OP-POHJOLA-RYHMÄN Yrityksen pankkiyhteys – kanavan eli Web Services –kanavan ja sen tunnistepalvelun sovellusohje

Maksuliikepalvelut

Sovellusohje
Elokuu 2011

1 Johdanto

Tässä ohjeessa kerrotaan sellaisista Web Services (jäljempänä WS) -kanavan käyttöön liittyvistä toimintatavoista ja käytännöistä, joita ei ole kuvattu pankkien yhteisessä sanomamäärityksessä.

Tämä ohje neuvoo myös miten OP Pohjola ryhmän WS-kanavan tarvitsemat varmenteet hankitaan ja miten niitä käytetään. Järjestelmästä käytetään tässä ohjeessa nimitystä WS-kanavan Tunnistepalvelu ja lyhyemmin Tunnistepalvelu.

Ohje kertoo WS-kanavan ja tunnistepalvelun toiminnot sekä sanomakuvaukset. Lisäksi mukana on ohjeita ohjelmiston toteuttajalle sekä esimerkkiaineistoja/sanomia hyödynnettäväksi toteutuksessa.

1.1 Web Services-kanava

Web Services -kanava on tarkoitettu OP-Pohjola-ryhmän yritysasiakkaan ja pankin palveluiden välisten konekielisten aineistojen turvalliseen välittämiseen.

WS-kanavan avulla asiakkaan järjestelmät voivat lähettää pankkiin ja noutaa pankista maksuliikeaineistoja kuten C2B-maksuaineistoja, tiliotteita, e-laskuaineistoja ja niiden ilmoitussanomia.

WS-kanavan sanomamääritykset on tehty useiden pankkiryhmien yhteistyönä ja määritykset ovat vapaasti saatavilla Finanssialan Keskusliiton sivuilta www.fkl.fi hakusanalla "web services".

WS-kanavassa sanoman ja palvelupyynnön muuttumattomuuden ja aitouden varmistaminen perustuu XML Digital Signature –tekniikkaan eli digitaaliseen allekirjoitukseen. Jotta vastaanottaja voi luottaa saamaansa sanomaan ja palvelupyyntöön, tarkistaa hän niiden allekirjoituksen. Allekirjoituksen tarkistamiseen tarvitaan allekirjoittajan julkinen avain, käytännössä varmenne. Tästä on syntynyt tarve Tunnistepalvelulle eli varmenteiden hallinnalle.

1.2 Web Services -kanavan Tunnistepalvelu

WS-kanavan Tunnistepalvelun tehtävä on tuottaa ja hallinnoida varmenteet, joita käytetään WS-kanavan allekirjoitusten tarkistamisessa.

Tunnistepalvelu muodostaa WS-kanavassa tarvittavat varmenteet ja huolehtii niiden sulkutietojen ylläpidosta ja julkaisusta.

Tunnistepalvelun toiminnoista suurin osa tapahtuu WS-kanavan kautta eli loppukäyttäjän näkökulmasta asiakkaan omaa tietojärjestälmää käyttämällä.

Varmenteeseen liittyvien käyttövaltuuksien vuoksi varmenteen elinkaaren alussa on asiakkaan käytävä pankissa tunnistautumassa, jotta varmenteen liittäminen WS-kanavan käyttäjätunnukseen voidaan tehdä turvallisesti. Tätä ensimmäistä tunnistamista ei voi suorittaa sähköisesti.

1.3 Rajaukset

Tämä ohjeistus ei anna asiakkaan ohjelmistoa koskevaa tietoa vaan ainoastaan kuvaa ne toiminnot, jotka asiakkaan käyttämässä ohjelmistossa tulisi olla

käytettävissä. Täsmälliset ja konkreettiset ohjeet tulee käyttäjän etsiä käyttämänsä ohjelmiston ohjeistuksesta.

Tämä pankin julkaisema ohje ei ole sitova eikä virallinen kuvaus osapuolten vastuista avainten ja varmenteiden käytössä. WS-kanavan sopimuksen ehdot sisältävät viralliset kuvaukset vastuista.

1.4 Lähdemateriaali

WS-kanavan yhteiset ohjeet eli sanomakuvaus on julkaistu Finanssialan Keskusliiton sivuilla www.fkl.fi. Kuvaus löytyy hakusanalla "web services".

1.5 Termit

ApplicationRequest	WS-kanavan sanoman sisältämä palvelupyyntö, käytännössä allekirjoitettu XML-asiakirja, joka sisältää tarvittavat tunnistetiedot ja liiketoiminta-aineiston
Avainpari	PKI-järjestelmässä eli julkisen avaimen järjestelmässä käytetyt avaimet; koska kyseessä on asymmetrinen salaus, avaimia on aina kaksi. Katso myös yksityinen avain ja julkinen avain.
CA	Certificate Authority, varmenteen tekijä, sama kuin Varmentaja.
CA-varmenne	Varmentajan varmenne, jonka avulla varmenteen vastaanottaja tarkistaa, että varmenne on aito. CA-varmenteen aitous tarkistetaan Juurivarmenteen avulla.
Certificate Authority	katso CA
Common Name	Varmenteen subjektin kenttä, joka kertoo varmenteen haltija. WS-kanavan Tunnistepalvelussa tässä kentässä on se WS-kanavan käyttäjätunnus, jonka käyttöön varmenne on myönnetty.
Julkinen avain	Avainparin julkinen osa. Tätä avainta jaetaan muille osapuolille. Julkista avainta ei tarvitse salata eikä suojella, se on nimensä mukaisesta julkinen. Useimmiten julkista avainta jaetaan varmenteen muodossa.
Juurivarmenne	Varmenneketjun ylimmäinen varmenne, jonka avulla tarkistetaan varmentajan varmenteen aitous. Juurivarmenne jaetaan käyttäjille aina eri reittiä kuin muut varmenteet, usein se tulee asiakkaan ohjelmiston asennuspaketin mukana.
Palvelupyyntö	WS-kanavan sisältämä XML-asiakirja nimeltään ApplicationRequest, joka sisältää asiakkaan tietojärjestelmän pankilta pyytämän palvelun ohjaustiedot, palvelupyyntöön mahdollisesti liittyvän aineiston sekä aitouden tarkistamiseen vaaditun digitaalisen allekirjoituksen.
pkcs10	Varmennepyynnön standardoitu muoto.

PKI	Public Key Infrastucture. Asymmetrisiin algoritmeihin perustuva salausjärjestelmä. Järjestelmä pitää sisällään myös julkisten avainten jakelun ja hallinnan varmenteiden muodossa.
Rekisteröinti	Rekisteröinti on tapahtuma, jossa uuden, syntyvän varmenteen haltija tunnistetaan. Tällä varmistetaan, että varmenteen haltija on varmasti tiedossa ja varmenteeseen voidaan kytkeä valtuuksia.
Revokointi	Varmenne suljetaan ennenaikaisesti eli revokoidaan. Varmenne ilmestyy sulkulistalle ja muihin sulkutietopalveluihin, jolloin varmenteeseen luottavat järjestelmät osaavat hylätä varmenteen eli käytännössä kieltäytyä siihen perustuvasta aitouden tarkistuksesta. Varmenne suljetaan eli revokoidaan erityisesti silloin, jos on tieto tai epäilys yksityisen avaimen joutumisesta vääriin käsiin.
Salainen avain	katso Yksityinen avain
Salasana	Sama kuin Siirtoavain. Tämä on WS-kanavan Tunnistepalvelun termi.
Siirtoavain	WS-kanavan Tunnistepalvelussa varmennepyynnön aitouden tarkistaminen perustuu siirtoavaimeen, jonka varmennepyynnön lähettävä tietojärjestelmä laittaa pyynnön mukaan. Tämä on WS-kanavan Tunnistepalvelun termi.
SOAP-sanoma	WS-kanavassa lähetetyt palvelupyynnöt ja niiden vastaukset ovat SOAP-sanomat sisällä. SOAP-sanoma on standardin mukainen XML asiakirja, joka sisältää mm. tietoturvaelementtejä.
Subjekti	Varmenteen sisältämä osio, joka kertoo tietoja varmenteen haltijasta. WS-kanavan Tunnistepalvelussa tärkein tieto on CN Common Name eli se WS-kanavan käyttäjätunnus, jonka käyttöön varmenne on myönnetty.
Tunnistepalvelu	OP-Pohjola-ryhmän palvelu, joka tuottaa WS-kanavassa tarvittavat asiakasvarmenteet ja niihin liittyvät tukitoiminnot, kuten sulkemispalvelun.
Varmenne	Varmenne on sähköinen asiakirja (esimerkiksi XML-asiakirja), jonka tärkein tehtävä on kytkeä julkinen avain ja tieto sen hatlijasta toisiinsa. Varmenne sisältää nämä kaksi tietoa ja muita tärkeitä tietoja, ja varmenne on allekirjoitettu Varmentajan toimesta. Varmentajan allekirjoitus vahvistaa nämä tiedot oikeiksi ja samalla varmistaa varmenteen muuttumattomuuden.
Varmennepyyntö	Asiakkaan tietojärjestelmän WS-kanavaan lähettämä sähköinen asiakirja, joka sisältää asiakkaan uuden julkisen avaimen ja asiakkaan tunnisteen. Pankin Tunnistepalvelu muodostaa varmennepyynnön mukaisen varmenteen ja antaa sen asiakkaan tietojärjestelmälle vastaussanomassa.

Varmentaja	katso CA Certificate Authority
Varmenteen sulkeminen	Jos asiakas epäilee tai tietää yksityisen avaimensa joutuneen vääriin käsiin, tulee asiakkaan sulkea varmenne välittömästi. Suljettu varmenne lakkaa toimimasta WS-kanavassa. Suljettua varmennetta ei voi enää ottaa uudestaan käyttöön vaan asiakkaan on rekisteröitävä uusi varmenne ja tehtävä uusi varmennepyyntö.
Web Services –kanava	Web Services ja SOAP standardeihin perustuva pankin palvelu, jota käyttäen pankin yritystasiakkaan tietojärjestelmät lähettävät pankkiin ja noutavat pankista konekielisiä aineistoja.
WS-kanava	katso Web Services –kanava
XML Digital Signature	katso XML-allekirjoitus
XML-allekirjoitus	Tekniikka, jolla varmistetaan XML-asiakirjan aitous ja muuttumattomuus. Allekirjoitus tehdään yksityisellä avaimella ja tarkistetaan julkisella avaimelle.
X.509v3	Standardoitu varmenteen tekninen esitysmuoto.
Yksityinen avain	Avainparin salainen osa, joka on vain haltijansa käytössä. Tätä avainta on varjeltava paljastumiselta ja kopioinnilta todella huolellisesti. Käytetään myös nimitystä Salainen avain.

2 Yleiset tietoturvakäytännöt

Tunnistepalvelussa kaikkein kriittisimmät tietoturvakohteet ovat seuraavat:

1. Yksityisen avaimen säilyttäminen ja käyttö on toteutettava siten, että avainta ei saa haltuunsa eikä pääse käyttämään kukaan, jolla ei ole siihen oikeutta. Yksityisen avaimen avulla asiakkaan ohjelmisto tekee allekirjoituksen, jonka perusteella pankki luottaa aineiston aitouteen ja varmistaa aineiston tekijän.

2. Varmenteen rekisteröinti, siirtoavaimen toimitus ja varmennepyynnön tunnistus tapahtuvat turvallisesti ja luotettavasti. Tällä varmistetaan, että varmenne syntyy todella siitä julkisesta avaimesta, jonka pankissa rekisteröinnin yhteydessä tunnistama asiakas on luonut.

3. Varmenteiden sulkupalvelu toimii ja sen antamat tiedot ovat aina ajan tasalla. Tämä koskee erityisesti pankkia, joka käyttää varmenteita asiakkailta tulevien liiketoiminta-aineistojen tarkistamiseen ja siten niiden käsittelyn sallimiseen. Jos asiakas on sulkenut eli revokoinut varmenteen, pankki ei saa hyväksyä allekirjoitusta joka on tehty kyseistä varmennetta vastaavalla salaisella avaimella.

Tunnistepalvelussa on muitakin tietoturvan kannalta kriittisiä ja oleellisia toimintoja, mutta nämä edellämainitut kolme ovat niistä tärkeimmät.

2.1 Avainparin laatu

Asiakkaan vastuulla on WS-kanavassa käyttämänsä avainparin luominen. Avainparin voi muodostaa siihen tarkoitetulla ohjelmistolla, sen voi muodostaa asiakkaan tietojärjestelmä. Asiakkaan ohjelmisto voi käyttää avainparin luomiseen ja säilyttämiseen tietoturvamodulia.

Pankki ei osallistu avainparin luomiseen eikä koskaan näe eikä käsittele asiakkaan yksityistä avainta.

