin pankkien välinen maksujärjestely. Siinä määritellään yhteiset säännöt ja menettelyt euromaksujen suoraveloitusta varten, niin kuin SCT määrittelee tilisiirtoa varten. Suoraveloitusta voidaan käyttää kahdella eri tavalla: velallinen antaa luvan maksun veloittamiseen joko pankilleen tai hän voi antaa luvan suoraan velkojalle. SEPA-suoraveloituksen määrittelynä on, että se on tilisiirron tavoin kaikkien käytettävissä yhtenäisellä euromaksualueella, ja sitä voidaan käyttää sekä toistuvien että yksittäisten euromääräisten maksujen kanssa. Lisäksi maksun on oltava perillä viiden pankkipäivän kuluessa alkaen siitä, kun maksu suoritetaan ensimmäistä kertaa tai kahdessa pankkipäivässä, jos sama maksu toistuu säännöllisesti. (Euroopan Keskuspankki 2006, 21.)

Korttimaksamiseen yhtenäinen euromaksualue tuo niin sanotut SEPA-korttimaksut. Korttien liikkeellelaskijoiden, korttiohjelmistojen, maksutapahtumien hyvittäjien ja välittäjien sekä operaattoreiden on noudatettava SEPA-korttimaksuissa yhteisiä periaatteita. Näitä Euroopan maksuneuvoston kehittämiä periaatteita kutsutaan SEPA-korttimaksamisen toimintaohjeistoksi (SEPA Card Framework, SCF). Korttimaksut kattavat sekä pankkikortit (suoraveloituskortit) että luottokortit. Euroopan maksuneuvosto on määritellyt SEPA-korttimaksamisen siten, että saman kortin on kelvattava koko euroalueella. Ainoa rajoitus kelpaamiselle on, että kaikkien korttiyhtiöiden kortteja ei välttämättä hyväksytä kaikissa liikkeissä. Lisäksi kortilla maksamisen ja maksun saamisen on hoiduttava koko euroalueella samalla tavalla. Kaikilla maksukorttien käsittelijöillä on oltava mahdollisuus tarjota palvelujaan kaikkialla euroalueella, jotta korttimarkkinoiden kilpailukyky, luotettavuus ja kustannustehokkuus paranisivat. (Euroopan Keskuspankki 2006, 22.)

### **2.3 Infrastrukturi**

Euroopan maksuneuvosto on luonut euromaksualueen infrastruktuurien toimittajille selvitys- ja toimitusohjeiston. Tällä pyritään siihen, että uudet maksutavat, SEPA-tilisiirto ja -suoraveloitus, toteutuvat. Selvityksellä tarkoitetaan maksumääräysten lähettämistä, täsmäyttämistä ja vahvistamista. Siinä kerrotaan, kuinka suuret summat lopulta siirtyvät. Toimituksella tarkoitetaan varojen siirtämistä maksajalta maksun saajalle ja maksajan pankilta maksun saajan pankille. Toimintaohjeistossa maksujärjestelyillä on oma tehtävänsä ja infrastruktuureilla omansa. Infrastruktuurien tehtävä on tarjota käsittelypalveluja rahoituslaitoksille. (Euroopan Keskuspankki 2006, 24.)

SEPA:n yhtenä tavoitteena on luoda yhteinen infrastrukturi, jossa kaikkien euromaksujen suoritus, vastaanotto ja toimitus voidaan hoitaa suoraan tai vähintään epäsuorasti. Siirtymävaiheen loppuvaiheilla eli vuoden 2010 lopussa kaikkien järjestelmien tulee pystyä käsittelemään kaikkia SEPA-maksuvälineitä. Laadittu selvitys- ja toimitusohjeisto on suunniteltu sellaiseksi, että kaikki euroalueen pankit ovat siinä mukana ja järjestelyt ovat infrastruktuureista riippumattomia. (Euroopan Keskuspankki 2006, 24.)

### **2.4 Tekniset standardit**

Liiketoiminnan tarpeiden pohjalta Euroopan maksuneuvosto havaitsi, että tiettyjen tietojen on siirryttävä rahoituksenvälittäjältä toiselle yhteisessä muodossa. Näiden havaintojen perusteella maksuneuvosto on laatinut teknisiä standardeja pankkiasiointia varten ja näistä standardeista ja

tiedoista on koottu sääntökirjat, jotka koskevat tilisiirtoja ja suoraveloitusta yhtenäisellä euromaksualueella. (Euroopan Keskuspankki 2006, 25.)

Sääntökirjoihin on sisällytetty loogiset tietoelementit (SEPA Data Model eli SEPA-tietomalli) sekä näihin tietoelementteihin perustuvat kansainvälisen standardisoimisjärjestö ISO:n (International Organization of Standardization) kehittämät UNIFI XML-sanomastandardit (UNiversal Financial Industry Message Standard), joiden tekninen nimi on ISO 20022. Sanomastandardien ansiosta maksusanomia voidaan laatia standardisoidulla kielellä, minkä johdosta niitä on helppo muodostaa ja lukea. UNIFI-standardien noudattaminen on Euroopan maksuneuvoston päätöksellä pakollista pankkien välisessä toiminnassa, ja niiden käyttöä suositellaan myös asiakkaan ja pankin välillä. Näiden standardien ansiosta euroissa suoritettavat maksut voidaan käsitellä täysin automaattisesti alusta loppuun. (Euroopan Keskuspankki 2006, 25.)

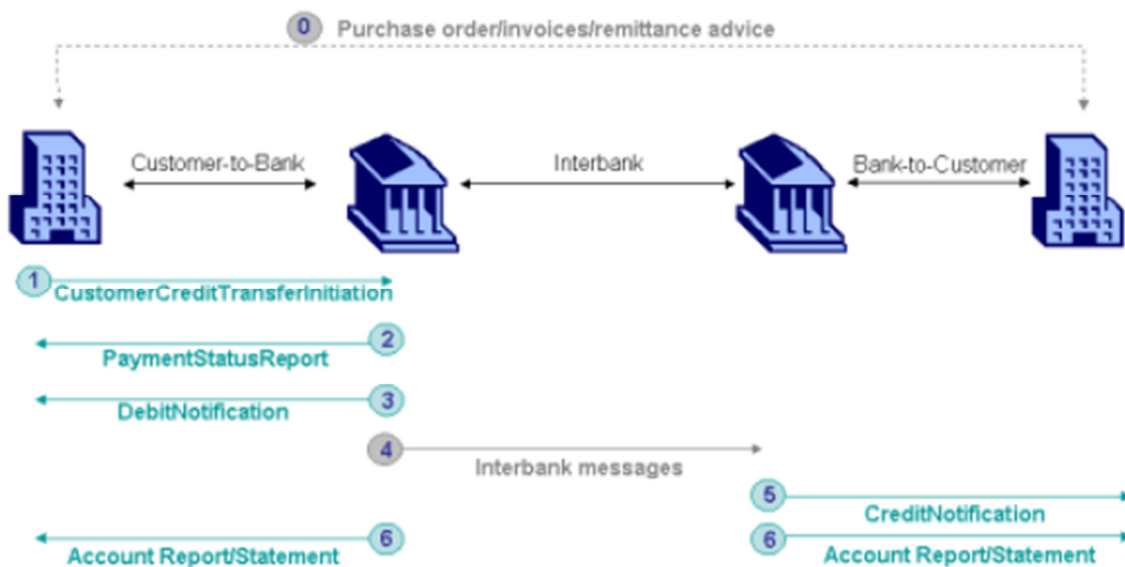
### 3 SEPA-TILISIIRRON VIESTINVAIHTO

SEPA-tilisiirron viestinvaihdoilla tarkoitetaan sanomaliikennettä maksamisen osapuolten välillä. Nämä osapuolet on kuvattu taulukossa 1, ja niihin viitataan myöhemmin tämän luvun tekstissä ja kuvioissa. Osapuolet ovat XML-sanomien tietokenttiä ja tärkeitä maksuaineiston muodostamisen kannalta. Asiakkaan ja pankin välinen viestinvaihto muodostuu useista sanomista varsinaisen maksusanoman lisäksi. Pankki muun muassa muodostaa maksusanomalle aina palautesanoman ja maksamisen jälkeen on mahdollista saada tiliote. (SWIFT 2009, hakupäivä 19.2.2011.)

TAULUKKO 1. Viestinvaihdon osapuolten ISO-käsitteet (Finanssialan Keskusliitto 2010a, 2)

ISO 20022	Käännös	Kuvaus
Debtor	Tilinomistaja, maksaja, ostaja	Osapuoli, jonka tililtä maksu veloitetaan.
Ultimate Debtor	Alkuperäinen laskun saaja/maksaja	Osapuoli, joka alun perin on ostanut tavaraa tai palvelua ja jolle myyjä on toimittanut laskun. Ultimate Debtorina käytetään, kun laskun saaja on eri osapuoli kuin maksaja.
Initiating Party	Toimeenpanija	Osapuoli, jonka aloitteesta maksuaineisto muodostetaan. Tämä voi olla maksaja itse, agenttuuri tai yrityksen oma palvelukeskus.
Creditor	Maksun saaja, myyjä	Osapuoli, jonka tilille maksu maksetaan.
Ultimate Creditor	Lopullinen saaja	Osapuoli, joka on maksun lopullinen saaja. Esimerkiksi maksu maksetaan rahoitusyhtiön tilille, mutta lopullinen saaja on rahoitusyhtiön asiakas.
Debtor Agent	Maksajan pankki	Osapuoli on maksajan tilipankki.
Creditor Agent	Saajan pankki	Osapuoli on saajan tilipankki.

Kuviossa 3 on kuvattu C2B-maksamiseen liittyvä viestinvaihto maksamisen osapuolten välillä yksinkertaisimmillaan. Tämän maksuprosessin perustapauksen osapuolia ovat maksaja, maksun saaja sekä näiden kahden pankit. Kuviossa ei ole erikseen määritelty, käytetäänkö tilisiirrossa lopullista maksun saajaa tai alkuperäistä maksajaa. Niiden käyttö ei vaikuta maksuprosessin kulkuun. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 3. Normaali maksusuoritus (SWIFT 2009, hakupäivä 19.2.2011)

Viestinvaihto alkaa sillä, että maksaja laittaa maksamisprosessin alulle lähettämällä C2B-maksuaineiston omalle pankilleen (1, Customer Credit Transfer Initiation). Tämän jälkeen pankki lähettää maksajalle kaksi viestiä: raportin maksun tilasta (2, Customer Payment Status Report) ja ilmoituksen tiliä koskevista veloituksista (3, Bank-To-Customer Debit/Credit Notification). Viestien lähettämisen jälkeen sekä maksajan että maksun saajan pankit keskustelevat keskenään (4), jonka jälkeen maksun saaja saa ilmoituksen omalta pankiltaan tililleen tehdyistä hyvityksistä (5, Bank-To-Customer Debit/Credit Notification). Viestinvaihto päättyy siihen, että maksaja ja maksun saaja saavat omilta pankeiltaan tiliotteen (6, Bank-To-Customer Account Report tai Statement). (SWIFT 2009, hakupäivä 19.2.2011.)

