OP Ryhmän
Yrityksen pankkiyhteys (Web Services) –kanavan asiakasohje

Lokakuu 2024

Sisältö

1 Johdanto

Web Services -kanava (myöhemmin WS-kanava) on OP Ryhmän yritys- ja yhteisöasiakkailleen tarjoama sähköinen tiedonsiirtokanava pankki- ja vakuutusaineistojen, viestien sekä toimeksiantojen turvalliseen lähettämiseen ja vastaanottoon.

Web Services on pankkien ja yritysasiakkaiden laitteiden välisen viestinnän liitäntäratkaisujen teknologia, ja ratkaisu perustuu kansainvälisiin standardeihin. WS-kanavan rajapintakuvaukset tehty useiden pankkiryhmien välisenä yhteistyönä ja määritykset ovat saatavilla Finanssialan sivuilta www.finanssiala.fi.

Tässä ohjeessa

- kuvataan ne toiminnot, jotka asiakkaan käyttämässä ohjelmistossa tulisi olla käytettävissä.
- kerrotaan Web Services -kanavan käyttöön liittyvistä toimintatavoista ja käytännöistä, joita ei ole kuvattu pankkien yhteisessä sanomamäärityksessä.
- kerrotaan Web Services -kanavan ja Tunnistepalvelun toiminnot sekä sanomakuvaukset.
- kerrotaan, miten OP Ryhmän Web Services -kanavan tarvitsemat varmenteet hankitaan ja miten niitä käytetään.
- Lisäksi mukana on ohjeita ohjelmiston toteuttajalle sekä esimerkkiaineistoja ja sanomia hyödynnettäväksi toteutuksessa. Tässä ohjeessa ei ole kuvattu maksuliikeaineistojen tai tiliraportoinnin sisältöä, niistä on omat tarkemmat kuvaukset.

Ohjelmistotoimittajia suositellaan seuraamaan op.fi:n Tietoa ohjelmistotoimittajille -sivua https://www.op.fi/yritykset/tietoa-ohjelmistotoimittajille. Sivulla viestitään WS-kanavan yleisistä asioista ja Maksuliikkeen palvelutiedotteessa mahdollisista häiriöistä.

Pankki ja asiakas tekevät WS-kanavan käytöstä sopimuksen. WS-kanavaa koskevan sopimuksen lisäksi WS-kanavan kautta käytettävistä Asiointipalveluista sovitaan erikseen.

1.1 Web Services -kanavan Tunnistepalvelu

WS-kanavan Tunnistepalvelu tuottaa ja hallinnoi varmenteita, joita käytetään WS-kanavan allekirjoitusten tarkistamisessa ja huolehtii varmenteiden sulkutietojen ylläpidosta ja julkaisusta.

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, vastaanottaja tarkistaa niiden allekirjoituksen. Allekirjoituksen avulla varmistetaan, että allekirjoitettu sanoma tai palvelupyyntö ei ole muuttunut allekirjoittamisen jälkeen.

Voimassa olevat WS-kanavan käytössä olevat varmenteet löytyvät op.fi-sivustolta kohdasta Yritysasiakkaat > Maksaminen ja laskutus > Pankkiyhteyskanava Web Services > Varmennepalvelu (www.op.fi/varmennepalvelu).

1.2 Varmenteen rekisteröinti ja siirtoavain

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

WS-kanavan käytön edellytys on, että asiakkaan ohjelmistolla on käytössään PKI-avainpari ja WS-kanavan Tunnistepalvelun myöntämä varmenne.

Kun WS-kanavan käytöstä on tehty sopimus, asiakas saa siirtoavaimen varmenteiden noutoa varten. WS-kanavan sopimusasiakirjalla näkyy WS-kanavan käyttäjätunnus (10 numeroa) ja siirtoavaimen ensimmäinen osa (kahdeksan numeroa). Siirtoavaimen toisen osan (kahdeksan numeroa) asiakas saa oman valintansa mukaan joko tekstiviestinä matkapuhelimeen tai postitettuna asiakkaan ilmoittamaan osoitteeseen.

Kun asiakkaalla on siirtoavaimen molemmat osat (yhteensä 16 numeroa), tulee hänen syöttää Siirtoavaimen molemmat osat sekä WS-kanavan käyttäjätunnus ohjelmistoonsa ja käynnistää varmenteen muodostusprosessi. Asiakkaan ohjelmisto lähettää varmennepyynnön Tunnistepalveluun ja saa vastaussanomassa asiakasvarmenteen.

1.3 Avainparin luonti

Asiakkaan vastuulla on WS-kanavassa käytetyn avainparin luominen. Pankki ei osallistu avainparin luomiseen eikä näe tai käsittele asiakkaan avainparia.

Asiakkaan ohjelmisto muodostaa avainparin siihen tarkoitetulla ohjelmistolla. Avainparin muodostavan ohjelman tulee huolehtia, että muodostukseen käytetty algoritmi on riittävän laadukas ja hyvien kryptografisten käytäntöjen mukainen. Avainpari tulee luoda sellaisella algoritmilla ja menetelmällä, joka takaa riittävän hyvän satunnaisuuden. Avaimen pituuden tulee olla 2048 bittiä ja algoritmi RSA, allekirjoituksen tiivistealgoritmi on sha256RSA.