Asiakkaan vastuulla on huolehtia, että sen avainpari on riittävän laadukas. Ensisijaisesti tämä tarkoittaa, että avaimen luomiseen käytetty satunnaisluku on tarpeeksi satunnainen eikä siten ole toistettavissa. Avainparin muodostavan ohjelman toteuttajan tulee huolehtia, että muodostukseen käytetty algoritmi on riittävän laadukas ja hyvien kryptografisten käytäntöjen mukainen.

2.2 Yksityisen avaimen säilyttäminen ja käyttö

Asiakkaan vastuulla on yksityisen eli salaisen avaimen turvallinen säilytys ja sen käytön hallinta.

Yksityistä avainta ei tule säilyttää salaamattomana eikä sen käyttöä tule sallia ilman riittävää tunnistamista.

Yksityisen avaimen avulla asiakkaan ohjelmisto tekee WS-kanavassa tarvittavan XML-allekirjoituksen, jonka perusteella pankki luottaa sanomaan ja sen sisältämään palvelupyyntöön ja samalla lähetettyyn aineistoon. Se, jonka hallussa yksityinen avain on, pystyy käytännössä lähettämään pankkiin WS-kanavan kautta palvelupyyntöjä ja aineistoja, jotka pankki toteuttaa yksityiseen avaimeen varmenteen avulla liitetyn asiakkaan nimissä.

Asiakas vastaa yksityisellä avaimellaan tehdyistä toimeksiannoista täysimääräisesti.

2.3 Varmennepyynnön tunnistaminen pankin Tunnistepalvelussa

Asiakkaan tietojärjestelmä tekee varmennepyynnön pankin Tunnistepalveluun WS-kanavan kautta.

Varmennepyynnön tyypistä riippuen pankin palvelu suorittaa varmennepyynnön tunnistamisen ja aitouden varmistamisen seuraavilla eri tavoilla. Kaikissa tunnistamistavoissa suojaus ulkopuolisilta perustuu sanoman lähetyksen SSL-suojaukseen.

Kun kyseessä on käyttäjätunnuksen ensimmäinen varmenne, tulee elementissä CertApplicationRequest.TransferKey antaa pankista saatu 16 numeroa pitkä siirtoavain, sekä elementissä CertApplicationRequest.CustomerId 10 numeroa pitkä käyttäjätunnus. Siirtoavaimen viimeinen numero on tarkiste, jonka avulla asiakkaan ohjelmisto voi paikallisesti varmistua siitä, että siirtoavain on syötetty oikein. Tarkiste on laskettu Luhnin modulo 10 algoritmilla.

Kun kyseessä on voimassaolevan varmenteen uusiminen, tulee CertApplicationRequest allekirjoittaa sillä avaimella, jonka varmenne on jo käytössä, sekä elementissä CertApplicationRequest.CustomerId 10 numeroa pitkä käyttäjätunnus.

Jos asiakkaan tietojärjestelmä tekee varmennepyynnön samasta avainparista kuin jo ennestään käytössä oleva varmenne, pankin Tunnistepalvelu ei muodosta uutta varmennetta vaan palauttaa kopion jo käytössä olevasta varmenteesta.

2.4 Varmenteen sulkeminen ja sulkutietojen hyödyntäminen

Asiakas voi sulkea eli revokoida varmenteensa soittamalla puhelinnumeroon 010 2528470.

Varmenteen sulkemiseen tarvitaan 10 numeroa pitkä WS-kanavan käyttäjätunnus tai varmenteen sarjanumero.

Kun varmenne on suljettu, se ei kelpaa WS-kanavassa eikä kyseistä varmennetta voi enää ottaa uudestaan käyttöön. Sulkemisen jälkeen on asiakkaan rekisteröitävä uusi varmenne ja tehtävä WS-kanavan kautta varmennepyyntö siirtoavaimen kanssa.

Pankki julkaisee asiakkaille varmenteiden sulkulistan osoitteessa http://wsk.op.fi/crl/ws/OP-Pohjola-ws.crl. Sulkulista päivittyy kerran vuorokaudessa ja on voimassa kaksi vuorokautta. Asiakkaan tietojärjestelmän velvollisuus on noutaa sulkulista siten, että se on aina ajan tasalla ja tarkistaa vastaussanoman digitaalisen allekirjoittajan varmenteen sulkutilanne sulkulistalta.

Pankki ei anna lupaa käyttää WS-kanavan varmenteita muihin tarkoituksiin kuin WS-kanavaan, joten pankki ei ota myöskään vastuuta asiakasvarmenteiden sulkutietojen julkaisun toiminnasta ja ajantasaisuudesta muuhun kun pankin sisäiseen käyttöön. Pankilla on itsellään ajantasainen tieto asiakasvarmenteiden sulkutilanteesta, mutta pankin ulkopuolelle ei tätä palvelua ole tarjolla.

3 Web Services -kanava

Web Services (jäljempänä WS) -kanava on tarkoitettu yritysasiakkaan tietojärjestelmän ja pankin palveluiden välisten konekielisten aineistojen turvalliseen välittämiseen.

WS-kanavan toiminta perustuu Suomessa toimivien pankkien yhdessä tekemään sanoma- ja tietoturvamääritykseen.

WS-kanavassa yhteystapa on ensisijaisesti SSL-suojattu https yleisen Internet-verkon yli. Kanavassa lähetettävä yksikkö on SOAP-sanoma, joka on digitaalisesti allekirjoitettu. Sanoma sisältää XML-asiakirjan ApplicationRequestin, joka on varsinainen palvelupyyntö. ApplicationRequest eli palvelupyyntö on myös digitaalisesti allekirjoitettu. ApplicationRequest sisältää palveluun liittyvän liiketoiminta-aineiston, esimerkiksi maksuaineiston.

WS-kanava on tarkoitettu eräaineistojen lähettämiseen ja noutamiseen. Asiakkaan tietojärjestelmä lähettää palvelupyynnön ja saa WS-kanavasta heti vastauksen. Lähetetty aineisto jää pankkiin odottamaan käsittelyä. Käsittelystä saattaa syntyä palauteaineisto, joka asiakkaan tietojärjestelmän tulee noutaa erikseen.

Tuotannon WSDL-tiedosto on noudettavissa osoitteesta

https://wsk.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristön WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristössä on käytössä Tuotannon käyttäjätunnus, mutta avainpari ja varmenne ovat vain testikäyttöön tarkoitetut, turvallisuussyistä.

3.1 Web Services -kanavan toiminnot

3.1.1 Aineiston lähettäminen pankkiin

WS-kanavan kautta pankin asiakkaan tai asiakkaan aineistonhoitajan ohjelmisto lähettää aineistoja pankkiin.

WS-kanava tarkistaa aineiston muodon oikeellisuuden heti lähetyksen yhteydessä ja hylkää aineiston, jos se ei ole muodollisesti ehjä. WS-kanava ei tallenna hylättyä aineistoa ollenkaan. WS-kanava antaa lähettävälle ohjelmistolle välittömästi virhevastauksen, jossa on virhekoodi 12 ja selite Schema validation failed.

Aineistoja voi lähettää vain yhden kerrallaan eli yhden aineiston per sanoma.

Suosittelemme lähetettävän aineiston pakkaamista riippumatta aineiston koosta. (Katso kohta aineiston pakkaaminen).

3.1.2 Aineiston hakeminen pankista

Asiakkaan ohjelmisto voi noutaa WS-kanavasta aineistoja, sekä asiakkaan itse kanavaan lähettämiä että pankin muodostamia noudettavia aineistoja.

Aineistoa noudettaessa tulee määritellä täsmälleen minkä aineiston haluaa noutaa, tämä tapahtuu aineiston tunnisteella (FileReference). Aineistojen tunnisteet saa tietoonsa tehtyään aineistojen listauksen. Sen jälkeen voi listalla olevia aineistoja

noutaa aineistotunnisteen perusteella. Lisäksi WS-kanavaan lähettämänsä aineiston tunnisteen saa aina aineiston lähetyksen vastaussanomassa.

Aineistoja voi hakea vain yhden kerrallaan.

WS-kanava säilyttää aineistoja kolme kuukautta ja poistaa ne sen jälkeen automaattisesti. Asiakkaan ei tarvitse itse poistaa aineistoja.

Vaikka asiakas olisi jo noutanut aineiston, voi sen noutaa yhä uudelleen. Noudetun aineiston tila muuttuu tilasta NEW tilaan DLD, mutta itse aineisto säilyy edelleen näkyvissä ja noudettavissa.

3.1.3 Aineiston pakkaaminen

Suosittelemme aina pakkaamaan pankkiin lähetettävän aineiston. Pakkausalgoritmi on RFC1952:n mukainen GZIP. Pakkaus suoritetaan alkuperäiselle aineistolle ennen base64-enkoodausta ja elementtiin ApplicationRequest.Content kirjoittamista. Elementin ApplicationRequest.Compression tulee olla 'true' kun aineisto on pakattu.

Aineistoja noudettaessa suosittelemme myös pyytämään pakkausta. Asettamalla noutopyynnössä ApplicationRequest.Compression = 'true' saa aineiston pankista pakattuna.

3.1.4 Ajantasapalvelut

WS-kanavassa on tarjolla tällä hetkellä alla luetellut ajantasapalvelut ja uusia lisätään vuoden 2011 mittaan. Uudet ajantasapalvelut päivitetään tähän asiakasohjeeseen kun tulevat käyttöön.

Ajantasapalvelut toimivat uploadFile –operaatiolla. WS-kanavaan ladataan pyyntö ApplicationRequest.Content –elementissä, ja ApplicationRequest.FileType on ajantasapalvelun nimi, esim. "TP1 1SS".

Nyt WS-kanavassa käytössä olevat ajantasapalvelut on toteutettu Eräsiirtopalvelun eli ns. PATU-kanavan mukaisilla palvelupyynnöillä ja –vastauksilla. Rinnalle avataan tulevaisuudessa XML-muotoiset SEPA-aikakauden vastaavat palvelut – ne eroavat siten että pyyntö- ja vastaussanomat ovat ISO20022 –standardin mukaisia tai niistä sovellettuja xml-asiakirjoja.

3.1.4.1 Saldokysely

Pankkiyhteysohjelma voi kysyä tilin saldoa.

Palvelun tekninen nimi ja samalla FileType on TP1 1SS.

Pankkiyhteysohjelma laittaa palvelyynnön elementtiin ApplicationRequest.Content base64-enkoodattuna seuraavan muotoisen pyynnön:

$$TP1 1SS konttorinumero tilinumero X

missä:

- konttorinumero 6 merkin mittaisena
- tilinumero 8 merkin mittaisena
- X on merkki X.

Saldokyselyn vastaus on elementissä ApplicationResponse.Content ja on rakenteeltaan seuraava.

Tiedon nimi	Pituus	Selitys
Tietueen järjestysnumero	1	=1
Vastaustyyppi	1	1=OK, muu=virhe*
Varalla	3	
Tapahtumakonttorin numero	6	
Päätenumero	2	
Tapahtumanumero	4	
Tilinomistajan nimi	15	
Konttorinumero	6	
Tilinumero	8	
Päivämäärä	6	ppkkvv
Saldo	11	2 des.
Saldon etumerkki	1	+/-
Luottoraja	11	2 des.
Luottorajan etumerkki	1	+/-
Nostovara	11	2 des.
Nostovaran etumerkki	1	+/-
Rahayksikön koodi	1	1=euro

3.1.4.2 Tapahtumaotekysely

Pankkiyhteysohjelma voi kysyä tilin kuluvan päivän noutamattomia tiliotetapahtumia.

Palvelun tekninen nimi ja samalla FileType on TP1 3ST.

Pankkiyhteysohjelma laittaa palvelyynnön elementtiin ApplicationRequest.Content base64-enkoodattuna seuraavan muotoisen pyynnön:

$$TP1 3ST konttorinumero tilinumero X

missä:

- konttorinumero 6 merkin mittaisena
- tilinumero 8 merkin mittaisena
- X on merkki 1 mikäli halutaan kaikki tapahtumat uudelleen päivän alusta, muussa tapauksessa palauttaa vain uudet, tällä WS-kanavan käyttäjätunnuksella (CustomerId) vielä noutamattomat tilitapahtumat.

Vastaussanoman tietuekuvaukset

Tietueet erotetaan toisistaan tietue-erottimilla. Jokainen tietue päättyy carriage return- ja line feed -merkkeihin.

Tapahtumaotteen perustietue

Kenttä	Tiedon nimi	Muoto	Kuvaus
1	Aineistotunnus	AN1	S
2	Tietuetunnus	AN2	00
3	Tietueen pituus	N3	322
4	Versionumero	AN3	001
5	Tilinumero	AN14	
6	Tapahtumaotteen no	AN3	Tyhjää
7	Kyselypäivä		
	.1 Alkupäivä	N6	VVKKPP
	.2 Loppupäivä	N6	VVKKPP
8	Muodostamisaika		
	.1 Kuluva päivä	N6	VVKKPP
	.2 Kelloaika	N4	HHMM
9	Asiakastunnus	AN17	

10	Ei käytössä	N6	
11	Ei käytössä	AN19	
12	Ei käytössä	N6	
13	Tilin valuutan tunnus	AN3	ISO-koodi
14	Tilin nimi	AN30	
15	Tilin limiitti	AN18	16 kok + 2 desim
16	Tilinomistajan nimi	AN35	
17	Pankin nimi	AN40	
18	Ei käytössä	AN40	
19	Ei käytössä	AN30	
20	Ei käytössä	AN30	
	YHTEENSÄ	322	

Kenttä 4 ilmoittaa tapahtumaotteen muodostuksessa käytetyn ohjelman version.