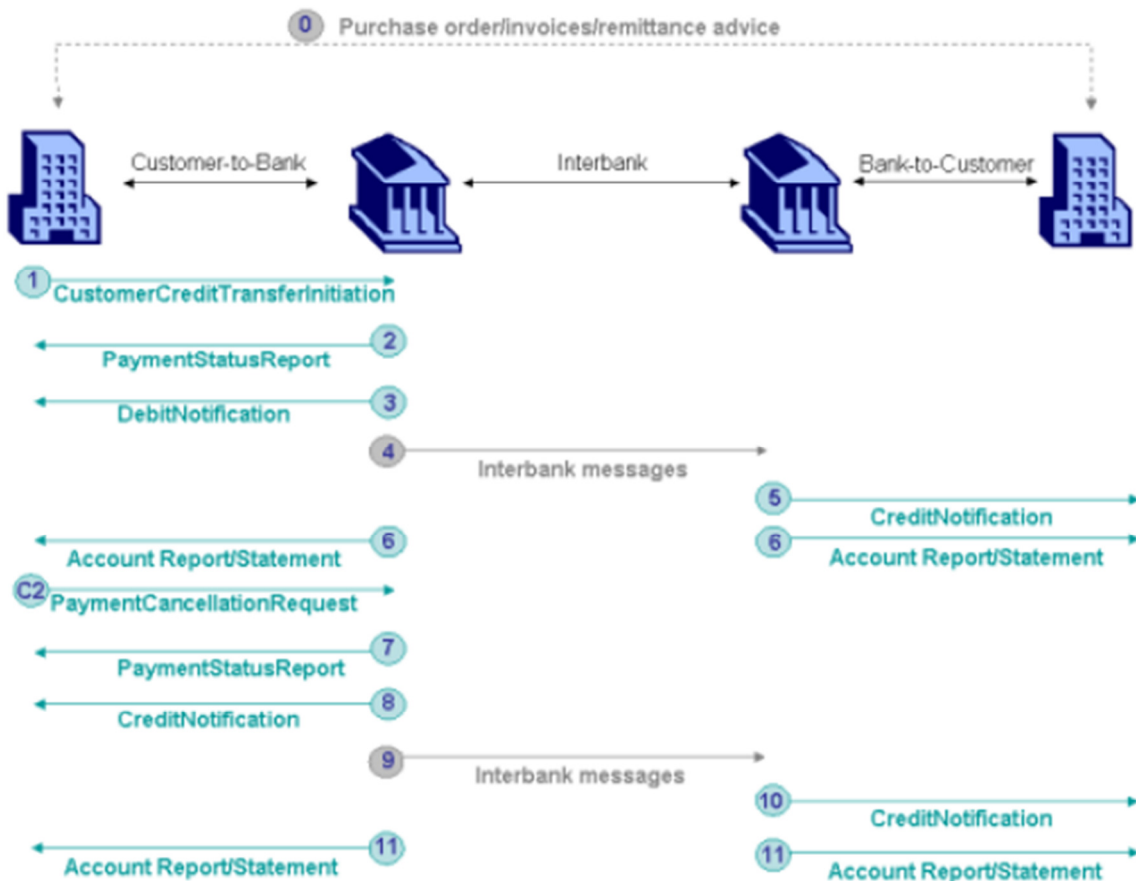
Yllä esitetyn maksuprosessin perustapauksen lisäksi on olemassa erilaisia poikkeustapauksia. Kuviossa 4 kuvataan maksun peruuttaminen ennen kuin maksu on toimeenpantu, eli ennen kuin maksun saaja on saanut rahat tililleen. Tässä tapauksessa viestinvaihto on ensimmäisen kolmen kohdan osalta sama kuin edellisessä tapauksessa. Seuraava kohta on kuitenkin erilainen, koska maksajan pankki ei ole ehtinyt ottaa yhteyttä maksun saajan pankkiin. Pankkien välisen

yhteydenpidon sijaan maksaja lähettääkin maksun peruutuspyynnön omalle pankilleen (C1, Customer Payment Cancellation Request). Peruutuspyynnön käsittelyn jälkeen maksajan pankki lähettää maksajalle raportin maksun tilasta (4, Customer Payment Status Report), jolloin maksaja tietää, että maksu on nyt peruutettu. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 4. Maksu peruutetaan ennen maksun toimeenpanoa (SWIFT 2009, hakupäivä 19.2.2011)

Toinen maksuprosessin erikoistapaus on maksun peruuttaminen maksun toimeenpanon jälkeen. Tällöin rahat ovat jo saapuneet maksun saajan tilille, jonka jälkeen ne palautetaan takaisin maksajalle. Tämä erikoistapaus on esitetty kuviossa 5 KUVIO 5. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 5. Maksu peruutetaan maksun toimeenpanon jälkeen (SWIFT 2009, hakupäivä 19.2.2011)

Kun maksu peruutetaan maksun toimeenpanon jälkeen, viestinvaihto on kaikkien kuuden ensimmäisen kohdan osalta sama kuin maksuprosessin perustapauksessa. Peruuttaakseen maksunsa tiliotteen saamisen jälkeen, maksajan on lähetettävä omalle pankilleen maksun peruutuspyyntö (C2, Customer Payment Cancellation Request). Pankki vastaa tähän lähettämällä maksajalle raportin maksun tilasta (7, Customer Payment Status Report) sekä ilmoituksen tilille tehdyistä hyvityksistä eli maksujen palautuksista (8, Bank-To-Customer Debit/Credit Notification). Sitten maksajan pankki lähettää viestin maksun peruutuksesta maksun saajan pankkiin (9), jolloin maksun saaja saa ilmoituksen tililleen tehdyistä veloituksista (10, Bank-To-Customer Debit/Credit Notification). Lopuksi maksaja ja maksun saaja saavat omilta pankeiltaan tiliotteen (11, Bank-To-Customer Account Report tai Statement). (SWIFT 2009, hakupäivä 19.2.2011.)

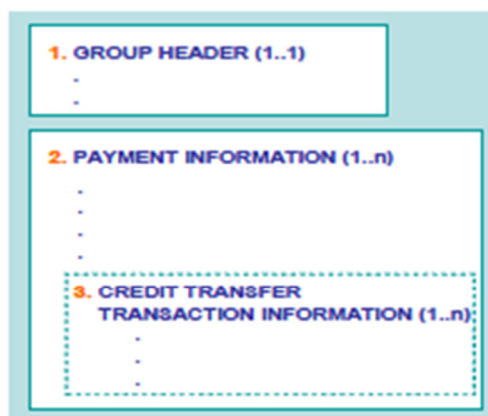


### 3.1 SEPA-tilisiirto

SEPA-tilisiirtoa eli C2B-maksua (tekniiseltä nimeltään Customer Credit Transfer Initiation, pain.001) käytetään varojen siirtämisessä maksajalta maksun saajalle. Se lähetetään maksajan toimesta pankille ja pankki prosessoi sen eteenpäin maksun saajalle. (SWIFT 2009, hakupäivä 19.2.2011.)

Sanomaa voi käyttää epäsuorasti, jolloin velallinen ei lähetä sitä suoraan pankille vaan huolitsijalle, joka välittää sen eteenpäin pankille. Esimerkiksi tytäryhtiö voi lähettää maksun pääkonttoriin, joka hoitaa maksamisen. Sama epäsuoruus on mahdollista myös vastaanottavassa päässä, eli maksut voidaan maksaa kootusti pääkonttorille, vaikka tytäryhtiö olisi velkojana. (SWIFT 2009, hakupäivä 19.2.2011.)

C2B-sanoman rakenne on esitetty kuviossa 6. Siitä näkyy, että sanoma koostuu kolmesta osasta: Group Headerista, Payment Informationista ja Credit Transfer Transaction Informationista (SWIFT 2009, hakupäivä 19.2.2011).



KUVIO 6. C2B-maksusanoman rakenne (SWIFT 2009, hakupäivä 19.2.2011)

Group Header pitää sisällään sanoman yhteiset tunnistetiedot, ja se saa esiintyä sanomassa ainoastaan kerran. Yhteisiä tunnistetietoja ovat muun muassa sanoman yksilöivä viite, rakenteen kuvaus ja luontiaika. (Finanssialan Keskusliitto 2010a, 4.)

Payment Information -elementti sisältää veloitukseen liittyvät tiedot. Sen on esiinnyttävä maksusanomassa vähintään yhden kerran, mutta rakenteen kuvauksesta riippuen se voi näkyä useamminkin. Payment Informationilla välitetään muun muassa maksajan nimi, maksutili,

maksutyyppi ja eräpäivä. Kun jokin edellisistä tiedoista vaihtuu, elementti toistetaan uusilla tiedoilla, esimerkiksi kun jokin maksuista halutaan suorittaa toiselta pankkitililtä tai jonkin maksun eräpäivä on eri kuin muiden. (Finanssialan Keskusliitto 2010a, 4.)

Credit Transfer Transaction Information on Payment Informationin sisällä oleva elementti, jota on pakko olla vähintään yksi jokaisessa Payment Informationissa. Elementti pitää sisällään maksuun liittyvät tiedot, joita ovat esimerkiksi saajan nimi, pankki ja tili sekä laskun yksilöintitiedot. (Finanssialan Keskusliitto 2010a, 4.)

C2B-maksusanoman rakenne mahdollistaa sen, että yhdessä pankille lähetettävässä tiedostossa on yhden tai useamman maksajan tiedot, ja yhtä maksajan tietoa kohden on yhden tai useamman maksun tiedot. Yhdistettynä tämä rakenne epäsuoraan maksamiseen, C2B-maksulla voidaan tehdä useita erilaisia maksutapauksia, jotka on kuvattu kuvioissa 7–12. Niissä esitellään viisi erilaista tilannetta SEPA-tilisiirrolla maksamisesta. Maksutilanteissa 2–5 hyödynnetään C2B-maksun epäsuoraa maksutapaa. Kuvioissa esiintyy lopullinen maksun saaja, mutta tilanteet voidaan toteuttaa myös ilman sitä. (SWIFT 2009, hakupäivä 19.2.2011.)

Kuviossa 7 kuvataan yksinkertaisin maksamistilanne, jossa maksaja on samalla alkuperäinen maksaja ja maksun saaja on lopullinen maksun saaja. Alkuperäistä maksajaa ja lopullista maksun saajaa ei siis tarvitse erikseen määritellä, koska ne ovat samat kuin maksaja ja maksun saaja. Maksaja lähettää C2B-maksusanoman pankilleen käsiteltäväksi, jonka jälkeen rahat ovat maksun saajan käytössä. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 7. C2B-maksamisen ensimmäinen maksutapaus (SWIFT 2009, hakupäivä 19.2.2011)

Toinen maksutilanne (kuvio 8) on hyvin yleinen esimerkiksi palvelukeskusmallia käytettäessä. Tässä tilanteessa pääkonttori hallinnoi tiliä, jolta rahat veloitetaan, mutta maksu suoritetaan tytäryhtiön puolesta. (SWIFT 2009, hakupäivä 19.2.2011.) Finanssialan Keskusliitto mainitsee esimerkkinä tapauksen, jossa yrityksen tytäryhtiö vastaanottaa laskun, josta emoyhtiö muodostaa

maksuaineiston ja maksaa laskun omalta tililtään. Maksun saaja voi esimerkiksi olla rahoitusyhtiö, jonka tilille maksu maksetaan, mutta lopullinen saaja on rahoitusyhtiön asiakas. (2010a, 3.)



KUVIO 8. C2B-maksamisen toinen maksutapaus (SWIFT 2009, hakupäivä 19.2.2011)

Kuvio 9 laajentaa C2B-maksamisen toista maksutapausta. Kuviossa on esitetty, miten pääkonttori maksaa laskut usean tytäryhtiön puolesta usealle velkojalle. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 9. C2B-maksamisen toinen maksutapaus, jossa useita alkuperäisiä maksajia (SWIFT 2009, hakupäivä 19.2.2011)

Kuvion 10 esittämä kolmas tilanne on myös hyvin yleinen. Siinä maksutili on sen osaston hallussa, joka on myös velvollinen maksamaan laskun, mutta maksu suoritetaan pääkonttorin toimesta tätä tiliä käyttäen. Näin pääkonttori ottaa vastuun velasta. (SWIFT 2009, hakupäivä 19.2.2011.) Erona toiseen maksutilanteeseen, jossa vain yhdellä organisaation osastolla on maksutili, jokaisella osastolla on omat tilinsä. Näitä tilejä hallinnoidaan kuitenkin keskitetysti pääkonttorista, joka hoitaa laskutuksen muiden osastojen puolesta näiden omilta tileiltä. Finanssialan Keskusliiton (2010a, 3) esimerkissä yrityksen emoyhtiö muodostaa maksuaineiston tytäryhtiön puolesta, mutta maksu kuitenkin veloitetaan tytäryhtiön tililtä.



KUVIO 10. C2B-maksamisen kolmas maksutapaus (SWIFT 2009, hakupäivä 19.2.2011)

Neljäs maksutapaus (kuvio 11) on hyvin samankaltainen kolmannen tapauksen kanssa, mutta tässä maksutilin omistaja on vastuussa velasta. Palvelukeskus siis suorittaa maksun velallisen puolesta, mutta ei ota mitään vastuuta velasta. (SWIFT 2009, hakupäivä 19.2.2011.)



KUVIO 11. C2B-maksamisen neljäs maksutapaus (SWIFT 2009, hakupäivä 19.2.2011)

Viidennessä tilanteessa (kuvio 12) yrityksen tytäryhtiö on alkuperäinen velallinen. Maksutilin omistaa pääkonttori, joka ei kuitenkaan suorita maksua, vaan sen tekee palvelukeskus (Shared Service Center). (SWIFT 2009, hakupäivä 19.2.2011.) Finanssialan Keskusliiton (2010a, 3) esimerkissä yrityksen palvelukeskus muodostaa maksuaineiston, jossa tytäryhtiölle osoitettu lasku veloitetaan emoyhtiön tililtä.



KUVIO 12. C2B-maksamisen viides maksutapaus (SWIFT 2009, hakupäivä 19.2.2011)

### 3.2 SEPA-tilisiirron palautesanoma

C2B-palautesanoma (tekniiseltä nimeltään Payment Status Report, pain.002) on C2B-maksusanomaa vastaava palautesanoma, jota maksajan pankki käyttää tilisiirtojen maksutilan ilmoittamiseen maksajalle. Eri maksutiloja ovat muun muassa vastaanotettu, hyväksytty, hyväksytty muutoksilla, osittain hyväksytty, käsittelemätön ja hylätty. (SWIFT 2009, hakupäivä 19.2.2011.)

Maksutilat muuttuvat sitä mukaa, kun pankki prosessoi maksua eteenpäin. Saadessaan asiakkaan lähettämän maksusanoman prosessoitavaksi, pankki asettaa sanoman tilaksi RCVD (Received) eli "vastaanotettu". Tämän jälkeen pankki suorittaa sanomalle testit, joilla tarkistetaan sanoman muoto ja todennetaan sanoman lähettäjä. Mikäli nämä tarkistukset menevät läpi, asetetaan tilaksi ACTC (AcceptedTechnicalValidation) eli "hyväksytyt teknisestä tarkistuksesta". Seuraavaksi pankki tarkistaa asiakkaan profiiliin eli tekee muun muassa erilaiset rahanpesu- ja riskitarkistukset. Jos nämä menevät läpi, tilaksi asetetaan ACCP (AcceptedCustomerProfile) eli "hyväksytyt asiakkaan profiilitarkistuksesta". Profiilitarkistuksen jälkeen maksu odottaa suoritusta eräpäivämäärään asti, jolloin tarkistetaan, onko tilillä katetta. Mikäli katetta on, tilaksi asetetaan ACSP (AcceptedSettlementInProcess) eli "hyväksytyt ja maksaminen käynnissä". Kun rahat ovat päätyneet vastaanottajan tilille, tilaksi laitetaan ACSC (AcceptedSettlementCompleted), mikä tarkoittaa, että maksu on hyväksytyt ja maksaminen suoritettu. (SWIFT 2009, hakupäivä 19.2.2011.)

Tilaa ACCW (AcceptedWithChange), "hyväksytyt muutoksin", käytetään tilanteessa, jossa pankki on korjannut tarkistuksessa havaitun virheen. Maksaja on esimerkiksi voinut syöttää BIC-koodin väärin, jolloin pankki korjaa sen oikeaksi. (SWIFT 2009, hakupäivä 19.2.2011.)

Maksu voidaan myös hylätä, jolloin sen tilaksi asetetaan RJCT (Rejected) eli "hylätty". Hylkäämisen syy annetaan erillisenä koodina. Tämä tila päättää maksun prosessoinnin ja maksajan täytyy lähettää uusi, korjattu maksusanoma. Jos palautesanoma sisältää sekä hyväksytyt että hylättyjä maksuja, tilaksi asetetaan PART (PartiallyAccepted) eli "hyväksytyt osittain". (SWIFT 2009, hakupäivä 19.2.2011.)

Mikäli maksusanoma odottaa lisäselvityksiä, sille asetetaan tilaksi PDNG (Pending) eli "käsiteltävänä". Käsitelysyy voidaan antaa erillisenä koodina. Lisäselvitysten saavuttua, tila päivitetään vastaamaan todellista tilaa. On myös mahdollista, että osa sanomista jää odottamaan lisäselvityksiä osan mennessä läpi, jolloin tilaksi asetetaan PART. (SWIFT 2009, hakupäivä 19.2.2011.)

### **3.3 Muut sanomat**

*Bank-To-Customer Debit/Credit Notification (camt.054)* -sanoma sisältää tiliä koskevat erittelytapahtumat, mutta ei saldotietoja (Finanssialan Keskusliitto 2010b, 2). Näitä erittelytapahtumia

ovat muun muassa tiliä koskevat veloitukset (Debit) ja hyvitykset (Credit) (SWIFT 2009, hakupäivä 19.2.2011).

Pankki raportoi tilitapahtumat asiakkaalle kahdella eri sanomalla. *Tiliraporttia* (Bank-To-Customer Account Report, camt.052) käytetään päivän sisäisten tapahtumien ja saldojen raportointiin (Finanssialan Keskusliitto 2010b, 2). *Tilילותesanomaa* (Bank-To-Customer Statement, camt.053) on Suomen kirjanpitolautakunnan hyväksymä virallinen tiliote, jota käyttäen pankki raportoi kirjatusta tilitapahtumista, mahdollisista erittelytapahtumista sekä saldotiedoista (Finanssialan Keskusliitto 2010c, 2).

Kun maksaja haluaa peruuttaa jonkin omista maksuistaan, hän lähettää *maksun peruutuspyynnön* (Payment Cancellation Request, pain.006) omaan pankkiinsa (SWIFT 2009, hakupäivä 19.2.2011). Tämän sijasta voidaan käyttää myös uudempaa Customer Payment Cancellation Request (camt.055) -peruutuspyyntöä (International Organization for Standardization 2011, hakupäivä 20.2.2011).

## 4 WEB SERVICES -PALVELUT

Euroopan maksuneuvosto on yhdessä kansainvälisen standardoimisjärjestön kanssa määritellyt ISO 20022 -maksusanomastandardin, mutta ei sitä, miten maksut välitetään asiakkaalta pankille ja pankilta asiakkaalle. SEPA-maiden pankit ovat kehittäneet omat maksujen vastaanottamiseen ja palautesanomien lähettämiseen tarkoitetut järjestelmänsä. Suomessa Nordea, OP-Pohjola-ryhmä ja Sampo Pankki (2008, 5) ovat sopineet Web Services (WS) -palveluun nojaavan yhteiskäytännön käyttöönotosta. WS on ohjelmistojärjestelmä, joka mahdollistaa tietokoneiden välisen vuorovaikutuksen tietoverkon yli (W3C 2011a, hakupäivä 25.4.2011). Edellä mainitut pankit ovat tehneet yhteisen Web Services -dokumentin, jossa määritellään muun muassa WS-palvelun tietoturvaan koskevat asiat sekä yksityiskohtaiset tiedot palvelussa tarvittavista XML-skeemoista ja WSDL (Web Services Definition Language) -sanomakuvauksesta. Tämän määrittelyn lisäksi kukin pankki julkaisee omat määrittelynsä PKI (Public Key Infrastructure) -tietoturvaratkaisun käytöstä eritoten siltä osin, miten sertifikaatit välitetään asiakkaalle. Näissä määrittelyissä otetaan kantaa myös testipalveluihin, tuettuihin tiedostotyyppeihin sekä niihin XML-skeemojen tietoelementteihin, jotka voivat poiketa yhteisestä WS-dokumentista. (Nordea ym. 2008, 5–6.)