Kenttä 7 Alkupäivä ja loppupäivä on sama eli kyselypäivä.

Kenttä 9 ilmoittaa tilinomistajasta pankissa käytettävän asiakastunnuksen ja sen mahdollisen tarkenteen

(alkuvaiheessa maatunnus tai vakio sekä tarkenne ovat tyhjiä).

- maatunnus X(4) tai .1 vakio X(4)
- asiakastunnus X(8) .2 asikastunnus X(10)
- asiakastarkenne X(5) .3 asiakastarkenne X(3)

Kentässä 15 on tilin limiitti luotollisella shekkitilillä. Tilillä ei ole limiittiä, mikäli kentän sisältö on nollia. Konsernitilipalvelun yksikkötilillä kentässä välitetään tilin sisäinen limiitti.

Tapahtuman perustietue

Kenttä	Tiedon nimi	Muoto	Kuvaus
1	Aineistotunnus	AN1	S
2	Tietuetunnus	AN2	10
3	Tietueen pituus	N3	188
4	Kellonaika, tap. syntyaika	N6	HHMMSS
5	Alkup. arkistointitunnus	AN18	
6	Kirjauspäivä	N6	VVKKPP
7	Arvopäivä	N6	VVKKPP
8	Maksupäivä	N6	VVKKPP
9	Tapahtumatunnus	AN1	1, 2, 3, 4
10	Kirjausselite .1;Koodi .2;Seliteteksti	 AN3 AN35	
11	Tapahtuman rahamäärä .1;Etumerkki .2;Määrä	 AN1 N18	 16 kok + 2 desim
12	Kuittikoodi	AN1	E = erittelyt eivät tule tapahtuma-otteeseen
13	Välitystapa	AN1	
14	Saaja/Maksaja .1 Nimi .2 Nimen lähde	 AN35 AN1	 tyhjäm., A,J tai K
15	Saajan tili .1 Tilinumero .2 Tili muuttunut -tieto	 AN14 AN1	 tyhjämerkki, *

16	Viite	AN20	
17	Lomakkeen numero	AN8	
18	Tasotunnus	AN1	0
	YHTEENSÄ	188	

Kentässä 5 on tapahtuman muodostaneen pankin antama arkistointitunnus, jonka avulla pystytään jäljittämään alkuperäinen maksutoimeksianto. Arkistointitunnus kertoo, minä päivänä pankki on käsitellyt maksutoimeksiannon sekä minkä pankin konttori tai järjestelmä on käsitellyt tapahtuman.

VVKKPP XXXXXXXXXXX

^_____yksilöintitieto

^_____ päivämäärä

Arkistointitunnuksen yksilöintitieto on pankkikohtainen. Sen ensimmäiset merkit kertovat pankkiryhmän tunnuksen.

Kentässä 9 on tapahtumatunnus, jonka arvot ovat:

1	=	pano
2	=	otto
3	=	panon korjaus
4	=	oton korjaus

Huom. Korjauksen korjaukset tulevat tapahtumatyypillä 1 (pano) tai 2 (otto).

Kentässä 10 annettava kirjausselite ilmoittaa, minkä palvelun kautta tai miten tapahtuma on tilipankissa kirjattu. Kirjausselitteen koodin ensisijaisena tarkoituksena on mahdollistaa asiakkaiden automaattinen tilitapahtumien tiliöinti omassa kirjanpidossaan. Automaattisesti tiliöitäville tapahtumille on nimetty yksilöivät koodit, muille tapahtumille annetaan yleiskoodit. Koodien arvot ovat kaikilla pankeilla samat. Selitetekstit ovat pankkikohtaisia.

Kirjausselitteen koodin arvot ovat:

700	=	maksuliikepalvelu pano/otto
701	=	toistuvaissuorituspalvelu pano/otto
702	=	laskujen maksupalvelu otto
703	=	maksupäätepalvelu pano
704	=	suoraveloituspalvelu/automaattinen maksupalvelu pano/otto
705	=	viitesuorituspalvelu pano
706	=	maksupalvelu otto
710	=	pano pano
720	=	otto otto
721	=	korttimaksu otto
722	=	shekki otto
723	=	taksibussiseteli otto
730	=	palkkio otto
740	=	korkoveloitus otto
750	=	korkohyvitys pano
760	=	laina (sisältäen lyhenyksen, koron ja palkkion) otto
761	=	lainan lyhennys otto

Korjauksissa koodeja käytetään sekä pano- että ottotapahtumalla.

Kentässä 12 on kuittikoodi, joka ilmoittaa, ovatko tositetiedot tiliotteella vai liittyykö tapahtumaan erillinen paperikuitti tai konekielisenä annettava erittely yksittäisistä tapahtumista.

Kuittikoodin arvot ovat:

tyhjämerkki	=	Pankki ei toimita asiakkaalle tapahtumasta paperikuittia.
E	=	Tapahtumaan liittyy erittely.
P	=	Pankki toimittaa asiakkaalle tapahtumasta paperikuitin.

Kentässä 13 on maksutoimeksiannon vastanottaneen pankin antama välitystapakoodi, joka kertoo miten maksutoimeksianto on välitetty pankkiin ja missä on alkuperäinen maksutoimeksianto.

Selvittelytilanteissa välitystavan avulla päätellään, mihin otetaan yhteyttä, jos tapahtumasta tarvitaan lisää tietoa. Välitystavan arvon ollessa A selvittelypyyntö osoitetaan aina suoraan toimeksiantajalle. Muissa tilanteissa otetaan yhteyttä tilikonttoriin.

Välitystapakoodin arvot ovat:

A	=	Asiakas on lähettänyt maksun konekielisenä tai maksanut sen itsepalveluna. Alkuperäinen maksutoimeksianto on asiakkaalla.
J	=	Tapahtuma on muodostettu pankin järjestelmässä. Perusteet sen syntyyn ovat selvitettävissä arkistointitunnuksen osoittaman järjestelmän selvittelypisteestä.
K	=	Tapahtuma on tehty pankin konttorissa toimihenkilön tallentamana. Maksutoimeksianto löytyy arkistointitunnuksen perusteella.

Kentässä 14 välitetään yksittäisellä tapahtumalla toisen osapuolen nimi aina, kun se on saatavissa. Tietoa ei ole koontitapahtumalla.

Nimi on joko saajan nimi yksittäisellä maksajan tapahtumalla tai maksajan nimi saajan yksittäisellä tapahtumalla. Nimen lähde on vain sellaisella tapahtumalla, jolla on Saaja/Maksaja-tieto ja se ilmoittaa välitetyn saajan tai maksajan nimen alkuperän.

Nimen lähde -tiedon arvot ovat:

A	=	Nimitieto on saatu asiakkaan konekielisestä aineistosta tai se on asiakkaan itsepalveluna tallentama.
J	=	Nimitieto on saatu pankin rekisteristä tilinumeron perusteella.
K	=	Nimitiedon on tallentanut toimihenkilö pankin konttorissa.

Kentässä 15 on maksajan tapahtumalla se saajan tilinumero, jonka maksajan pankki on tapahtumaa välittäessään sille antanut. Tiedon avulla maksaja voi tarkistaa, mille tilille maksu on osoitettu. Tili muuttunut -tieto liittyy vain saajan tilinumeroon ja se ilmoittaa maksajan alunperin antaneen tilin muuttuneen pankin järjestelmissä.

Tili muuttunut -tiedon arvot ovat:

tyhjämerkki	=	ei muutettu
*	=	muutettu

Tapahtuman lisätietue

Kenttä	Tiedon nimi	Muoto	Kuvaus
1	Aineistotunnus	AN1	S
2	Tietuetunnus	AN2	11
3	Tietueen pituus	N3	
4	Lisätiedon tyyppi	AN2	
5	Lisätieto	ANnnn	
	YHTEENSÄ	8+nnn	

Tapahtuman lisätietue muodostuu kaikille lisätietueille yhteisestä alkuosasta ja lisätiedosta, jonka pituus vaihtelee lisätiedon tyypin mukaisesti.

Vapaa viesti, tyyppi = 00			
5.1	Viesti - 1	AN35	
5.2	Viesti - 2	AN35	
...	.....		
5.12	Viesti - 12	AN35	
	YHTEENSÄ	Max 420	

Kpl-määrä, tyyppi = 01			
5.1	Tapahtumien kpl-määrä	N8	
	YHTEENSÄ	8	

Laskutapahtuman tiedot, tyyppi = 02			
5.1	Asiakasnumero	AN10	
5.2	Tyhjä	AN1	
5.3	Laskun numero	AN15	
5.4	Tyhjä	AN1	
5.5	Laskun päiväys	AN6	VVKKPP
	YHTEENSÄ	33	

Korttitapahtuman tiedot, lisätiedon tyyppi = 03			
5.1	Kortin numero	AN19	
5.2	Tyhjä	AN1	
5.4	Kaupan arkistoviite	AN14	
	YHTEENSÄ	34	

Korjaustapahtuman tiedot, tyyppi = 04			
5.1	Korjattavan tapahtuman alkuperäinen arkistointitunnus	AN18	
	YHTEENSÄ	18	

Valuuttatapahtuman tiedot, lisätiedon tyyppi = 05			
5.1	Vasta-arvo		
	.1 Etumerkki	AN1	
	.2 Määrä	N18	16 kok + 2 desim
5.2	Tyhjä	AN1	
5.3	Valuutan ISO-koodi	AN3	
5.4	Tyhjä	AN1	
5.5	Valuuttakurssi	N11	4 kok + 7 desim
5.6	Kurssiviite	AN6	
	YHTEENSÄ	41	

Toimeksiantajan tiedot, tyyppi = 06			
5.1	Toimeksiantajan tieto-1	AN35	
5.2	Toimeksiantajan tieto-2	AN35	
	YHTEENSÄ	70	

Pankin lisätiedot, tyyppi = 07			
5.1	Lisätieto-1	AN35	
5.2	Lisätieto-2	AN35	
...	.....		
5.12	Lisätieto-12	AN35	
	YHTEENSÄ	Max 420	

Maksunaiheen tiedot, tyyppi = 08			
5.1	Maksunaihekoodi	N3	
5.2	Tyhjä	AN1	
5.3	Maksunaiheen selite	AN31	
	YHTEENSÄ	35	

Nimitarkenteen tiedot, tyyppi = 09			
5.1	Saajan/maksajan nimen tarkenne	AN35	
	YHTEENSÄ	35	

Saldotietue

Kenttä	Tiedon nimi	Muoto	Kuvaus
1	Aineistotunnus	AN1	S
2	Tietuetunnus	AN2	40
3	Tietueen pituus	N3	50
4	Kyselypäivä	N6	VVKKPP
5	Kyselyhetken saldo .1 Etumerkki .2 Määrä	 AN1 N18	 16 kok + 2 desim
6	Käytettävissä oleva saldo .1 Etumerkki .2 Määrä	 AN1 N18	 16 kok + 2 desim
	YHTEENSÄ	50	

Tiedotetietue

Tämä tietue välitetään asiakkaalle vain, jos kysely ei onnistu tai häiriöiden takia tiedot eivät ole ajantasalla.

Kenttä	Tiedon nimi	Muoto	Kuvaus
1	Aineistotunnus	AN1	S
2	Tietuetunnus	AN2	70
3	Tietueen pituus	N3	
4	Pankkiyhtymän tunnus	AN3	
5	Tiedote .1 Rivi - 1 (esim häiriön syy) … .6 Rivi - 6	 AN80 AN80	
	YHTEENSÄ	Max 489	

3.1.4.3 Pikamaksu

Ajantasainen maksu toiseen rahalaitokseen.

Palvelun tekninen nimi eli aineistotyyppi on TP4 PS01.

Pankkiyhteysohjelma laittaa palvelyynnön elementtiin ApplicationRequest.Content base64-enkoodattuna seuraavan muotoisen pyynnön:

Tiedon nimi	Pituus	Selitys
Ohjauskomento	11	”$$TP4 PS01 ”
Maksajan konttori	6	5nnnnn
Maksajan tilinumero	8	
Maksajan nimi	30	
Saajan konttori	6	
Saajan tilinumero	8	
Saajan nimi	30	
Siirrettävä rahamäärä	14	Penneinä tai sentteinä, ks. alla
Rahayksikkökoodi	1	1 euro
Eräpäivä	10	pp.kk.vvvv, toistaiseksi tyhjä
Viite	20	Etunollatäyttö
Viesti	140	
Paperikuitti maksajalle	1	”E”, ei kuitteja toistaiseksi
Ilmoitus saajalle	1	0 ei ilmoitusta 1 puhelin

		2 fax 9 muu
Saajan yhteystiedot	70	Saajan yhteystiedot, kun ilmoitetaan saajalle, muuten tyhjä
Aikaleima	15	Vvkkppttmmssnnn, yksilöllinen
Sanomaversio	1	”1”
Käyttöavaimen sukupolvi	1	0 .. 9
Tarkiste	16	ei käytössä, laitettava nollia

Esimerkki pikamaksun pyynnöstä. Välilyönnit on tässä korvattu pisteellä, jotta niiden määrä ja sijainti näkyisi – oikeassa pyyntösanomassa pitää olla välilyönnit.

```
$$TP4.PS01.57803820021333Saku.Eeroila.................13934600001181Simo.Sammila..
...............00000000000001127.11.201100000000000000001245.....................
.....................................................................................
.....................................E0.............................................
.......................1107271457000001000000000000000000
```

Vastaanotettava pikamaksukuittaus

Pikamaksukuittaus on tiedosto, jossa on kaksi tietuetta; kuittaustietue ja osuuspankin eräsiirtopalvelun tapahtuman päättymistietue ($$EOF). Pikamaksukuittaus saattaa olla myös pelkkä osuuspankin eräsiirto-palvelun $$ERROR-virhevastaus esim. PERMISSION ERROR tai NO RESPONSE FROM HOST. Pankkiyhteysohjelman on varauduttava pikamaksussa normaalia pitempään vasteaikaan; noin 120 sekuntia (tapahtuma voidaan käsitellä muussa rahalaitoksessa). Jos kuittausta ei saada osuuspankin eräsiirtopalvelusta tai se on $$ERROR - NO RESPONSE FROM HOST-virhevastaus, pitää pankkiyhteysohjelman pyytää käyttäjää ottamaan yhteyttä pankkiinsa tai tarkistamaan esim. tapahtumakyselyn avulla onnistuiko pikamaksu. Jos tilillä on pikamaksua vastaava tapahtuma, pikamaksu on onnistunut.

Kuittaustietueelle on laskettu MAC-tarkiste PATU-standardin mukaan ks. PATU-järjestelmäkuvaus, Suomen Pankkiyhdistys. Tarkiste lasketaan käyttöavaimella kuittaustietueen alusta tarkistekenttään asti kuten muissakin PATU-sanomissa (ESI, SUO, VAR ja PTE).

Tiedon nimi	**Pituus**	**Selitys**
Onnistumiskoodi	2	”00” Onnistui muut numeroarvot ovat virheitä, jolloin seliteteksti kertoo syyn esim. ”HYLÄTTY, KATE EI RIITÄ.”
Seliteteksti	80	Seliteteksti, asiakkaan kielellä
Arkistointitunnus	22	Jos onnistui, muuten tyhjä
Aikaleima	15	Vvkkppttmmssnnn
Sanomaversio	1	”1”
Käyttöavaimen sukupolvi	1	0 .. 9
Tarkiste	16	Ei käytössä, nollia

3.1.4.4 Ajantasamaksu – tilisiirto omien tilien välillä

Pankkiyhteysohjelma voi tehdä tilisiirron omien tilien välillä.

Palvelun tekninen nimi ja samalla FileType on TP1 ES.

Pankkiyhteysohjelma laittaa palvelyynnön elementtiin ApplicationRequest.Content base64-enkoodattuna seuraavan muotoisen pyynnön:

$$TP1 ES X vknro vtnro hknro htnro euromäärä viesti

missä

- X on merkki X
- vknro veloitettava konttorinumero 6 merkin mittaisena
- vtnro veloitettava tilinumero 8 merkin mittaisena
- hknro hyvitettävä konttorinumero 6 merkin mittaisena
- htnro hyvitettävä tilinumero 8 merkin mittaisena
- euromäärä siirrettävä rahamäärä sentteinä ilman desimaalipistettä max 11 merkkiä
- viesti max 70 merkkiä pitkä lainausmerkkien välissä

Esimerkki jossa siirretään 1500 euroa tililtä 500015-118 tilille 500015-22228 viestillä Mallitilisiirto

$$TP1 ES X 500015 10000018 500015 20002228 150000 "Mallitilisiirto"

Tilisiirron vastaussanoma

Tiedon nimi	Pituus	Selitys
Tietueen järjestysnumero	1	1
Vastaustyyppi	1	1=OK, muu=virhe*
Varalla	3	
Tapahtumakonttori	6	
Päätenumero	2	
Tapahtumanumero	4	
Tilinomistajan nimi	15	
Päivämäärä	6	ppkkvv
Veloitettu konttorinumero	6	
Veloitettu tilinumero	8	
Veloitetun tilin saldo	11	sentteineen ilman desimaalipistettä
Saldon etumerkki	1	+/-
Hyvitetty konttorinumero	6	
Hyvitetty tilinumero	8	
Varalla	12	
Siirretty euromäärä	11	sentteineen ilman desimaalipistettä
Etumerkki	1	+
Rahayksikön koodi	1	1=euro

3.1.4.5 Konsernitilikysely

Pankkiyhteysohjelma voi kysyä konsernitilin saldon, otot sekä panot.

Palvelun tekninen nimi ja samalla FileType on TP1 2KS.

Pankkiyhteysohjelma laittaa palvelyynnön elementtiin ApplicationRequest.Content base64-enkoodattuna seuraavan muotoisen pyynnön:

$$TP1 2KS konttorinumero tilinumero X

missä

- konttorinumero 6 merkin mittaisena
- tilinumero 8 merkin mittaisena
- X on merkki X.

Konsernitilikyselyn vastausosa

Tiedon nimi	Pituus	Selitys
Tietueen järjestysnumero	1	1
Vastaustyyppi	1	1=OK, muu=virhe*
Varalla	3	
Tapahtumakonttori	6	
Päätenumero	2	
Tapahtumanumero	4	
Tiliomistajan nimi	15	
Konsernikonttorinumero	6	
Konsernitilinumero	8	
Päiväys	6	ppkkvv
Saldo	13	2 des.
Etumerkki	1	+/-
Päivän otot	13	2 des.
Etumerkki	1	+/-
Päivän panot	13	2 des.
Etumerkki	1	+/-
Rahayksikön koodi	1	1=euro

3.1.4.6 Uusintatiliotteen tilaus

Pankkiyhteysohjelma voi tilata tilioteuusinnan Osuuspankin WS-kanavasta.

Palvelun tekninen nimi ja samalla FileType on ORDER TU.

Tilaus on muotoa:

$$ORDER TU alkupäivä loppupäivä konttorinumero tilinumero

missä

- alkupäivä on tiliotejakson alkupäivä muodossa vvvvkkpp
- loppupäivä on tiliotejakson loppupäivä muodossa vvvvkkpp

- konttorinumero 6 merkin mittaisena
- tilinumero 8 merkin mittaisena

Jos tilaus onnistui, vastauskoodi on 00 OK. Uusintatiliote muodostuu tiliotteiden muodosaikataulussa seuraavaksi aamuksi.

3.1.5 Aineistojen listaus

Asiakkaan järjestelmä voi noutaa WS-kanavasta listauksen aineistoista. Listauksen haussa voi käyttää seuraavia hakukriteerejä:

- Aineiston tallennushetki kanavassa rajattuna tietylle aikavälille, päivämäärän tarkkuudella.

- Aineiston tilatieto

    - asiakkaan lähettämissä aineistoissa

- WFP – odottaa käsittelyä (Waiting for Processing)
- FWD – laitettu jatkokäsittelyyn (Forwarded)

o asiakkaan noudettavissa olevissa aineistoissa

- DLD – noudettu (Downloaded)
- NEW – noutamaton (New)

- Aineiston tyyppi, esimerkiksi pain.001.001.02, pain.002.001.02.

Asiakkaan deleteFile-operaatiolla itse poistamat aineistot eivät näy listauksessa (katso kohta Aineiston poistaminen).

Aineistoja listatessa on syytä huomioida, että asiakkaan pankkiin lähettämät ja pankin asiakkaan noudettavaksi asettamat aineistot näkyvät molemmat aineistolistauksessa. Käyttämällä sopivia suodattimia getFileList-operaatiossa asiakkaan ohjelmisto voi valita mitä aineistoja haluaa listauksessa nähdä.

3.1.6 Aineiston poistaminen

Asiakkaan järjestelmä voi poistaa WS-kanavaan lähettämänsä aineiston. Poistaminen estää aineiston lähettämisen jatkokäsittelyyn.

WS-kanavassa asiakkaalla on mahdollisuus poistaa pankkiin lähettämänsä aineisto deleteFile-operaatiolla. Aineiston poistaminen muuttaa ainoastaan aineiston tilan tilasta WFP tilaan DEL. Tämä tilamuutos estää aineiston viemisen käsittelyyn, muuta vaikutusta sillä ei ole. Poistetut aineistot eivät näy getFileList-operaatiolla.

Aineiston poistamisesta on hyötyä ja se on yleensäkin mahdollista tehdä vain siinä aikaikkunassa, joka on aineiston pankkiin lähettämisen ja sen käsittelyyn ottamisen välillä. Esimerkiksi SEPA C2B-maksuaineistoilla tämä aikaväli on korkeintaan puoli tuntia.

Aineiston poistaminen tulee siis tehdä varsin nopeasti aineiston lähettämisen jälkeen, sillä käsittelyyn jo laitettua aineistoa (tila on FWD) ei voi WS-kanavassa enää poistaa tai peruuttaa. Tällaisen aineiston poistoyritykseen WS-kanava vastaa virheilmoituksella.

Aika, jonka aineisto odottaa WS-kanavassa jatkokäsittelyyn laittamista riippuu palvelusta ja aineistotyypistä. Esimerkiksi C2B-maksuaineistot käsitellään pankkipäivinä klo 7.00-18.00 puolen tunnin välein.

3.1.7 Aineistonhoitaja ja valtuutukset

Maksuliikeaineiston valtuutus perustuu WS-kanavan käyttäjätunnuksen Muodostaja-rooliin. Kyseisen käyttäjätunnuksen WS-kanavan sopimuksen asiakastunnus ja käyttäjätunnuksen parametrina oleva toimipaikkanumero muodostavat ns. aineistonhoitajan tunnisteen. Tämä aineistonhoitajan tunniste eli toimipaikka tulee olla merkittynä sallituksi lähettäjäksi tai noudettavan aineiston vastaanottajaksi siinä maksuliikesopimuksessa, jonka mukaisesti aineistoa käsitellään ja muodostetaan.

Aineistonhoitaja on maksuliikesopimukseen merkitty sallittu lähettäjä tai aineiston vastaanottaja. Aineistonhoitajalla on oma WS-kanavan sopimus ja siihen liittyvät omat käyttäjätunnukset ja käyttäjätunnusten varmenteet.

3.2 Esimerkkisanomia ja –palvelupyyntöjä

3.2.1 Pyyntösanoma

Tässä on malliksi getFileList –operaation SOAP-pyyntösanoma. Base64-enkoodatut elementtien sisällöt on lyhennetty ja poistetut osat korvattu kolmella pisteellä luettavuuden parantamiseksi.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
   <env:Header>
      <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
      wssecurity-secext-1.0.xsd" env:mustUnderstand="1">
         <wsse:BinarySecurityToken wsu:Id="bst_ag0md1SPzDjcLWHg" xmlns:wsu="http://docs.oasis-
         open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
         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">MIIC9TCCA...z2nIv3xpHPU=</wsse:BinarySecurityToken>
         <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
            <dsig:SignedInfo>
               <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
               c14n#"/>
               <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <dsig:Reference URI="#Body_87p1SixC35qs3Lpk">
                  <dsig:Transforms>
                     <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <exc14n:InclusiveNamespaces
                        xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList=""/>
                     </dsig:Transform>
                  </dsig:Transforms>
                  <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <dsig:DigestValue>ztKnhKXLpBQM/r3we3D0BdVeibE=</dsig:DigestValue>
               </dsig:Reference>
               <dsig:Reference URI="#Timestamp_MpXSne5nUJot8ltt">
                  <dsig:Transforms>
                     <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <exc14n:InclusiveNamespaces
                        xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#" PrefixList=""/>
                     </dsig:Transform>
                  </dsig:Transforms>
                  <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <dsig:DigestValue>NRvpjFck2OEDAcgy0WxxV1WTz3w=</dsig:DigestValue>
               </dsig:Reference>
            </dsig:SignedInfo>
            <dsig:SignatureValue>UPzp6yAQ...6Od5+GRI0w==</dsig:SignatureValue>
            <dsig:KeyInfo>
               <wsse:SecurityTokenReference xmlns:wsse="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" wsu:Id="str_2u1tu89DgKYG7uPe">
                  <wsse:Reference URI="#bst_ag0md1SPzDjcLWHg" ValueType="http://docs.oasis-
                  open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3"/>
               </wsse:SecurityTokenReference>
            </dsig:KeyInfo>
         </dsig:Signature>
         <wsu:Timestamp wsu:Id="Timestamp_MpXSne5nUJot8ltt" xmlns:wsu="http://docs.oasis-
         open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
            <wsu:Created>2011-08-16T11:42:28Z</wsu:Created>
            <wsu:Expires>2011-08-16T13:22:28Z</wsu:Expires>
         </wsu:Timestamp>
      </wsse:Security>
   </env:Header>
   <env:Body wsu:Id="Body_87p1SixC35qs3Lpk" xmlns:wsu="http://docs.oasis-
   open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
      <cor:downloadFileListin xmlns:cor="http://bxd.fi/CorporateFileService">
         <mod:RequestHeader xmlns:mod="http://model.bxd.fi">
            <mod:SenderId>1000000000</mod:SenderId>
            <mod:RequestId>1313494952760</mod:RequestId>
```