Pankkien käyttämän Web Services -palvelun tietoturvan tulee vastata erilaisiin vaatimuksiin. Ensinnäkin WS-palvelun pitää olla kansainvälisten standardien mukainen, jotta ohjelmistokehittäjät voivat kehittää ohjelmistoja, jotka kommunikoivat pankkien kanssa. Toisekseen kunkin pankin pitää voida valita luotettavat varmenteita myöntävät tahot (CA, Certificate Authority). Kolmanneksi salaukseen ja allekirjoitukseen käytettävien avainten tulee olla riittävän vahvoja, jotta niitä voidaan käyttää vielä vuosienkin päästä. Vaatimuksena on myös esimerkiksi XML-datan salausmahdollisuus. Lisäksi loppukäyttäjien tulee voida jakaa maksaminen kahteen osioon, maksusanoman luontiin ja WS-yhteyteen, jotta esimerkiksi WS-kanavan käyttö voidaan ulkoistaa. (Nordea ym. 2008, 7.)

### 4.1 Maksuliikennepalvelu

Pankkien sopimassa Web Services -palvelukuvauksessa on seitsemän eri komentoa. Komennoista käytetyimmät ovat UploadFile, jota käyttäen tiedostot voidaan lähettää pankkiin, DownloadFile, jota käytetään tiedoston lataamiseen pankin palvelimelta, ja DownloadFileList, jolla käyttäjä saa ladattua listan pankin palvelimella olevista tiedostoista. Näiden kolmen komennon

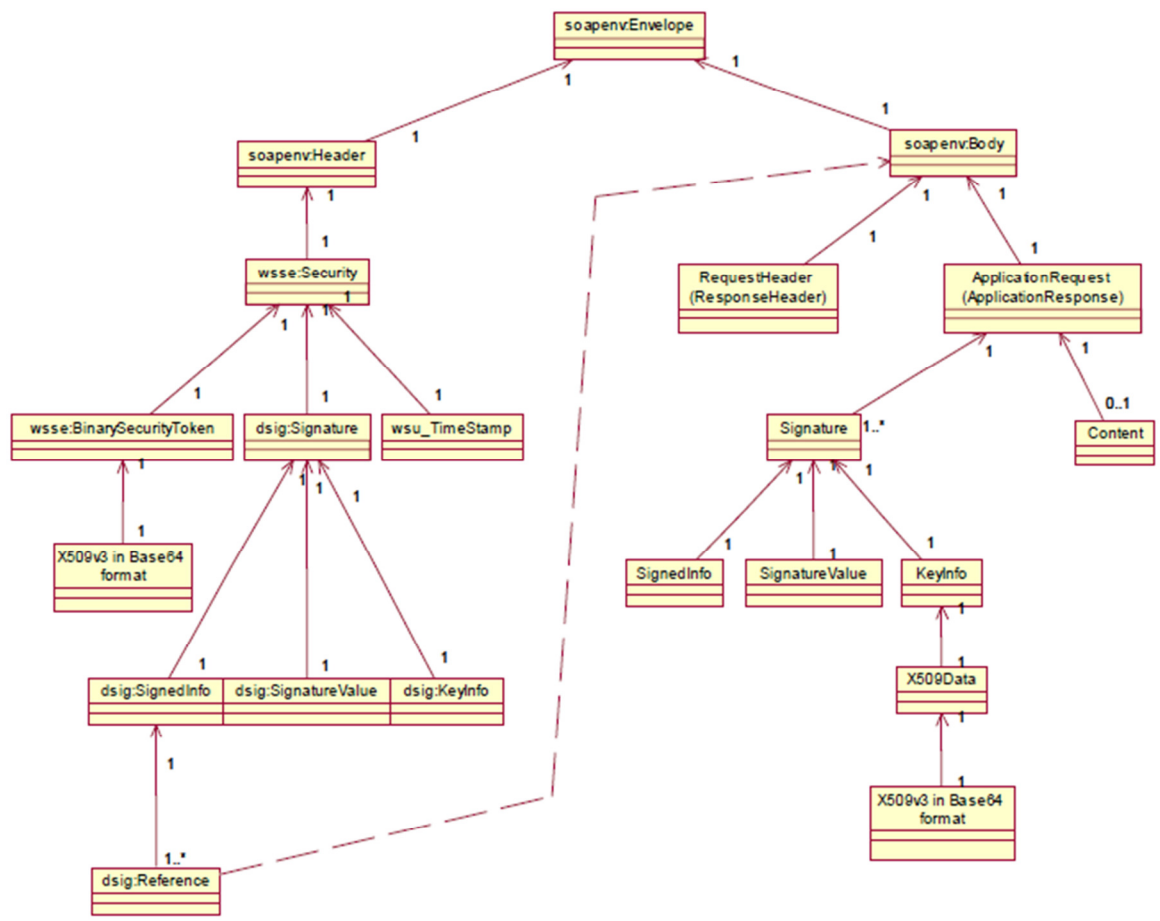
lisäksi on olemassa myös DeleteFile, jolla voidaan poistaa tiedosto, GetFileDetails, jolla saadaan jostain tiedostosta yksityiskohtaiset tiedot, ja GetUserInfo, jonka avulla voidaan hakea tietoa niistä tiedostotyypeistä, jotka käyttäjällä on oikeus noutaa pankista. Dokumentaatiossa on myös yksi tarkemmin määrittelemätön komento ConfirmFile. (Nordea ym. 2008, 24–25.)

Jotta näitä komentoja voidaan käyttää, on muodostettava SOAP-protokollan (Simple Object Access Protocol) mukainen sanoma (Nordea ym. 2008, 10). SOAP on XML-teknologiaa hyödynnävä rakenteellisen tiedon välittämiseen käytetty protokolla (W3C 2011b, hakupäivä 25.4.2011). Muodostetulla SOAP-sanomalla pankille välitetään komento ja komentoon liittyvät parametrit. Tähän sanomaan tulee pankilta palautteena komennon vastikkeen sisältävä SOAP-sanoma. (Nordea ym. 2008, 10–11.)

#### **4.1.1 SOAP-sanoma**

Pankkien Web Services -palveluun lähetettävän SOAP-sanoman rakenne esitetään kuviossa 13, josta näkyy myös tietojen pakollisuus sanomassa. Numero 1 tarkoittaa sitä, että tiedon on esiintyttävä vain yhden kerran. Merkintä 0..1 tarkoittaa, että tiedon esiintyminen ei ole pakollista, mutta jos se esiintyy, se saa esiintyä vain kerran. Merkinnällä 1..\* ilmaistaan, että tieto esiintyy vähintään kerran, mutta voi esiintyä myös useammin. (Nordea ym. 2008, 15.)





KUVIO 13. SOAP-sanoman rakenne (Nordea ym. 2008, 15)

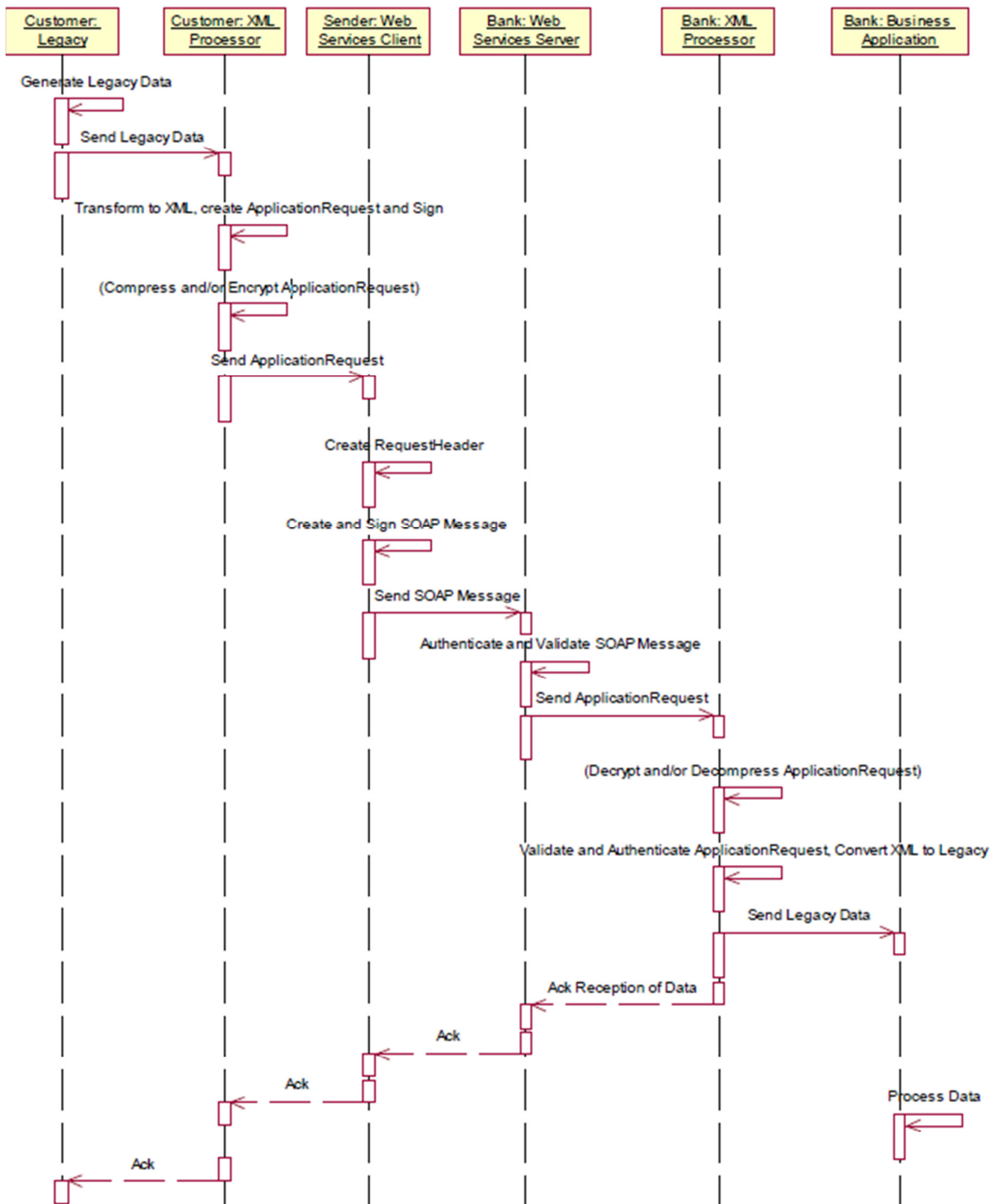
SOAP-sanoma koostuu kahdesta osasta: Headerista ja Bodysta. Headeriin tulevat SOAP-sanoman turvallisuuteen liittyvät tietokentät, kuten allekirjoitus ja aika, jolloin sanoma lähetettiin. Body jakaantuu pyyntösanomaa lähetettäessä kahteen tietokenttään, RequestHeaderiin ja ApplicationRequestiin, ja vastaussanomassa ResponseHeaderiin ja ApplicationResponseen. (Nordea ym. 2008, 15.)