```
            <mod:Timestamp>2011-08-16T14:42:28.031+03:00</mod:Timestamp>
            <mod:Language>FI</mod:Language>
            <mod:UserAgent>OP Client</mod:UserAgent>
            <mod:ReceiverId>OKOYFIHH</mod:ReceiverId>
         </mod:RequestHeader>
         <mod:ApplicationRequest
         xmlns:mod="http://model.bxd.fi">PD94bWwg...ZXF1ZXN0Pg==</mod:ApplicationRequest>
      </cor:downloadFileListin>
   </env:Body>
</env:Envelope>
```

3.2.2 Vastaussanoma

```
<?xml version="1.0" encoding="UTF-8"?>
<S:Envelope xmlns:exc14n="http://www.w3.org/2001/10/xml-exc-c14n#"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-
1.0.xsd" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-
secext-1.0.xsd" xmlns:S="http://schemas.xmlsoap.org/soap/envelope/">
   <S:Header>
      <wsse:Security S:mustUnderstand="1">
         <wsu:Timestamp wsu:Id="_3" xmlns:ns11="http://docs.oasis-open.org/ws-sx/ws-
         secureconversation/200512" xmlns:ns10="http://www.w3.org/2003/05/soap-envelope">
            <wsu:Created>2011-08-16T11:42:29Z</wsu:Created>
            <wsu:Expires>2011-08-16T11:47:29Z</wsu:Expires>
         </wsu:Timestamp>
         <wsse:BinarySecurityToken wsu:Id="uuid_5ac774c6-d670-4168-be0f-084dcb8d92ac"
         EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-
         security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-
         200401-wss-x509-token-profile-1.0#X509v3" xmlns:ns11="http://docs.oasis-open.org/ws-
         sx/ws-secureconversation/200512" xmlns:ns10="http://www.w3.org/2003/05/soap-
         envelope">MIID2DCC...iuycKgsL6euA==</wsse:BinarySecurityToken>
         <ds:Signature Id="_1" xmlns:ns11="http://docs.oasis-open.org/ws-sx/ws-
         secureconversation/200512" xmlns:ns10="http://www.w3.org/2003/05/soap-envelope">
            <ds:SignedInfo>
               <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-
               c14n#"/>
               <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <ds:Reference URI="#_5002">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>lkuQU09sgqWIp02wRR1BDxCrxyk=</ds:DigestValue>
               </ds:Reference>
               <ds:Reference URI="#_3">
                  <ds:Transforms>
                     <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                  </ds:Transforms>
                  <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                  <ds:DigestValue>dz7uPSeuk9tmjOU777o6/+GczFE=</ds:DigestValue>
               </ds:Reference>
            </ds:SignedInfo>
            <ds:SignatureValue>BDV8Ctp...8rc0GX95w==</ds:SignatureValue>
            <ds:KeyInfo>
               <wsse:SecurityTokenReference>
                  <wsse:Reference ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-
                  200401-wss-x509-token-profile-1.0#X509v3" URI="#uuid_5ac774c6-d670-4168-be0f-
                  084dcb8d92ac"/>
               </wsse:SecurityTokenReference>
            </ds:KeyInfo>
         </ds:Signature>
      </wsse:Security>
   </S:Header>
   <S:Body wsu:Id="_5002">
```

```
     <ns2:downloadFileListout xmlns="http://model.bxd.fi"
     xmlns:ns2="http://bxd.fi/CorporateFileService">
        <ResponseHeader>
           <SenderId>1000000000</SenderId>
           <RequestId>1313494952760</RequestId>
           <Timestamp>2011-08-16T14:42:29.672+03:00</Timestamp>
           <ResponseCode>00</ResponseCode>
           <ResponseText>OK.</ResponseText>
           <ReceiverId>OKOYFIHH</ReceiverId>
        </ResponseHeader>
        <ApplicationResponse>PD94bWwgd...BvbnNlPg==</ApplicationResponse>
     </ns2:downloadFileListout>
   </S:Body>
</S:Envelope>
```

3.2.3 Palvelupyyntö getFilelist

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T09:48:31.177+03:00</Timestamp>
   <Status>NEW</Status>
   <Environment>TEST</Environment>
   <SoftwareId>soft</SoftwareId>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI="">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>sPNzEb+Mf5dchY5MTGq7GL1grEg=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>aIqreFNkxuy...nM4SXE8g==</SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>MIIC9TCCA...Iv3xpHPU=</X509Certificate>
         </X509Data>
      </KeyInfo>
   </Signature>
</ApplicationRequest>
```

3.2.4 Palveluvastaus getFileList

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationResponse xmlns="http://bxd.fi/xmldata/"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T09:48:33.668+03:00</Timestamp>
   <ResponseCode>00</ResponseCode>
   <ResponseText>OK.</ResponseText>
   <FileDescriptors>
      <FileDescriptor>
         <FileReference>5802</FileReference>
         <TargetId>MLP</TargetId>
         <ParentFileReference>5801</ParentFileReference>
         <FileType>pain.002.001.02</FileType>
         <FileTimestamp>2011-07-29T12:00:16.483+03:00</FileTimestamp>
```

```
      <Status>NEW</Status>
    </FileDescriptor>
    <FileDescriptor>
      <FileReference>5803</FileReference>
      <TargetId>MLP</TargetId>
      <ParentFileReference>5801</ParentFileReference>
      <FileType>pain.002.001.02</FileType>
      <FileTimestamp>2011-07-29T12:01:16.971+03:00</FileTimestamp>
      <Status>NEW</Status>
    </FileDescriptor>
  </FileDescriptors>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
      20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>LlpU5jyiDd5kO5FjJDIL7AWZyBQ=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>WKtQ1t8V1...LkGV9DMz0cQ==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIID1zCCAr...JKaoOlc5gLu</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</ApplicationResponse>
```

3.2.5 Palvelupyyntö getFile

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
  <CustomerId>1000000000</CustomerId>
  <Timestamp>2011-08-15T13:01:46.911+03:00</Timestamp>
  <StartDate>2011-08-15+03:00</StartDate>
  <Environment>TEST</Environment>
  <FileReferences>
    <FileReference>5803</FileReference>
  </FileReferences>
  <Compression>true</Compression>
  <SoftwareId>soft</SoftwareId>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
      20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>OQA4fiudfd6KJKR0KINTsE9Fyxc=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>c2RzFUa...9VBAnMQ==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIC9TC....v3xpHPU=</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
```

```
</ApplicationRequest>
```

3.2.6 Palveluvastaus getFile

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationResponse xmlns="http://bxd.fi/xmldata/"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T13:01:49.591+03:00</Timestamp>
   <ResponseCode>00</ResponseCode>
   <ResponseText>OK.</ResponseText>
   <Compressed>true</Compressed>
   <CompressionMethod>RFC1952</CompressionMethod>
   <Content>H4sIAAAA...epSdAwAA</Content>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI="">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>gQf1Tmlhw7KdS7MT10L5yaTDmm4=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>bzS0Itu...U/y6jRg==</SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>MIID1zCCA...oOlc5gLu</X509Certificate>
         </X509Data>
      </KeyInfo>
   </Signature>
</ApplicationResponse>
```

3.2.7 Palvelupyyntö uploadFile

```
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T13:01:31.990+03:00</Timestamp>
   <Environment>TEST</Environment>
   <TargetId>target</TargetId>
   <Compression>true</Compression>
   <SoftwareId>soft</SoftwareId>
   <FileType>pain.001.001.02</FileType>
   <Content>H4sIAAA...KU0HAAA=</Content>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI="">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>o9/bmBaH58Phw01oiQS/ttrP/sY=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>NwNRa...dTtMMqvg==</SignatureValue>
      <KeyInfo>
```

```
        <X509Data>
           <X509Certificate>MIIC9TC...nIv3xpHPU=</X509Certificate>
        </X509Data>
     </KeyInfo>
   </Signature>
</ApplicationRequest>
```

3.2.8 Palveluvastaus uploadFile

Tässä esimerkkitapauksessa on havaittu validointivirhe asiakkaan lähettämässä pain.001.001.02 -aineistossa.

```
<ApplicationResponse xmlns="http://bxd.fi/xmldata/"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:date="http://exslt.org/dates-and-times">
   <CustomerId/>
   <Timestamp>2011-08-15T12:29:04+03:00</Timestamp>
   <ResponseCode>601</ResponseCode>
   <ResponseText>Technical error in frontline, local:///xslt/maksuliike/decodeContent.xsl:57:
    xsl:message terminate=yes value='dp:parse() error: mismatched tag, expected MsgIfd at
    offset 335 of *dp:parse*' - Tranid = 241951411</ResponseText>
   <Compressed>false</Compressed>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI="">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
               <Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>ZnOs52PTalH/qv4cqFuQiUO+UNI=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>YQzRY1/...KQ1mz7/GQ==</SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>MIID1zCCAr...KaoOlc5gLu</X509Certificate>
            <X509IssuerSerial>
               <X509IssuerName>CN=OPK z/OS Certificate Authority, OU=TES3, O=OPK, L=Helsinki,
               C=FI</X509IssuerName>
               <X509SerialNumber>46</X509SerialNumber>
            </X509IssuerSerial>
         </X509Data>
      </KeyInfo>
   </Signature>
</ApplicationResponse>
```

Toisenlaiseen schema-virheeseen vastaus tulee tällaisena.

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationResponse xmlns="http://bxd.fi/xmldata/"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T13:01:34.851+03:00</Timestamp>
   <ResponseCode>12</ResponseCode>
   <ResponseText>Schemavalidation failed.</ResponseText>
   <FileType>pain.002.001.02</FileType>
   <Content>PD94bWw...dW1lbnQ+Cg==</Content>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
```

```
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <Reference URI="">
           <Transforms>
              <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
           </Transforms>
           <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
           <DigestValue>3GyOY2gXwgT7RFP8CIli4KQ5kcg=</DigestValue>
        </Reference>
     </SignedInfo>
     <SignatureValue>cBs4Lm...QvD1Q==</SignatureValue>
     <KeyInfo>
        <X509Data>
           <X509Certificate>MIID1zC...aoOlc5gLu</X509Certificate>
        </X509Data>
     </KeyInfo>
   </Signature>
</ApplicationResponse>
```

Tässä toisessa virhe-esimerkissä elementti ApplicationResponse.Content sisältää seuraavan pain.002.001.02 –aineiston (tietysti Base64-enkoodattuna). Katso näiden maksupalautteiden sisältö ja käyttö erillisestä SEPA C2B-maksamisen ohjeesta.

```
<?xml version="1.0" encoding="UTF-8"?>
<Document xmlns="urn:iso:std:iso:20022:tech:xsd:pain.002.001.02"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
<pain.002.001.02>
<GrpHdr>
<MsgId>1313401940313</MsgId>
<CreDtTm>2011-08-15T12:52:20+03:00</CreDtTm>
</GrpHdr>
<OrgnlGrpInfAndSts>
<NtwkFileNm>1313401937067</NtwkFileNm>
<OrgnlMsgNmId>pain.001.001.02</OrgnlMsgNmId>
<GrpSts>RJCT</GrpSts>
<StsRsnInf>
<StsOrgtr>
<Id>
<OrgId>
<PrtryId>
<Id>1000000000</Id>
</PrtryId>
</OrgId>
</Id>
</StsOrgtr>
<StsRsn>
<Cd>NARR</Cd>
</StsRsn>
<AddtlStsRsnInf>pain.001.001.02 could not be processed, please verify structure.cvc-
datatype-valid.1.2.1: 'A1001.00' is n</AddtlStsRsnInf>
<AddtlStsRsnInf>ot a valid value for 'decimal'.cvc-complex-type.2.2: Element 'InstdAmt' must
have no element [children],</AddtlStsRsnInf>
<AddtlStsRsnInf>and the value must be valid.</AddtlStsRsnInf>
</StsRsnInf>
</OrgnlGrpInfAndSts>
</pain.002.001.02>
</Document>
```

3.2.9 Palvelupyyntö deleteFile

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationRequest xmlns="http://bxd.fi/xmldata/">
   <CustomerId>1000000000</CustomerId>
   <Timestamp>2011-08-15T09:53:53.778+03:00</Timestamp>
   <StartDate>2011-08-15+03:00</StartDate>
```