Lähetettävän pyyntösanomassa RequestHeader-tietokenttä pitää sisällään pankille lähetettävään dataan liittyviä tunnistetietoja, kuten asiakkaan tunnistenumeron ja ajankohdan, jolloin sanoma on muodostettu. ApplicationRequest sisältää tiedot käytettävään komentoon liittyen. Esimerkiksi lisättäessä tiedostoa UploadFile-komennolla, ApplicationRequestin Content-tietokenttään sijoitetaan lähetettävä aineisto. Tai ladattaessa DownloadFileList-komennolla tiedostolistausta, ApplicationRequestiin voidaan määritellä päivämäärät, joiden välillä muodostetut tiedostot haetaan. (Nordea ym. 2008, 15.)

Paluusanoman mukana tuleva ResponseHeader sisältää muun muassa pankilta tulevan palautekoodin ja koodia vastaavan ilmoituksen tekstinä. Koodi kertoo, menikö pyyntö läpi vai ilmenikö sen käsittelyssä jokin virhe. ApplicationResponse pitää sisällään tiedot, jotka antavat palautteen asiakkaan tekemään pyyntösanomaan. Esimerkiksi DownloadFileList-komentoa vastaava ApplicationResponse sisältää listan pankin palvelimelta löytyneistä tiedostoista, jotka vastaavat pyyntösanoman tietoja, kuten ajankohtaa, jolloin ne on muodostettu. (Nordea ym. 2008, 29–38.)

#### **4.1.2 SOAP-sanoman muodostus ja elinkaari**

Kuviossa 14 esitetään SOAP-sanoman muodostaminen ja prosessointi lähetettäessä maksuaineistoa pankkiin. Siinä näytetään sekä asiakkaan (kuviossa Customer ja Sender) että pankin (kuviossa Bank) toimenpiteet maksusanoman muodostamisesta palautteen vastaanottamiseen. (Nordea ym. 2008, 10–11.)



KUVIO 14. SOAP-sanoman muodostaminen ja prosessointi (Nordea ym. 2008, 12)

Prosessi alkaa maksajan muodostaessa lähetettävän aineiston (Legacy Data). Tämä aineisto voi olla esimerkiksi C2B-maksusanoma. Aineisto välitetään XML-prosessorille, joka muodostaa siitä ApplicationRequestin ja allekirjoittaa sen, jonka jälkeen se voidaan pakata ja kryptata. Allekirjoitettu ApplicationRequest toimitetaan Web Services -ohjelmistolle, joka muodostaa sille RequestHeaderin. Lopuksi ApplicationRequestista ja RequestHeaderista muodostetaan SOAP-

sanoma, joka allekirjoitetaan lähettäjän yksityisellä avaimella ja lähetetään pankille https-yhteyden yli. (Nordea ym. 2008, 10–11.)

Pankin WS-palvelun tulee tarkistaa allekirjoituksen perusteella SOAP-sanoman muuttumattomuus ja lähettäjän aitous. Tämän jälkeen ApplicationRequest irrotetaan SOAP-sanomasta ja viedään pankin XML-prosessorille. Jos ApplicationRequestin sisällä ollut aineisto oli pakattu tai salattu, XML-prosessori purkaa pakkauksen tai salauksen. Sitten pankki tarkistaa ApplicationRequestin allekirjoituksen samalla tavoin kuin se tarkistaa SOAP-sanoman allekirjoituksen. Seuraavaksi aineisto verrataan XML-skeemaa vasten, millä varmistetaan, että kaikki tarvittavat tietoelementit löytyvät. Varmistuksen jälkeen XML-prosessori muuntaa aineiston muotoon, jota pankin muut järjestelmät ymmärtävät, ja lähettää sen eteenpäin niille. Lopuksi pankki generoi vastaussanoman ja lähettää sen asiakkaalle. (Nordea ym. 2008, 10–11.)

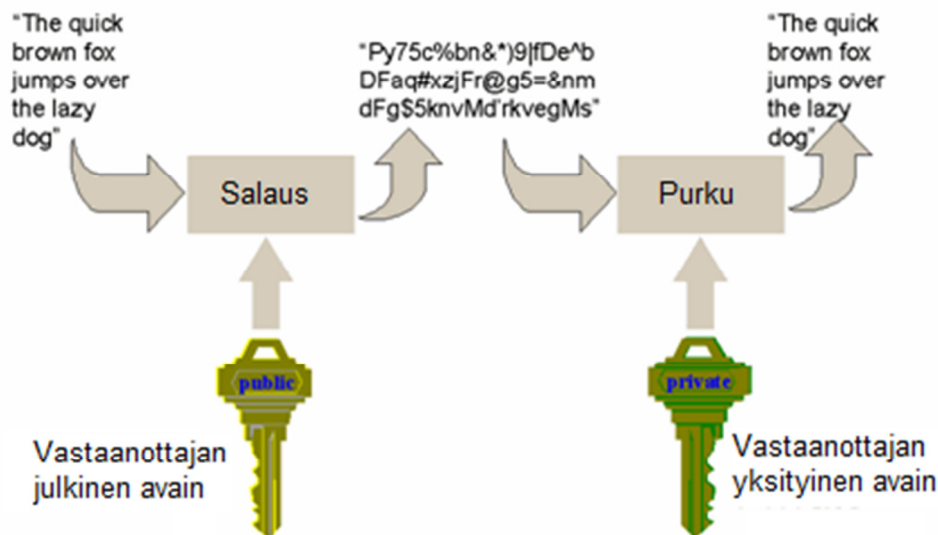
## **4.2 Tietoturva**

Nordean tietoturvaratkaisussa on kaksi osaa, joilla pyritään varmistamaan riittävän turvallinen maksuprosessi. Ensinnäkin kaikki pankin ja asiakkaan välinen liikennöinti tapahtuu salattua http-yhteyttä käyttäen. Http-yhteyden salaus hoidetaan SSL:ää (Secure Socket Layer) käyttäen ja Nordea vaatii, että SSL:n versio on vähintään 3.0. Toisekseen pankille lähetettävä ApplicationRequest pyyntö ja pankilta tuleva ApplicationResponse vastaus allekirjoitetaan. Näiden lisäksi myös SOAP-sanomat, joiden sisällä nämä pyynnöt ja vastaukset kuljetetaan, on allekirjoitettu. SOAP-sanoman allekirjoitukseen käytettävä avain voi olla eri kuin ApplicationRequestin avain. (Nordea 2010, 4.)

### **4.2.1 Julkisen avaimen menetelmä ja digitaalinen allekirjoitus**

Nordea käyttää viestien allekirjoittamiseen ja allekirjoitusten purkamiseen julkisen avaimen menetelmää eli PKI:ta (Public Key Infrastructure) (Nordea 2010, 3). Tämä tarkoittaa sitä, että sekä Nordea että asiakas muodostaa oman avainparinsa eli julkisen ja yksityisen avaimen. Cibernariumin mukaan julkinen avain julkistetaan ja lähetetään toiselle osapuolelle eli asiakas lähettää oman julkisen avaimensa pankille ja pankki omansa asiakkaalle. Yksityinen avain pidetään vain omana tietona. Jos sen yksityisyys vaarantuu, on vaarassa koko tietoturva. PKI pohjautuu siihen, että yksityistä avainta ei ole mahdollista päätellä julkisen avaimen ja käytetyn algoritmin avulla. (2011a, hakupäivä 1.4.2011.)

Julkisen avaimen menetelmän toimintaperiaate ilmenee kuviossa 15. Viestinvaihdossa viestin lähettäjä salaa viestin vastaanottajalta saamallaan julkisella avaimella. Vastaanottaja purkaa tämän salauksen omalla yksityisellä avaimellaan. (Cibernarium 2011a, hakupäivä 1.4.2011.)



KUVIO 15. PKI:n toimintaperiaate (muokattu lähteestä Petri 2009, hakupäivä 1.4.2011)

Nordea edellyttää, että maksuliikennettä koskevat lähetetyt SOAP-sanomat ja Application-Requestit on allekirjoitettu digitaalisesti (Nordea 2010, 9). Näissä allekirjoituksissa sovelletaan julkisen avaimen menetelmää, ja tällä tavoin varmistetaan viestien eheys. Tiivistealgoritilla (Hash) viestistä muodostetaan vakiomittainen tiiviste, jota ei enää voida muuntaa alkuperäiseksi viestiksi. Tämän jälkeen tiiviste salataan lähettäjän yksityisellä avaimella, ja tällä tavoin saatu digitaalinen allekirjoitus ja alkuperäinen viesti lähetetään vastaanottajalle. Vastaanottaja purkaa tiivisteeseen lähettäjän julkista avainta käyttäen ja tiivistää alkuperäisen viestin samalla tiivistealgoritilla. Jos vastaanottajan muodostama tiiviste on sama kuin lähettäjän tekemä, on viestin eheys varmistettu eli viesti on kulkenut verkon yli muuttumattomana. (Cibernarium 2011b, hakupäivä 1.4.2011.)

#### 4.2.2 Nordean varmennepalvelu

Nordean pankkipalvelu tarjoaa automatisoidun keinon Nordean julkisen avaimen noutamiseen Web Services -kanavaa käyttäen. Haettava julkinen avain pohjautuu varmenteen allekirjoituspyyntöön (Certificate Signing Request, CSR), jonka asiakkaan pankkiyhteisöohjelmisto muodostaa ja lähettää Nordealle. (Nordea 2010, 4.)

Julkisen avaimen hakeminen alkaa siten, että asiakas tekee pankin kanssa sopimuksen WS-yhteyden käytöstä. Sopimuksen teon jälkeen asiakas saa pankilta tekstiviestinä kymmennumeroisen aktivointikoodin, joka on voimassa seitsemän päivän ajan. Mikäli koodi ehtii vanheta, tulee asiakkaan hankkia uusi koodi Nordean asiakastuen kautta. (Nordea 2010, 5.)

Tämän jälkeen asiakkaan tulee hankkia tai muodostaa oma 1024-bittinen varmenne, joka sisältää sekä yksityisen että julkisen avaimen. Sitten varmenteesta muodostetaan PKCS#10-standardin mukainen allekirjoituspyyntö. Pyyntö tulee olla DER-koodattu, ja sen algoritmina tulee olla SHA-1. PKCS#10:stä ja tekstiviestinä saadusta aktivointikoodista muodostetaan HMAC-tunnistieto, jonka avulla varmennetaan allekirjoituspyynnön lähettäjä ja pyynnön sisällön muuttumattomuus. (Nordea 2010, 5.)

HMAC:sta ja allekirjoituspyynnöstä muodostetaan Nordean CertApplicationRequest-XML-skeeman mukainen varmennepyyntö. Tämä pyyntö lähetetään Nordean varmennepalvelun WS-kanavaan allekirjoittamattoman SOAP-sanoman sisällä. Paluuviestinä tulee CertApplicationResponse-XML-skeeman mukainen vastaus, joka sisältää julkisen avaimen, jota käytetään yhdessä aiemmin muodostetun yksityisen avaimen kanssa. (Nordea 2010, 5–6.) Tällöin PKI-tietoturvamenetelmä toteutuu eli asiakkaalla on oma yksityinen avain ja pankin julkinen avain, ja pankilla on asiakkaan julkinen avain ja oma yksityinen avain.

## 5 TULOKSET

Euroopan keskuspankin, Finanssialan Keskusliiton ja Nordean dokumentaatioiden pohjalta kehitettiin luokkakirjasto, jolla voidaan muodostaa ja maksaa SEPA-tilisiirtoja. Kehitysympäristönä oli .NET Framework 2.0 ja työkaluna Visual Studio 2008 ja myöhemmin 2010. Ohjelmointikielenä käytettiin VB.NET:iä. Vaikka .NET Frameworkista olisi ollut tarjolla versio 4.0, päädyttiin 2.0:aan, koska tämän rajapinnan ohjelmointiratkaisut eivät vaatineet uudempaa versiota. Tällöin asiakkaiden ei tarvitse tämän luokkakirjaston vuoksi päivittää .NET Frameworkia.

### 5.1 Luokkakirjastojen toteutus

Luokkakirjasto jaettiin kahteen moduuliin: SepaContentiin ja SepaBankiin. SepaContentin tarkoitus oli muodostaa aineisto. SepaBank oli yhteydessä pankin maksuliikenne- ja varmennepalveluun.

SepaContentia tehdessä tuli ottaa huomioon ISO 20022 -standardin sanomakuvaukset. Näiden sanomakuvausten XML-skeematiedostojen pohjalta toteutettiin luokat pain.001 ja pain.002 -sanomista. Nämä luokat serialisoimalla saatiin muodostettua C2B-maksuaineistot XML-muotoisina tiedostoina, jollaisia niiden piti olla pankille lähetettäessä.

Liitteenä 1 on SepaContentia käyttäen muodostettu C2B-maksuaineisto XML-muodossa. Siinä esiintyy yksi jokaista sanoman osiota eli yksi Group Header (GrpHdr) ja yksi Payment Information (PmtInf), jonka sisällä on yksi Credit Transfer Transaction Information (CdtTrfTxInf). Maksajana on kuvitteellinen saksalainen Maksaja Oy, jonka IBAN-muotoinen tilinumero on DE0252910820037221 ja pankin BIC-tunnistetiето GERMBANK. Maksun saajana on kuvitteellinen ranskalainen Ostaja Oy. Maksettava summa on sadan euron suuruinen.

Euroopan keskuspankki saattaa julkaista lisää sanomia tai sanomista uusia versioita. Tämän ja opinnäytetyön rajausten vuoksi SepaContentin yhtenä tärkeänä vaatimuksena oli, että sen pitää olla helposti muokattavissa jälkeenpäin. Sanomia tulee voida lisätä ja päivittää uusiin versioihin nopeasti ja vähällä vaivalla. Tämä vaatimus saavutettiin opinnäytetyössä hyvin. Sanomia on helppo lisätä, mutta ne ovat sen verran erilaisia toisiinsa nähden, että niiden lisäämisestä aiheutuu jonkin verran ohjelmointityötä. Suurimman työn aiheuttaa kuitenkin sanomien tieto-

kenttiin ja eri pankkien vaatimuksiin tutustuminen, koska joissain sanomissa pankit eivät käytä samoja tietokenttiä täysin samalla tavalla tai jättävät joitain käyttämättä.

SepaContent oli erillinen moduuli SepaBankista muun muassa syystä, että sanomia saatetaan muokata ja lisätä, mutta pankkirajapinnan ei uskota muuttuvan. Toisaalta rajapinta saattaa muuttua, mutta sanomakuvaukset pysyvät samana. Kun päivitettäviä moduuleita on vähemmän, ohjelmistopäivityksiä on helpompi jakaa asiakkaille.

SepaBank-moduuli toimii rajapintana BookMaster Laskutus 2011 -ohjelmiston ja Nordean maksuliikenne- ja varmennepalvelun välillä, ja näin ollen se sisältää CertApplicationRequest ja ApplicationRequest -skeemat. Sen tehtävä on lähettää ja vastaanottaa SOAP-sanomia. Moduulin kehittämisessä käytettiin apuna Microsoftin Web Services Enhancements (WSE) -luokkakirjaston versiota 3.0. Tämä kirjasto toi tarvittavia toimintoja SOAP-sanoman muodostamiseen, etenkin sanoman allekirjoittamisen osalta. Myös Windows Communication Foundationin (WCF) käyttöä mietittiin, mutta WSE:hen löytyi hyviä esimerkkejä, jotka vastasivat tämän luokkakirjaston tarpeita. Lisäksi WCF olisi vaatinut .NET Frameworkin version 3.0.

SepaBankin varmenteen muodostus ja haku noudattaa Nordean automatisoidun varmenteen-hakupalvelun ohjeistusta. SepaBank muodostaa itse oman 1024 bittisen x509v3-muotoisen varmenteen, joka pitää sisällään sekä julkisen että yksityisen avaimen. Tästä varmenteesta muodostetaan PKCS#10-standardin mukainen allekirjoituspyyntö, jonka algoritmina on SHA-1. Pyyntö sijoitetaan Nordean CertApplicationRequestin Content-tietokenttään DER-koodattuna. Tästä pyynnöstä ja käyttäjän antamasta aktivointikoodista lasketaan HMAC-tunnistetieto, joka sijoitetaan sille tarkoitettuun kenttään CertApplicationRequestissa. Tämän jälkeen SepaBank lähettää CertApplicationRequestin allekirjoittamattoman SOAP-sanoman sisällä pankille ja vastaanottaa paluuviestinä tulleen SOAP-sanoman ja sen sisältä CertApplicationResponseen. Tämä sisältää julkisen avaimen, joka yhdistetään aiemmin itse luotuun yksityiseen avaimeen ja tallennetaan asiakkaan tietokoneelle myöhempää käyttöä varten.

HMACin laskemiseen tarvittavat funktiot löytyivät .NET 2.0:n Security-kirjaston Cryptography-nimiavaruudesta, mutta muissa varmenteeseen liittyvissä toiminnoissa käytettiin apuna kahta kolmannen osapuolen luokkakirjastoa. Varmenteen ja PKCS#10-allekirjoituspyynnön muodostamisessa ja DER-koodauksessa käytettiin apuna Bouncy Castle Crypto API:a. Varmenteiden yhdistämisessä käytettiin apuna OpenSSL-kirjastoa. Molempien kirjastojen sopimusehdot



todettiin sellaisiksi, että niitä voi käyttää apuna luokkakirjastoja tehdessä, vaikka kirjasto tulikin osaksi kaupallista ohjelmistoa.

Avaimen muodostamisen jälkeen käyttäjän on mahdollista lähettää pankkiin tai noutaa pankista aineistoja. SepaBankin maksuliikenneyhteys Nordeaan alkaa siten, että SepaContentilla muodostettu XML-muotoinen aineisto asetetaan ApplicationRequestin sisälle Content-elementtiin. Myös muut ApplicationRequestin sisältämät elementit täytetään laskutusohjelmalta tulevien syötteiden mukaisesti. Osan syötteistä antaa käyttäjä, mutta suurin osa syötteistä annetaan automatisoidusti laskutusohjelman asetuksista. Valmis ApplicationRequest allekirjoitetaan käyttäjän aiemmin muodostamalla avaimella. Tämän jälkeen muodostetaan RequestHeader ja koodataan ApplicationRequest base64-muotoon. Lopuksi ohjelmisto kutsuu WS-palvelun UploadFile-funktiota, jolle välitetään parametrina RequestHeader ja ApplicationRequest. SOAP-sanoman muodostus jätetään .NET Frameworkin tehtäväksi. Ainoastaan allekirjoituksen lisäämisessä kirjoitetaan jonkin verran koodia ja käytetään apuna WSE:n luokkia ja funktioita.

Liitteessä 2 on SepaBankilla muodostettu ja pankkiin lähetetty SOAP-sanoma. Käyttäjätunnuksena on Nordean testitunnus ja allekirjoitukseen on käytetty Nordean testivarmennetta. Joitain base64-koodattuja kohtia liitteessä on lyhennetty poistamalla niistä merkkejä.

Pankilta tulee vastauksena SOAP-sanoma, jonka allekirjoitus tarkistetaan käyttäjän varmennetta vasten, jotta tiedetään, että sanoman sisältö ei ole muuttunut matkalla. Vastauksen ResponseHeaderista tarkistetaan, että pyyntösanomassa ei ole ilmennyt virheitä. Jos pankilta on noudettu tiedosto DownloadFile-komennolla, tiedosto puretaan ApplicationResponsein Content-tietokentästä, ja se palautetaan laskutusohjelmistolle, joka esimerkiksi näyttää sen käyttäjälle tai käyttää SepaContentia jonkin tiedon saamiseen aineistosta.

Tilisiirtoaineiston lähettämisen jälkeen pankilta on noudettavissa aineiston pain.002-muotoinen palautesanoma. Laskutusohjelmisto hakee palautesanoman rajapintaa käyttäen kun käyttäjä haluaa päivittää maksujensa tilan nähdäkseen esimerkiksi onko jonkin maksun prosessoinnissa tapahtunut virheitä. Noutaminen tapahtuu siten, että haetaan DownloadFileList-komennolla tiedot kaikista pankin palvelimella odottavista komennosta, jonka jälkeen ne voidaan ladata DownloadFile-komennolla.

## 5.2 Luokkakirjastojen testaus

Opinnäytetyöhön kuului myös toteutetun luokkakirjaston testaus. Jo kehitysvaiheessa tehtiin paljon testausta, kun tarkistettiin, toimiiko jokin toteutettu osa niin kuin sen oletettiin toimivan. Yksikkötestausta tai vastaavaa ei suoritettu, vaan tehtiin testiohjelma, jolla eri osat testattiin. Ohjelma otti vastaan syötteitä ja muodosti niiden perusteella aineiston tai SOAP-sanoman ja tallensi sekä aineistot että pankin paluuviestit hakemistoon, josta tuloksia pystyi tarkastamaan ja käymään läpi.