```
   <Environment>TEST</Environment>
   <FileReferences>
      <FileReference>6152</FileReference>
   </FileReferences>
   <SoftwareId>soft</SoftwareId>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
      <SignedInfo>
         <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
         20010315#WithComments"/>
         <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
         <Reference URI="">
            <Transforms>
               <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            </Transforms>
            <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
            <DigestValue>TsZYDgKXMO6/nfTlGGFGlHL43pI=</DigestValue>
         </Reference>
      </SignedInfo>
      <SignatureValue>dgUhp4b...qelFFvQ==</SignatureValue>
      <KeyInfo>
         <X509Data>
            <X509Certificate>MIIC9TCCAd2g...Iv3xpHPU=</X509Certificate>
         </X509Data>
      </KeyInfo>
   </Signature>
</ApplicationRequest>
```

3.2.10 Palveluvastaus deleteFile

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationResponse xmlns="http://bxd.fi/xmldata/"
xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
     <CustomerId>1000000000</CustomerId>
     <Timestamp>2011-08-15T09:53:56.147+03:00</Timestamp>
     <ResponseCode>00</ResponseCode>
     <ResponseText>OK.</ResponseText>
     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="">
                    <Transforms>
                         <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                         signature"/>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>F4NXYMUcrwJ83p92msZ48Jga7+c=</DigestValue>
               </Reference>
          </SignedInfo>
          <SignatureValue>OUjhFKVG...qL5xb4MQ==</SignatureValue>
          <KeyInfo>
               <X509Data>
                    <X509Certificate>MIID1zCC...aoOlc5gLu</X509Certificate>
               </X509Data>
          </KeyInfo>
     </Signature>
</ApplicationResponse>
```

4 Web Services –kanavan tunnistepalvelu

4.1 Tunnistepalvelun toiminnot

4.1.1 Varmenteen rekisteröinti ja siirtoavain

Jotta WS-kanavaa voisi käyttää, tulee asiakkaan ohjelmistolla olla käytössään avainpari ja OP-Pohjola-ryhmän WS-kanavan Tunnistepalvelun myöntämä varmenne.

Asiakkaan ohjelmisto hakee varmenteen pankin WS-kanavasta.

Varmenteen hakemista varten asiakkaan tulee antaa ohjelmistolle siirtoavain, jonka avulla pankin Tunnistepalvelu tunnistaa ja tarkistaa ohjelmiston lähettämän pyynnön.

Asiakas saa siirtoavaimen tekemällä pankissa rekisteröinnin. Rekisteröinnin suorittaa pankin toimihenkilö. Rekisteröinti kohdistuu aina tiettyyn WS-kanavan käyttäjätunnukseen.

Rekisteröinnin yhteydessä pankin toimihenkilö tunnistaa asiakasta edustavan henkilön ja tarkastaa kyseisen henkilön valtuutuksen. Asiakas saa pankista asiakirjan, johon on tulostettu WS-kanavan käyttäjätunnus ja siirtoavaimen ensimmäinen osa, kahdeksan numeroa.

Siirtoavaimen toisen osan asiakas saa oman valintansa mukaan joko SMS-tekstiviestinä matkapuhelimeen tai postitettuna asiakkaan ilmoittamaan osoitteeseen.

Kun asiakkaalla on siirtoavaimen molemmat osat, yhteensä 16 numeroa, tulee hänen syöttää ne ohjelmistoonsa ja käynnistää varmenteen muodostusprosessi.

4.1.2 Avainparin luominen

Avaimen pituus on 2048 bit ja algoritmi RSA, allekirjoituksen tiivistealgoritmi on SHA-1.

Avainpari tulee luoda sellaisella algoritmilla ja menetelmällä, joka takaa riittävän hyvän satunnaisuuden.

4.1.3 Yksityisen avaimen säilytys

Yksityistä avainta tulee säilyttää niin turvallisesti, että ei ole vaaraa sen joutumisesta vääriin käsiin. Turvallisin säilytystapa on fyysinen turvamoduli, Hardware Security Module, HSM. Turvamodulia käytettäessä yksityinen avain luodaan turvamodulin sisällä eikä normaalikäytössä koskaan sitä voida siirtää turvamodulin ulkopuolelle. Jos yksityinen avain ei ole turvamodulissa, tulee sen vähintään olla riittävän vahvasti salatussa muodossa

Yksityisen avaimen käytön valvonta tulee järjestää niin turvallisesti, että vain valtuuden omaavat ohjelmistot pystyvät käyttämään yksityistä avainta.

Yksityisen avaimen haltija on itse vastuussa avaimen käytöstä, säilytyksestä ja mahdollisista väärinkäytöksistä.

Jos syntyy epäilys tai tulee tieto yksityisen avaimen joutumisesta vääriin käsiin tai jo tapahtuneesta väärinkäytöstä, tulee kyseiseen avaimeen liittyvä varmenne sulkea välittömästi pankin sulkupalvelun kautta.

4.1.4 Varmennepyynnön tekeminen

Asiakkaan ohjelmisto suorittaa varmennepyynnön pankin WS-kanavan Tunnistepalveluun. Ohjelmisto tarvitsee tähän toimintoon asiakkaan syöttämän 16-numeroisen siirtoavaimen ja WS-kanavan 10-numeroisen käyttäjätunnuksen.

Ohjelmisto suorittaa varmennepyynnön ja saatuaan pankin Tunnistepalvelusta varmenteen, tallentaa sen tulevaa käyttöä varten.

Julkisesta avaimesta tulee muodostaa pkcs10-muotoinen varmennepyyntö.

Varmennepyynnön subjektissa täytetään seuraavat kaksi tietoa:

```
C=FI

CN=[WS-kanavan käyttäjätunnus, 10 numeroa]
```

Varmennepyyntöjä on useita erilaisia ja niille tehdään pankin Tunnistepalvelussa tilanteesta riippuen erilainen tunnistus ja aitouden tarkistus.

Elementissä CertApplicationRequest.Content olla binäärinen pkcs10-varmennepyyntö (DER).

Kun varmennepyyntö perustuu pankissa tehtyyn rekisteröintiin eli siirtoavaimeen, tulee lisäksi elementissä CertApplicationRequest.TransferKey tulee olla 16-numeroinen siirtoavain. CertApplicationRequest ei tarvitse olla allekirjoitettu, kuten ei SOAP-sanomankaan.

Kun varmennepyyntö perustuu aiempaan varmenteeseen, tulee elementissä CertApplicationRequest.Content olla binäärinen pkcs10-varmennepyyntö. (Binäärinen content-elementin sisältö on scheman mukaisesti aina Base64-enkoodattu). CertApplicatIonRequest tulee olla allekirjoitettu sellaisella avaimella, jota vastaava varmenne on saman käyttäjätunnuksen käytössä jolle tässä haetaan varmennetta. SOAP-sanoma ei tarvitse olla allekirjoitettu.

Jos asiakkaan tietojärjestelmä hakee varmennetta sarjanumerolla, on elementissä CertApplicationRequest.SerialNumber oltava varmenteen sarjanumero. CertApplicationRequest ei tarvitse olla allekirjoitettu, kuten ei SOAP-sanomakaan.

Jos varmennepyynnössä oleva julkinen avain on jo saman käyttäjätunnuksen jossain aiemmassa varmenteessa, varmennepyyntö palauttaa tuon aiemman varmenteen, vaikka se olisi jo vanhentunutkin. Tästä ei tule virheilmoitusta vaan pyytävän ohjelman tulee itse havaita, että se sai kopion vanhasta varmenteesta, eikä syntynyt uutta varmennetta.

Asiakkaan ohjelmiston tulee varmennepyyntöä tehdessä ehdottomasti tarkistaa pankin Tunnistepalvelun SSL-varmenne, joka on tehty domainille wsk.op.fi. Tällä tarkistuksella ohjelmisto varmistaa varmennepyynnön todella menevän pankin palveluun.

4.1.5 Avaimen ja varmenteen käyttö

Asiakkaan yksityisellä avaimella tekee asiakkaan tietojärjestelmä digitaalisia allekirjoituksia. WS-kanavassa tulee allekirjoittaa sekä palvelupyyntö (ApplicationRequest) että SOAP-sanoma, kumpikin erikseen.

Allekirjoitus tehdään yksityisellä avaimella. Allekirjoittavan järjestelmän tulee laittaa allekirjoituksen yhteyteen myös varmenne. Tämä varmenne sisältää allekirjoitukseen käytettyä yksityistä avainta vastaavan julkisen avaimen. Tätä julkista avainta käyttäen vastaanottaja tarkistaa allekirjoituksen.

Allekirjoituksen avulla varmistetaan, että allekirjoitettu sanoma tai palvelupyyntö ei ole muuttunut allekirjoittamisen jälkeen, ja samalla todetaan sanoman tai palvelupyynnön lähettäjä, sillä vain yksityisen avaimen haltija on voinut sen allekirjoittaa.

Varmenteella yhdistetään julkinen avain ja sitä kautta koko avainpari haltijaan. WS-kanavan varmenteissa haltijan tunnisteena toimii varmenteen subjektissa oleva CommonName –tieto (CN), jossa lukee WS-kanavan käyttäjätunnus.

4.1.6 Varmenteen elinikä ja uusiminen

Asiakkaan ohjelmisto käyttää muodostamaansa tai muualta saamaan yksityistä avainta WS-kanavan sanomien ja palvelupyyntöjen digitaaliseen allekirjoittamiseen. Lisäksi ohjelmiston tulee laittaa kyseiseen avaimeen liittyvä pankin Tunnistepalvelusta saamansa varmenne jokaiseen allekirjoitukseen.

Varmenne on voimassa kaksi vuotta. Varmenne tulee uusia ennen edellisen vanhenemista. Uusimisen voi suorittaa aikaisintaan 60 kalenteripäivää ennen edellisen varmenteen vanhenemista. Jos varmenne vanhenee ennen uuden noutamista, on asiakkaan aloitettava koko rekisteröintiprosessi uudelleen eli haettava pankista uudet siirtoavaimet.

Asiakkaan vastuulla on havaita varmenteen lähestyvä vanheneminen ja suorittaa varmenteen uusiminen ajoissa. Asiakkaan ohjelmisto huolehtii varmenteen uusimisesta automaattisesti. Ohjelmisto näkee helposti varmenteen päättymispäivän joka kerta varmennetta käyttäessään.

Uuteen varmenteeseen on tehtävä uusi avainpari. Jos varmenteen uusimispyyntö tehdään aiemman varmenteen avainparilla, Tunnistepalvelu palauttaa vain kopion vanhasta varmenteesta.

Varmenteen uusintapyyntö on samanlainen kuin uuden varmenteen hakeminen, mutta uusinnassa ei käytetä siirtoavainta (CertApplicationRequest.TransferKey) vaan sen sijaan CertApplicationRequest allekirjoitetaan sellaisella yksityisellä avaimella, johon käyttäjätunnuksella on voimassaoleva varmenne. Uusintapyynnön aitouden tarkastaminen pankin Tunnistepalvelussa perustuu siis käyttäjätunnuksen edelliseen varmenteeseen, jonka on pyyntöä tehtäessä oltava voimassa.

4.1.7 Sulkutietojen nouto ja käyttö

Asiakkaan järjestelmän tulee noutaa Tunnistepalvelun sulkulista ja tarkistaa luottamiensa varmenteiden sulkutilanne tätä sulkulistaa vasten. Käytännössä sulkulistaa vasten tulee tarkistaa pankin vastaussanomassa olevat pankin palveluvarmenteet.

Tunnistepalvelu muodostaa sulkulistan kerran vuorokaudessa ja se on voimassa kaksi vuorokautta. Tunnistepalvelu saattaa muodostaa uuden sulkulistan myös varmenteen sulkemisesta, siis ohi normaalin päivitysrytmin.

4.1.8 Varmenteen ennenaikainen sulkeminen

Jos asiakas epäilee tai tietää yksityisen avaimen joutuneen vääriin käsiin, tulee hänen sulkea varmenne välittömästi soittamalla numeroon 010 252 8470.

Katso sulkemisen ohjeet ylempää tästä asiakirjasta.

4.2 Tunnistepalvelun sanomakuvaukset

Tässä on kuvattu Tunnistepalvelun WS-kanavassa käytetyt sanomat ja palvelupyynnöt.

SOAP-sanomien rakenne ja Tunnistepalvelun osoite ilmenee WSDL-tiedostosta.

Tuotannon WSDL-tiedosto on noudettavissa osoitteesta

https://wsk.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristön WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristössä on käytössä Tuotannon käyttäjätunnus, mutta avainpari ja varmenne ovat vain testikäyttöön tarkoitetut, turvallisuussyistä.

4.2.1 SOAP-sanomat ja WSDL

WSDL-tiedosto kuvaa SOAP-sanoman rakenteen.