SepaContentin testauksessa apuna käytettiin XML-sanomien muodon tarkistamista. Tämä tapahtuu siten, että muodostettua XML-aineistoa verrataan sen skeemaan. Skeemasta näkyy, mitä elementtejä aineistossa tulee esiintyä, ja jos XML-aineistossa esiintyy jotain muita kuin sallittuja elementtejä tai jokin vaadituista elementeistä puuttuu, niin aineisto ei mene tarkistuksesta läpi. Sampo Pankki tarjosi ilmaista työkalua tätä tarkoitusta varten, jota myös opinnäytetyön aikana hyödynnettiin.

SepaBankin testauksessa käytettiin apuna ohjelmia, joilla tarkkaillaan Internet-liikennettä. Tällainen ohjelma on esimerkiksi Fiddler. Se näyttää, mitä tietoja tietokoneelta lähtee http- ja https-liikenteen yli ja mitä vastaanotetaan. Tämä oli iso apu tilanteessa, jossa ei oltu täysin varmoja, millaisen SOAP-sanoman .NET Framework muodostaa tai miten WSE lisää allekirjoituksen siihen.

Lisäksi SepaBankin testaamiseen käytettiin SoapUI-ohjelmaa. Se mahdollistaa WSDL-sanomakuvausten nopean käytön ilman, että pitää kirjoittaa testiohjelma, joka toteuttaa WSDL-kuvauksen mukaisen WS-yhteyden. SoapUI muodostaa sanomakuvausten pohjalta SOAP-sanomat, joihin vaaditut tietokentät voi täyttää itse. Nämä SOAP-sanomat lähetetään ohjelmaa käyttäen pankille, jonka jälkeen ohjelma näyttää pankilta tulleen vastaussanoman. Lisäksi SoapUI:lla voidaan liittää allekirjoitus SOAP-sanomaan. Ohjelmaa käyttäen oli kätevä ensin rakentaa toimiva sanoma, ja sen jälkeen tehdä koodi, joka muodosti samanlaisen sanoman.

## 6 POHDINTA

Opinnäytetyön kehittämistehtävänä oli suunnitella ja toteuttaa luokkakirjasto, jota käyttäen pystyi muodostamaan SEPA-tilisiirtoja ja lähettämään ne Nordean Web Services -maksuliikennepalveluun. Kehittämistehtävän teossa onnistuttiin määritysten mukaisesti. Lopputuloksena syntyi kirjasto, joka suoriutui sille asetetuista tavoitteista.

Kehittämistehtävä oli minulle mielenkiintoinen, koska sille oli selkeä tarve. Sen vaatimukset tukivat opiskelujani, ja sitä tehdessäni opin lisää Web Serviceistä ja sovellusten tietoturvasta. Näiden asioiden ansiosta motivaationi oli korkealla työtä tehdessä. Aluksi toteutin luokkakirjastoa yksin, mutta myöhemmin myös toinen yrityksen työntekijöistä alkoi tehdä sitä. Hän muun muassa hoiti luokkakirjaston käyttöönoton BookMaster Laskutus 2011 -ohjelmistoon, ja auttoi myös SepaBankin toiminnallisuuden toteuttamisessa ja oli yhteydessä pankkien toimihenkilöihin.

Opin uusia asioita myös ohjelmistokehityksestä, osittain yrityksen ja erehdyksen kautta. Alussa olin liiankin innostunut kehitettävästä ohjelmasta, joten en suunnitellut riittävästi ennen ohjelmoinnin aloittamista. Tämän vuoksi jouduin tekemään joitain asioita uudestaan tai tein asioita, joita ei olisi tarvinnut tehdä. Ohjelmointityökalunan käytin minulle entuudestaan hyvin tuttuja Visual Studion versioita 2008 ja 2010. Visual Studion mukana tulevista työkaluista opin kuitenkin uutta. Esimerkiksi Visual Studio Command Prompt -työkalua käyttäen ajettu xsd-komento oli erittäin hyödyllinen, kun tein ISO 20022 -sanomakuvauksista luokat Visual Basic -kielelle.

Toisaalta hankaluuksien syynä olivat myös pankkien puutteelliset ohjeistukset ja muuttuvat menetelmät. Nordean tietoturvaratkaisut aiheuttivat kehitystyölle joitakin ongelmia. Dokumentaation mukaan varmenteet jaettiin loppukäyttäjille Internet-sivuston kautta, mutta myöhemmin Nordea muutti jakamisen täysin automatisoiduksi. Tämä lisäsi työmäärää jonkin verran, koska muutoksen myötä luokkakirjastoon piti ottaa mukaan myös tämän varmennepalvelun Web Services -palvelukuvaus ja toteuttaa varmenteen haku sitä vasten. Tämä oli kuitenkin samalla yksi palkitsevimista asioista työtä tehdessä, kun se saatiin toimimaan. Jos tietoturva-vaatimukset olisivat olleet tiedossa jo hyvissä ajoin, luokkakirjaston toteutus olisi ehkä jaettu kolmeen moduuliin: SepaBankiin, joka on yhteydessä pankin maksuliikennepalveluun, SepaContentiin,

joka muodostaa aineistot, ja SepaSecurityyn, joka hoitaa varmenteiden käsittelyn ja yhteyden pankkien varmennepalveluun.

Kokonaisuutena automatisoitu varmenteen haku oli iso haaste sen vuoksi, että siinä oli monta tekijää..NET Framework ei kyennyt yksistään suoriutumaan kaikista sen osa-alueista, joten avuksi jouduttiin ottamaan kaksi muuta kirjastoa, Bouncy Castle Crypto API ja OpenSSL. Ensimmäisellä toteutettiin varmenteen ja PKCS#10:n muodostus. OpenSSL:ää käytettiin muiden osien toteutukseen. Jälkikäteen tarkasteltuna pelkällä OpenSSL:llä olisi pärjätty, koska se pystyi samaan mihin Bouncy Castle Crypto API. Koska Bouncy Castle Crypto API otettiin ensi käyttöön, ei enää haluttu hylätä toimivaa koodia ja toteuttaa samaa asiaa OpenSSL:llä.

Myös pankkien puutteelliset testausympäristöt aiheuttivat ongelmia erityisesti työtä aloittaessa. Tästä sekä tietoturva vaatimusten erilaisuudesta johtuen työ piti rajata koskemaan vain yhtä pankkia, Nordeaa. Nordean testausjärjestelmät olivat kehittyneemmät kuin muiden pankkien. Esimerkiksi Sampo Pankilla testausaineisto piti lähettää sähköpostilla, jonka jälkeen sai sähköpostitse vastauksen aineiston oikeellisuudesta.

Raportin kolmannen luvun tärkein lähde oli englanninkielinen, ja se sisälsi paljon termejä, jotka olisivat auenneet paremmin finanssialalla työskentelevälle kuin ohjelmoijalle. Tämä aiheutti minulle hankaluuksia, mutta onneksi löysin Finanssialan Keskusliiton tekemän dokumentaation, jota käyttäen pystyin ymmärtämään alkuperäislähteen termit paremmin. Muuten kaikki englanninkielisetkin lähteet olivat selkeitä.

Työn alkuperäinen aikataulu oli todella tiukka, sillä suunnittelin tekeväni luokkakirjaston ja kirjoittavani raportin reilun kolmen kuukauden aikana. Osittain aikataulumuutokset johtuivat kehitystyön haasteista ja pankkien myöhästelystä, sillä SEPA:n käyttöönotto myöhästyi myös pankkien osalta ja vanhat järjestelmät toimivat vielä vuoden 2011 aikanakin. Lisäksi opinnäytetyön tekeminen siirtyi hetkeksi taka-alalle, kun sain SeBitti Oy:ltä työpaikan. Toteutin siellä aluksi muita työtehtäviä, jotka olivat kiireellisempiä kuin opinnäytetyön SEPA-luokkakirjasto. Vuoden 2010 syksyllä olin ulkomailla opiskelijavaihdossa, minkä aikana en tehnyt lainkaan opinnäytetyötä. Luokkakirjasto otettiin käyttöön keväällä 2011, ja opinnäytetyöraportin kirjoitin pääasiassa saman vuoden talven ja kevään aikana.

Tiedän, että rajapintaa kehitetään jatkossa siten, että se toimii myös muiden pankkien osalta. Tämä on nyt helppoa, kun kaikki vaatimukset toimivat yhden pankin osalta, ja sitä voi käyttää esimerkkinä. Oikeastaan ainoa haaste muiden pankkien osalta on erilaisissa varmennepalveluissa. Lisäksi jotkin tietoelementit ApplicationRequestissa voivat sisältää erilaista tietoa pankista riippuen. SepaContentiin lisätään myös tulevaisuudessa muita tarpeellisia sanomia, kuten tiliote.

Kokonaisuutena pidän opinnäytetyötäni opintojeni tärkeänä osana. Se antoi hyvän näkemyksen siitä, millaisia ohjelmistoja työelämässä tehdään. Lisäksi aiemmin oppimani asiat syventyivät työtä tehdessäni, mikä tuki ammatillista kehitystäni.

## LÄHTEET

Cibernarium. 2011a. Julkisen avaimen menetelmä. Hakupäivä 1.4.2011  
<http://www.cibernarium.tamk.fi/tietoturva2/PKI.htm>

Cibernarium. 2011b. Digitaalinen allekirjoitus. Hakupäivä 1.4.2011  
[http://www.cibernarium.tamk.fi/tietoturva2/digitaalinen\\_allekirjoitus.htm](http://www.cibernarium.tamk.fi/tietoturva2/digitaalinen_allekirjoitus.htm)

Euroopan Keskuspankki. 2006. Yhtenäinen euromaksualue (SEPA): Yhteiset pienten maksujen markkinat. Hakupäivä 17.2.2011 [http://www.ecb.int/pub/pdf/other/sepa\\_brochure\\_2006fi.pdf](http://www.ecb.int/pub/pdf/other/sepa_brochure_2006fi.pdf)

Finanssialan Keskusliitto. 2009. Yhtenäinen euromaksualue yrityksille. Hakupäivä 19.4.2011  
[http://www.fkl.fi/teemasivut/sepa/vaikutukset\\_yritystoimintaan/Dokumentit/Sepa\\_yrityksille.pdf](http://www.fkl.fi/teemasivut/sepa/vaikutukset_yritystoimintaan/Dokumentit/Sepa_yrityksille.pdf)

Finanssialan Keskusliitto. 2010a. ISO 20022 maksut Opas Sanomat: Pain.001.001.03 Pain.002.001.03 Hakupäivä 19.4.2011 [http://www.fkl.fi/teemasivut/sepa/tekninen\\_dokumentaatio/Dokumentit/ISO20022\\_maksut.pdf](http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/ISO20022_maksut.pdf)