Tunnistepalvelussa SOAP-sanomaa ei allekirjoiteta, aitouden varmistaminen allekirjoituksella tehdään vain palvelupyynnön (CertApplicationRequest) tasolla, ja joissain tapauksissa ei edes siellä.

4.2.2 Palvelupyynnöt ja schemat

XML Schema-tiedostot kuvaavat sanoman sisältämän palvelupyynnön ja palveluvastauksen.

Tunnistepalvelun WSDL on osoitteessa
https://wsk.op.fi/wsdl/MaksuliikeCertService.xml

Tunnistepalvelun Asiakastestiympäristön WSDL on osoitteessa
https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeCertService.xml

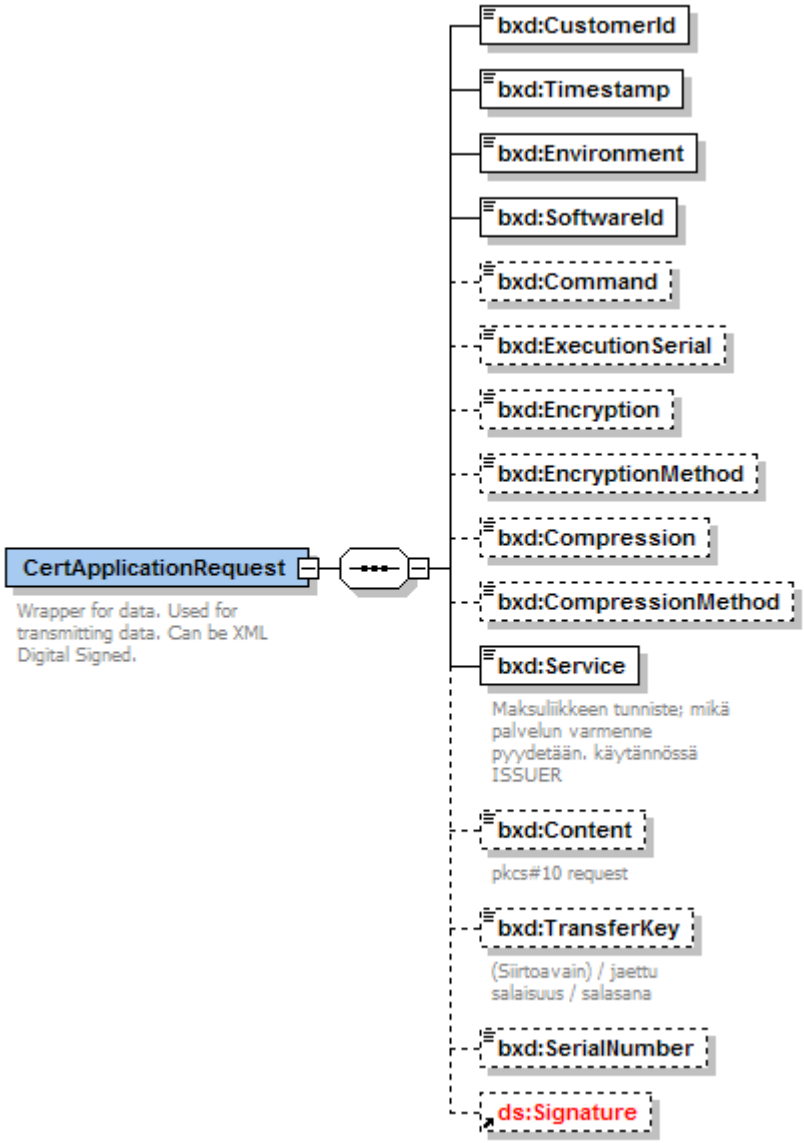
Schema-tiedostot löytyvät osoitteista:

https://media.op.fi/media/certapplication/CertApplicationRequest_200812.xsd

https://media.op.fi/media/certapplication/CertApplicationResponse_200812.xsd

Asiakkaan lähettämä palvelupyyntö on nimeltään CertApplicationRequest ja pankin Tunnistepalvelun antama palveluvastaus on nimeltään CertApplicationResponse.

4.2.2.1 CertApplicationRequest



Varmennepyynnön palvelupyynnössä keskeisimmät täytettävät elementit ovat:

CustomerId – varmenteen pyytäjän WS-kanavan käyttäjätunnus, 10 numeroa

Content – pkcs10- muotoinen varmennepyyntö base64 enkoodattuna

TransferKey – siirtoavain 16 numeroa, jos ollaan tekemässä ensimmäistä varmennepyyntöä käyttäjätunnuksella

Signature – XML-allekirjoitus jos ollaan tekemässä varmenteen uusimista

Lisäksi on joukko pakollisia tietoja:

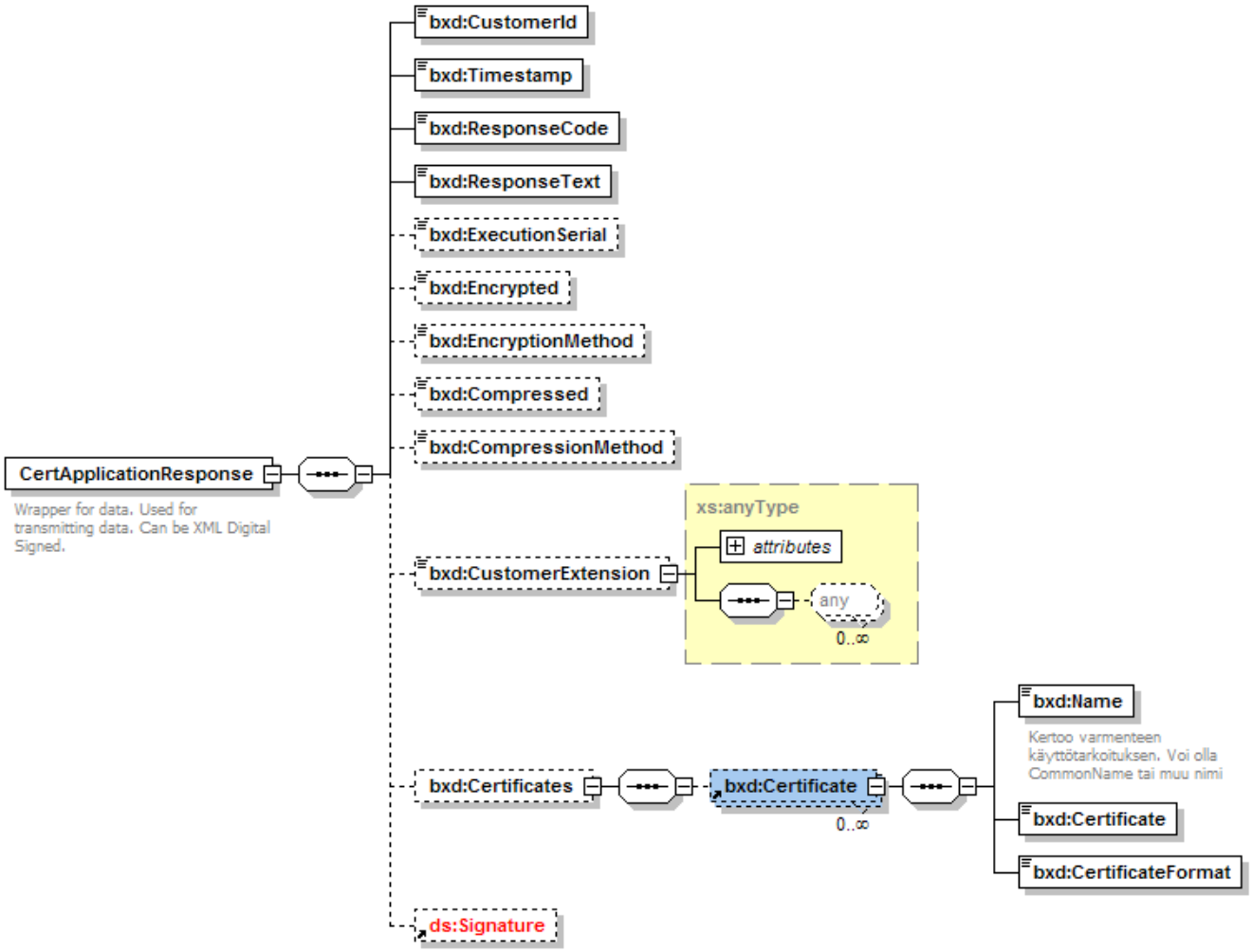
Timestamp – palvelupyynnön muodostushetken aikaleima, käytetään lähinnä selvittelyn apuna

Environment – tuotannossa oltava PRODUCTION, muuten pyyntö hylätään

SofwareId – palvelupyynnön tehneen ohelmiston nimi ja versio, käytetään lähinnä selvittelyn apuna

Service – MATU

4.2.2.2 CertApplicationResponse



4.3 Tunnistepalvelun esimerkkiaineistoja

4.3.1 Pyyntösanoma

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
     <env:Header/>
     <env:Body>
          <opc:getCertificatein xmlns:opc="http://mlp.op.fi/OPCertificateService">
               <opc:RequestHeader>
                    <opc:SenderId>1000012222</opc:SenderId>
                    <opc:RequestId>123</opc:RequestId>
                    <opc:Timestamp>2010-01-26T14:32:43.800+02:00</opc:Timestamp>
               </opc:RequestHeader>
               <opc:ApplicationRequest>PD94bWwgdmVy...
               GlvblJlcXVlc3Q+</opc:ApplicationRequest>
          </opc:getCertificatein>
     </env:Body>
</env:Envelope>
```

4.3.2 Vastaussanoma

```
<?xml version="1.0" encoding="UTF-8"?>
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
     <env:Header/>
     <env:Body>
          <opc:getCertificateout xmlns:opc="http://mlp.op.fi/OPCertificateService">
               <opc:ResponseHeader>
                    <opc:SenderId>1000012222</opc:SenderId>
                    <opc:RequestId>123</opc:RequestId>
                    <opc:Timestamp>2010-01-26T14:32:45.909+02:00</opc:Timestamp>
                    <opc:ResponseCode>00</opc:ResponseCode>
                    <opc:ResponseText>OK.</opc:ResponseText>
               </opc:ResponseHeader>
               <opc:ApplicationResponse>PD94bWwgdmVyc2...
               W9uUmVzcG9uc2U+</opc:ApplicationResponse>
          </opc:getCertificateout>
     </env:Body>
</env:Envelope>
```

4.3.3 Palvelupyyntö varmenteen uusiminen

Tässä esimerkissä on kyseessä varmenteen uusintapyyntö käyttäjätunnuksella 1000000047. Palvelupyyntö on allekirjoitettu, koska tunnistaminen ja aitouden tarkistaminen perustuu voimassaolevaan saman käyttäjätunnuksen varmenteeseen.

```
<?xml version="1.0" encoding="UTF-8"?>
<CertApplicationRequest xmlns="http://op.fi/mlp/xmldata/">
     <CustomerId>1000000047</CustomerId>
     <Timestamp>2010-01-26T14:32:44.191+02:00</Timestamp>
     <Environment>TEST</Environment>
     <SoftwareId>soft</SoftwareId>
     <Compression>false</Compression>
     <Service>MATU</Service>
     <Content>MIICZzCCAU8CA... 3slAmKGflLvw==</Content>
     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="">
                    <Transforms>
                         <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
               signature"/>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>i81y7OKgB8FBmOlv4gQWNtcCmLg=</DigestValue>
               </Reference>
          </SignedInfo>
          <SignatureValue>ZWSGuxU... gkZMGWA==</SignatureValue>
          <KeyInfo>
               <X509Data>
                    <X509Certificate>MIIDmjCCAoKg... Ct1jB0+UOw=</X509Certificate>
               </X509Data>
          </KeyInfo>
     </Signature>
</CertApplicationRequest>
```

4.3.4 Palveluvastaus varmenteen uusiminen

```
<?xml version="1.0" encoding="UTF-8"?>
<xd:CertApplicationResponse xmlns:xd="http://op.fi/mlp/xmldata/">
     <xd:CustomerId>1000000047</xd:CustomerId>
     <xd:Timestamp>2010-01-26T14:32:51.808+02:00</xd:Timestamp>
```

```
     <xd:ResponseCode>00</xd:ResponseCode>
     <xd:ResponseText>OK.</xd:ResponseText>
     <xd:Certificates>
          <xd:Certificate>
               <xd:Name>CN=1000000047,C=FI</xd:Name>
               <xd:Certificate>MIICvTCCAa... Ne+0U19z3z25nFb</xd:Certificate>
               <xd:CertificateFormat>X509v3</xd:CertificateFormat>
          </xd:Certificate>
     </xd:Certificates>
     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="">
                    <Transforms>
                         <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
               signature"/>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>ZdaOhjgcjfFb5aRwgMeWtlR5Oj0=</DigestValue>
               </Reference>
          </SignedInfo>
          <SignatureValue>PXPPXC... +TLjnO2g==</SignatureValue>
          <KeyInfo>
               <X509Data>
                    <X509Certificate>MIIDnDCCAo... A7xVA==</X509Certificate>
               </X509Data>
          </KeyInfo>
     </Signature>
</xd:CertApplicationResponse>
```

4.3.5 Palvelupyyntö varmennepyyntö siirtoavaimella