Finanssialan Keskusliitto. 2010b. ISO20022 Tapahtumaraportti-opas v1.2. Hakupäivä 3.4.2011  
[http://www.fkl.fi/teemasivut/sepa/tekninen\\_dokumentaatio/Dokumentit/ISO20022\\_Tapahtumaraportti-opas\\_V1\\_1\\_01032010.pdf](http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/ISO20022_Tapahtumaraportti-opas_V1_1_01032010.pdf)

Finanssialan Keskusliitto. 2010c. ISO20022 Tiliote-opas v1.2. Hakupäivä 3.4.2011  
[http://www.fkl.fi/teemasivut/sepa/tekninen\\_dokumentaatio/Dokumentit/ISO20022\\_Tilioteopas\\_V1\\_1\\_01032010.pdf](http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/ISO20022_Tilioteopas_V1_1_01032010.pdf)

Finanssialan Keskusliitto. 2011. Yhtenäisen euromaksualueen SEPAn toteutuminen Suomessa. Hakupäivä 19.4.2011 [http://www.fkl.fi/teemasivut/sepa/usein\\_kysyttya/Dokumentit/SEPA\\_Kysymyksia\\_ja\\_vastauksia\\_pdf.pdf](http://www.fkl.fi/teemasivut/sepa/usein_kysyttya/Dokumentit/SEPA_Kysymyksia_ja_vastauksia_pdf.pdf)

International Organization for Standardization. 2011. International Organization for Standardization - ISO 20022. Hakupäivä 20.2.2011 [http://www.iso20022.org/UNIFI\\_message\\_archive.page](http://www.iso20022.org/UNIFI_message_archive.page)

Nordea. 2010. Web Services Security and Communication Description. Hakupäivä 29.3.2011  
[http://www.nordea.fi/sitemod/upload/Root/fi\\_org/liite/e/yritys/pdf/web\\_services\\_ohjelmistotalot.pdf](http://www.nordea.fi/sitemod/upload/Root/fi_org/liite/e/yritys/pdf/web_services_ohjelmistotalot.pdf)

Nordea, OP-Pohjola Group, Sampo Bank. 2008. Security and Message Specification for Financial Messages using Web Services. Hakupäivä 19.4.2011 [http://www.fkl.fi/teemasivut/sepa/tekninen\\_dokumentaatio/Dokumentit/WebServices\\_Messages\\_20081022\\_105.pdf](http://www.fkl.fi/teemasivut/sepa/tekninen_dokumentaatio/Dokumentit/WebServices_Messages_20081022_105.pdf)

Petri, D. 2009. More about Public (PKI) Key Infrastructre. Hakupäivä 1.4.2011  
[http://www.petri.co.il/public\\_key\\_infrastructure\\_pki.htm](http://www.petri.co.il/public_key_infrastructure_pki.htm)

SWIFT. 2009. ISO 20022 Customer-to-Bank Message Usage Guide v3.0. Hakupäivä 19.2.2011  
[http://www.swift.com/corporates/resources/Getting\\_Started/MIG\\_ISO20022/ISO20022\\_usage\\_guide\\_V3.pdf](http://www.swift.com/corporates/resources/Getting_Started/MIG_ISO20022/ISO20022_usage_guide_V3.pdf)

W3C. 2011a. Web Services Activity Statement. Hakupäivä 25.4.2011 <http://www.w3.org/2002/ws/Activity>

W3C. 2011b. SOAP Version 1.2 Part1: Messaging Framework (Second Edition). Hakupäivä 25.4.2011 <http://www.w3.org/TR/soap12-part1/>

Wikipedia. 2011. Single Euro Payments Area. Hakupäivä 25.4.2011 [http://en.wikipedia.org/wiki/Single\\_Euro\\_Payments\\_Area](http://en.wikipedia.org/wiki/Single_Euro_Payments_Area)

## C2B-MAKSUAINEISTO

```
<?xml version="1.0" encoding="utf-8"?>
<Document xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns="urn:iso:std:iso:20022:tech:xsd:pain.001.001.02">
  <pain.001.001.02>
    <GrpHdr>
      <MsgId>23982938928398</MsgId>
      <CreDtTm>2011-04-27T20:03:22.6549582+03:00</CreDtTm>
      <BtchBookg>true</BtchBookg>
      <NbOfTxes>1</NbOfTxes>
      <CtrlSum>100</CtrlSum>
      <Grpg>MIXD</Grpg>
      <InitgPty>
        <Nm>Maksaja Oy</Nm>
        <PstlAdr>
          <AdrTp>ADDR</AdrTp>
          <AdrLine>Maksajankatu 1</AdrLine>
          <AdrLine>90100 Saksa</AdrLine>
          <Ctry>FI</Ctry>
        </PstlAdr>
        <Id>
          <OrgId>
            <BkPtyId>123456789</BkPtyId>
          </OrgId>
        </Id>
        <CtryOfRes>FI</CtryOfRes>
      </InitgPty>
    </GrpHdr>
    <PmtInf>
      <PmtInfId>11223321</PmtInfId>
      <PmtMtd>TRF</PmtMtd>
      <PmtTpInf>
        <SvcLvl>
          <Cd>SEPA</Cd>
        </SvcLvl>
      </PmtTpInf>
      <ReqdExctnDt>2011-05-11</ReqdExctnDt>
      <Dbtr>
        <Nm>Maksaja Oy</Nm>
        <PstlAdr>
          <AdrTp>ADDR</AdrTp>
          <AdrLine>Maksajankatu 1</AdrLine>
          <AdrLine>90100 Saksa</AdrLine>
          <Ctry>DE</Ctry>
        </PstlAdr>
        <Id>
          <OrgId>
            <BkPtyId>898989898</BkPtyId>
          </OrgId>
```



```

    </Id>
    <CtryOfRes>DE</CtryOfRes>
  </Dbtr>
  <DbtrAcct>
    <Id>
      <IBAN>DE0252910820037221</IBAN>
    </Id>
  </DbtrAcct>
  <DbtrAgt>
    <FinInstnId>
      <BIC>GERMBANK</BIC>
    </FinInstnId>
  </DbtrAgt>
  <ChrgBr>SLEV</ChrgBr>
  <CdtTrfTxInf>
    <PmtId>
      <InstrId>28765678-9</InstrId>
      <EndToEndId>99889999</EndToEndId>
    </PmtId>
    <Amt>
      <InstdAmt Ccy="EUR">100</InstdAmt>
    </Amt>
    <ChrgBr>SLEV</ChrgBr>
    <CdtrAgt>
      <FinInstnId>
        <BIC>FRANSKA</BIC>
      </FinInstnId>
    </CdtrAgt>
    <Cdtr>
      <Nm>Ostaja Oy</Nm>
      <PstlAdr>
        <AdrTp>ADDR</AdrTp>
        <AdrLine>ostajantie 2</AdrLine>
        <AdrLine>09890 RANSKA</AdrLine>
        <Ctry>FR</Ctry>
      </PstlAdr>
      <CtryOfRes>FR</CtryOfRes>
    </Cdtr>
    <CdtrAcct>
      <Id>
        <IBAN>FR0952987620087665</IBAN>
      </Id>
    </CdtrAcct>
  </CdtTrfTxInf>
</PmtInf>
</pain.001.001.02>
</Document>

```

## SOAP-SANOMA

```

<?xml version="1.0" encoding="utf-8"?>
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:wsa="http://schemas.xmlsoap.org/ws/2004/08/addressing"
xmlns:wss="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
  <soap:Header>
    <wsa:Action/>
    <wsa:MessageID>urn:uuid:3974e4b7-7128-40ab-abf9-
39639e9ce6f7</wsa:MessageID>
    <wsa:ReplyTo>
      <wsa:Address>http://schemas.xmlsoap.org/ws/2004/08/
addressing/role/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:To>https://filetransfer.nordea.com/services/
CorporateFileService</wsa:To>
    <wsse:Security soap:mustUnderstand="1">
      <wsu:Timestamp wsu:Id="Timestamp-8dddab49-a58a-4659-ad67-
4afe02a68d33">
        <wsu:Created>2010-12-01T08:29:06Z</wsu:Created>
        <wsu:Expires>2010-12-01T08:34:06Z</wsu:Expires>
      </wsu:Timestamp>
      <wsse:BinarySecurityToken ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"
EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
soap-message-security-1.0#Base64Binary" xmlns:wsu="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
wsu:Id="SecurityToken-c7e8da6d-f6f2-4a04-99b2-
8f9bde95e92d">MIID+jCCAuKgAwIBAgIEAMdxxTANBgkqhkiG9w0BAQUFADBsmQswCQYD
VQQGEwJTRTEeMBwGA1UE... (poistettu osa tekstistä) ...pyLwFtfw=
</wsse:BinarySecurityToken>
      <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
          <ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"/>
          <SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
          <Reference URI="#Id-26a774bb-b26a-49f7-af51-e1517b5f80b8">
            <Transforms>
              <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#"/>
            </Transforms>
          <DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <DigestValue>N43pNiZ2Phz8gc+GQNEDE8Ru8qyU</DigestValue>
        </Reference>
      </Signature>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
  </soap:Body>
</soap:Envelope>

```

```

    </SignedInfo>
    <SignatureValue>XoosFG0JiLj6AkTTLhAxyz4MWSZ0tHv17pHjpVsTRgbEng3G85h7B0
    OqvRiRzgIK... (poistettu osa tekstistä) .../yBR7q0j4L+gw=
    </SignatureValue>
    <KeyInfo>
      <wsse:SecurityTokenReference>
        <wsse:Reference URI="#SecurityToken-c7e8da6d-f6f2-4a04-
        99b2-8f9bde95e92d" ValueType="http://docs.oasis-
        open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
      </wsse:SecurityTokenReference>
    </KeyInfo>
  </Signature>
</wsse:Security>
</soap:Header>
<soap:Body wsu:Id="Id-26a774bb-b26a-49f7-af51-e1517b5f80b8">
  <getUserInfo xmlns="http://bxd.fi/CorporateFileService">
    <RequestHeader xmlns="http://model.bxd.fi">
      <SenderId>11111111</SenderId>
      <RequestId>2</RequestId>
      <Timestamp>2010-04-04T10:28:48.8169208+02:00</Timestamp>
      <Language>FI</Language>
      <UserAgent>BM Test</UserAgent>
      <ReceiverId>12345678</ReceiverId>
    </RequestHeader>
    <ApplicationRequest
    xmlns="http://model.bxd.fi">PD94bWwgdMvyc2lvbj0iMS4wIiBlbmNvZGluZz0idX
    RmLTgiIHN0YW5... (poistettu osa tekstistä) ...aW9uUmVxdWVzdD4=
  </ApplicationRequest>
  </getUserInfo>
</soap:Body>
</soap:Envelope>

```