```
<?xml version="1.0" encoding="UTF-8"?>
<CertApplicationRequest xmlns="http://op.fi/mlp/xmldata/">
     <CustomerId>1000010583</CustomerId>
     <Timestamp>2010-02-04T12:40:00.929+02:00</Timestamp>
     <Environment>TEST</Environment>
     <SoftwareId>software 1.01</SoftwareId>
     <Compression>false</Compression>
     <Service>MATU</Service>
     <Content>MIICZz... Vr5kiQ==</Content>
     <TransferKey>2251401483958635</TransferKey>
</CertApplicationRequest>
```

4.3.6 Palveluvastaus varmennepyyntö siirtoavaimella

```
<?xml version="1.0" encoding="UTF-8"?>
<xd:CertApplicationResponse xmlns:xd="http://op.fi/mlp/xmldata/">
     <xd:CustomerId>1000010583</xd:CustomerId>
     <xd:Timestamp>2010-02-04T12:29:32.704+02:00</xd:Timestamp>
     <xd:ResponseCode>00</xd:ResponseCode>
     <xd:ResponseText>OK.</xd:ResponseText>
     <xd:Certificates>
          <xd:Certificate>
               <xd:Name>CN=1000010583,C=FI</xd:Name>
               <xd:Certificate>MIICvT... AssyGCD</xd:Certificate>
               <xd:CertificateFormat>X509v3</xd:CertificateFormat>
          </xd:Certificate>
     </xd:Certificates>
     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
```

```
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="">
                    <Transforms>
                         <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
               signature"/>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>pROjhxTaOs2FznVwOPhA7lbJYAE=</DigestValue>
               </Reference>
          </SignedInfo>
          <SignatureValue>Kv0oDf... 9BU3Iw==</SignatureValue>
          <KeyInfo>
               <X509Data>
                    <X509Certificate>MIIDn... xVA==</X509Certificate>
               </X509Data>
          </KeyInfo>
     </Signature>
</xd:CertApplicationResponse>
```

4.3.7 Palvelupyyntö hae varmenne sarjanumerolla

```
<?xml version="1.0" encoding="UTF-8"?>
<CertApplicationRequest xmlns="http://op.fi/mlp/xmldata/">
  <CustomerId>1000010583</CustomerId>
  <Timestamp>2010-02-04T12:53:55.325+02:00</Timestamp>
  <Environment>TEST</Environment>
  <SoftwareId>software 1.01</SoftwareId>
  <Compression>false</Compression>
  <Service>MATU</Service>
  <SerialNumber>442519889</SerialNumber>
</CertApplicationRequest>
```

4.3.8 Palveluvastaus hae varmenne sarjanumerolla

```
<?xml version="1.0" encoding="UTF-8"?>
CertApplicationResponseDocument::<xd:CertApplicationResponse
               xmlns:xd="http://op.fi/mlp/xmldata/">
  <xd:CustomerId>1000010583</xd:CustomerId>
  <xd:Timestamp>2010-02-04T12:54:02.370+02:00</xd:Timestamp>
  <xd:ResponseCode>00</xd:ResponseCode>
  <xd:ResponseText>OK.</xd:ResponseText>
  <xd:Certificates>
    <xd:Certificate>
      <xd:Name>CN=1000010583,C=FI</xd:Name>
      <xd:Certificate>MIICvTC... AssyGCD</xd:Certificate>
      <xd:CertificateFormat>X509v3</xd:CertificateFormat>
    </xd:Certificate>
  </xd:Certificates>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>fYSxDgACYGnJyt3R0Vg9aOLkdyk=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>O4vxL... n/th4DA==</SignatureValue>
```

```
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIDnD... 7xVA==</X509Certificate>
      </X509Data>
    </KeyInfo>
  </Signature>
</xd:CertApplicationResponse>
```

4.3.9 Palvelupyyntö hae palveluvarmenteet

```
<CertApplicationRequest xmlns="http://op.fi/mlp/xmldata/">
  <CustomerId>1000010522</CustomerId>
  <Timestamp>2010-02-04T12:59:35.727+02:00</Timestamp>
  <Environment>TEST</Environment>
  <SoftwareId>software 1.01</SoftwareId>
  <Service>MATU</Service>
</CertApplicationRequest>
```

4.3.10 Palveluvastaus hae palveluvarmenteet

```
<?xml version="1.0" encoding="UTF-8"?>
<xd:CertApplicationResponse xmlns:xd="http://op.fi/mlp/xmldata/">
     <xd:CustomerId>1000010522</xd:CustomerId>
     <xd:Timestamp>2010-02-04T12:59:36.589+02:00</xd:Timestamp>
     <xd:ResponseCode>00</xd:ResponseCode>
     <xd:ResponseText>OK.</xd:ResponseText>
     <xd:Certificates>
          <xd:Certificate>
               <xd:Name>CN=OPK z/OS Certificate Authority, OU=TES3, O=OPK, L=Helsinki,
               C=FI</xd:Name>
               <xd:Certificate>MIIDz... mRFjA==</xd:Certificate>
               <xd:CertificateFormat>X509v3</xd:CertificateFormat>
          </xd:Certificate>
          <xd:Certificate>
               <xd:Name>CN=MATU-demo-CA, C=FI</xd:Name>
               <xd:Certificate>MIICxD... BpA==</xd:Certificate>
               <xd:CertificateFormat>X509v3</xd:CertificateFormat>
          </xd:Certificate>
     </xd:Certificates>
     <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
          <SignedInfo>
               <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
               20010315#WithComments"/>
               <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
               <Reference URI="">
                    <Transforms>
                         <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
               signature"/>
                    </Transforms>
                    <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                    <DigestValue>k1wtlZ83yQmxQSAEdNHU4xIGfMo=</DigestValue>
               </Reference>
          </SignedInfo>
          <SignatureValue>Den... dCheQ==</SignatureValue>
          <KeyInfo>
               <X509Data>
                    <X509Certificate>MIID...A7xVA==</X509Certificate>
               </X509Data>
          </KeyInfo>
     </Signature>
</xd:CertApplicationResponse>
```

5 Testausympäristö ja testaaminen

OP-Pohjola tarjoaa WS-kanavan asiakasohjelmiston kehittäjille testausympäristön ja maksuliikepalveluiden loppukäyttäjille oman testausympäristön.

Ohjelmistokehittäjän testausympäristössä on tuotantopalvelua vastaava toiminnallisuus ja joissain tapauksissa sitä uudempi versio palvelusta. Tässä testiympäristössä käyttäjätunnukset ja varmenteet ovat vain testikäyttöön tarkoitetut. Tässä testiympäristössä ei suoriteta aineistoille vain tekninen validointi, muuta käsittelyä ei tehdä. Tämä testiympäristö on tarkoitettu lähinnä WS-kanavan client-ohjelmiston toteutuksen kehittämiseen, testaamiseen ja todentamiseen.

Loppukäyttäjän testausympäristössä on WS-kanavan toiminnallisuuden lisäksi myös liiketoiminta-aineistojen käsittelyä. Katso erillisestä asiakasohjeesta minkälaista aineistonkäsittelyä tässä ympäristössä on tarjolla. Tämä testausympäristö toimii asiakkaan tuotantopalvelun käyttäjätunnuksella, maksatustunnuksilla, tilinumeroilla. Ainoa tuotantokäytöstä eroava tunnus on varmenne, sillä oikeata tuotantoavainta varmenteineen ei voi turvallisuussyistä käyttää testausympäristössä. Tämä testausympäristö on tarkoitettu lähinnä loppuasiakkaiden pankkiyhteyden ja muiden ohjelmistojen todentamiseen ennen uusien palvelujen käyttöönottoa.

5.1 Ohjelmistokehittäjän testausympäristö wsk.asiakastesti.op.fi

5.1.1 Testaustunnusten tilaaminen

Testausympäristössä käytetään samoja käyttäjätunnuksia, SenderId ja CustomerId, kuin Tuotantoympäristössäkin. Avainpari ja varmenne ovat kuitenkin turvallisuussyistä testipuolella omansa, jotta asiakkaan testausympäristöstä ei olisi valtuuksia tuotantopalveluiden käyttöön.

Neuvoja ja apua voi pyytää osoitteesta

opk-sepa@op.fi

Testaustunnuksia ei siis tilata erikseen vaan ne saa pyydettäessä tai samalla kun tekee sopimuksen WS-kanavan käytöstä.

Testaustunnuksen varmennepyyntöä varten toimitetaan oma siirtoavain.

5.1.2 Testausympäristön osoite ja tiedostojen sijainti

Testausympäristön WS-kanavan WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristön Tunnistepalvelun WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeCertService.xml

5.1.3 Testivarmenteen hankkiminen

Asiakkaan ohjelmisto hakee WS-kanavan Asiakastestiympäristöstä varmenteen käyttäen WS-kanavan Tunnistepalvelun rajapintaa. Rajapinta on kuvattu tässä samaisessa ohjeessa.

Asiakkaan ohjelma muodostaa avainparin tässä ohjeessa luvussa Web Services – kanavan tunnistepalvelu kerrotulla tavalla. Asiakkaan ohjelma muodostaa julkisesta

avaimesta varmennepyynnön ja suorittaa varmennepyyntöoperaation WS-kanavan tunnistepalvelun Asiakastestiosoitteeseen.

WS-kanavan tunnistepalvelun Asiakastesti palauttaa varmennepyynnön vastauksena varmenteen, joka toimii siitä eteenpäin asiakkaan testikäyttäjätunnuksen kanssa.

5.2 Loppukäyttäjän testausympäristö wsk.asiakastesti.op.fi

5.2.1 Testaustunnusten hankkiminen

Loppuasiakkaan testausympäristössä asiakas käyttää samaa WS-kanavan käyttäjätunnusta kuin oikeassakin palvelussa. Samoin C2B-maksuaineistossa asiakas käyttää oikean palvelunsa maksatustunnusta ja maksutilejä. Testiympäristö ei suorita oikeasti maksuja, mutta aineiston oikeellisuuden tarkistus tapahtuu asiakkaan oikeita tili- ja sopimustietoja vasten.

Asiakas saa WS-kanavan käyttäjätunnuksen WS-kanavan sopimustulosteelta. Sopimuksen liitteeksi tulostuu tuotantovarmenteen siirtoavaimen lisäksi pyydettäessä erikseen myös testausympäristön varmenteen kaksiosainen siirtoavain.

Asiakkaan ohjelmisto muodostaa avainparin ja lähettää varmennepyynnön WS-kanavan testausympäristöön tässä ohjeessa kerrotulla tavalla.

Asiakastestiympäristön varmennepyyntöön asiakkaan tulee laittaa asiakastestiympäristön siirtoavain, jonka asiakas on saanut WS-kanavan sopimuksen liitteenä. Asiakastestiympäristö ei toimi oikealla tuotantovarmenteella tietoturvasyistä. Testiavainta ja testivarmennetta voi asiakas käyttää vapaammin testaamiseen ja todentamiseen, kun taas tuotantoavaimen ja tuotantovarmenteen tulee pysyä hyvin suojattuna.

Sähköpostiosoitteeseen opk-sepa@op.fi asiakas voi lähettää WS-kanavaa ja SEPA-siirtymää koskevia teknisiä kysymyksiä.

5.2.2 Testausympäristön osoite ja tiedostojen sijainti

Testausympäristön WS-kanavan WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeWS.xml

Testausympäristön Tunnistepalvelun WSDL-tiedosto on osoitteessa

https://wsk.asiakastesti.op.fi/wsdl/MaksuliikeCertService.xml

Tunnistepalvelun schema-tiedostot ovat osoitteessa

https://media.op.fi/media/certapplication/CertApplicationRequest_200812.xsd

https://media.op.fi/media/certapplication/CertApplicationResponse_200812.xsd

5.2.3 Testivarmenteen hankkiminen

Asiakkaan ohjelmisto hakee WS-kanavan Asiakastestiympäristöstä varmenteen käyttäen WS-kanavan Tunnistepalvelun rajapintaa. Rajapinta on kuvattu tässä samaisessa ohjeessa.

Asiakkaan ohjelma muodostaa avainparin tässä ohjeessa luvussa Web Services – kanavan tunnistepalvelu kerrotulla tavalla. Asiakkaan ohjelma muodostaa julkisesta avaimesta varmennepyynnön ja suorittaa varmennepyyntöoperaation WS-kanavan tunnistepalvelun Asiakastestiosoitteeseen.

WS-kanavan tunnistepalvelun Asiakastesti palauttaa varmennepyynnön vastauksena varmenteen, joka toimii siitä eteenpäin asiakkaan testikäyttäjätunnuksen kanssa.

6 Yleisimpiä kysymyksiä ja vastauksia

Tähän lisätään usein eteen tulevia kysymyksiä ja ongelmatilanteita.