1.4 Avaimen ja varmenteen käyttö

WS-kanavassa sekä palvelupyyntö (ApplicationRequest) että SOAP-sanoma allekirjoitetaan kumpikin erikseen.

Asiakkaan ohjelmisto käyttää asiakkaan yksityistä avainta (avainparin yksityinen osa) WS-kanavan sanomien ja palvelupyyntöjen digitaaliseen allekirjoittamiseen.

Allekirjoittavan järjestelmän tulee laittaa allekirjoituksen yhteyteen yksityistä avainta vastaava varmenne. Varmenne sisältää julkisen avaimen, jota käyttäen vastaanottaja tarkistaa allekirjoituksen. Se, jonka hallussa yksityinen avain on, pystyy lähettämään pankkiin WS-kanavan kautta palvelupyyntöjä ja aineistoja, jotka pankki toteuttaa yksityiseen avaimeen varmenteen avulla liitetyn asiakkaan nimissä.

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.

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.

1.5 Varmenteen elinikä ja uusiminen

Asiakasvarmenne on voimassa enintään kaksi vuotta ja varmenne tulee uusia ennen sen vanhenemista. Asiakkaan vastuulla on suorittaa varmenteen uusiminen ajoissa. Asiakkaan ohjelmisto huolehtii varmenteen uusimisesta automaattisesti ja ohjelmisto voi todeta varmenteen päättymispäivän joka kerta, kun varmennetta käytetään.

Varmenteen uusimisen voi suorittaa aikaisintaan 60 kalenteripäivää ennen voimassa olevan varmenteen vanhenemista. Jos varmenne vanhenee ennen uuden noutamista, on asiakkaan haettava pankista uudet siirtoavaimet.

Uuteen varmenteeseen on luotava uusi avainpari. Jos asiakkaan ohjelmisto tekee varmennepyynnön samasta avainparista kuin jo ennestään käytössä oleva varmenne, pankin Tunnistepalvelu ei muodosta uutta varmennetta vaan palauttaa kopion jo aiemmin tehdystä varmenteesta.

Uuden varmenteen hakeminen, kun edellinen varmenne on aktiivinen (60 päivän uusimisajan kuluessa), edellyttää uusien julkisten ja yksityisten avainten luomista ja CSR:n (Certificate Signing Request) luomista. Jos samoilla avaimilla luodaan uusi CSR, se toimii edelleen alkuperäisenä ja edellisen varmenteen kopio on taas käytettävissä. Turvallisuussyistä tulee käyttää uusia avaimia.

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 voimassa oleva varmenne. Uusintapyynnön aitouden tarkastaminen pankin Tunnistepalvelussa perustuu käyttäjätunnuksen edelliseen varmenteeseen, jonka on pyyntöä tehtäessä oltava voimassa.

1.6 Varmennepyynnön tekeminen ja varmenteen luominen

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

Julkisesta avaimesta tulee muodostaa pkcs10-muotoinen varmennepyyntö.

Varmennepyynnön subjektissa tulee olla ainoastaan nämä kaksi tietoa:

- C=FI
- CN= [WS-kanavan käyttäjätunnus, 10 numeroa]

Kun kyseessä on käyttäjätunnuksen ensimmäinen varmenne (ilman varmennetta tehtävä ensimmäinen varmennepyyntö), perustuu se pankissa tehtyyn rekisteröintiin eli siirtoavaimeen. Tällöin elementissä CertApplicationRequest. TransferKey tulee olla 16-numeroinen siirtoavain sekä elementissä CertApplicationRequest.CustomerId 10 numeroa pitkä WS-kanavan 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. CertApplicationRequest:in eikä SOAP-sanoman tarvitse olla allekirjoitettuja.

Kun kyseessä on voimassa olevan varmenteen uusiminen (varmennepyyntö perustuu aiempaan varmenteeseen), tulee CertApplicationRequest allekirjoittaa sillä avaimella, jota vastaava varmenne on saman käyttäjätunnuksen käytössä, jolle haetaan varmennetta. Elementissä CertApplicationRequest.CustomerId tulee olla 10 numeroa pitkä WS-kanavan käyttäjätunnus. SOAP-sanoman ei tarvitse olla allekirjoitettu

Jos asiakkaan ohjelmisto hakee varmennetta sarjanumerolla, tulee elementissä CertApplicationRequest.SerialNumber olla varmenteen sarjanumero. CertApplicationRequest:in eikä SOAP-sanoman tarvitse olla allekirjoitettuja.

Jos varmennepyynnössä oleva julkinen avain on sama kuin jo saman käyttäjätunnuksen jossain aiemmassa varmenteessa, pankin vastaussanoma palauttaa julkista avainta vastaavan aiemman varmenteen, vaikka se olisi jo vanhentunut. Tästä ei tule virheilmoitusta, vaan pyytävän ohjelman tulee havaita, että se sai kopion vanhasta varmenteesta eikä uutta varmennetta syntynyt.

1.7 Varmenteen sulkeminen, sulkutietojen nouto ja käyttö

Jos asiakas epäilee tai tietää yksityisen avaimensa joutuneen vääriin käsiin, tulee asiakkaan sulkea varmenne välittömästi.

Asiakas voi sulkea varmenteensa soittamalla puhelinnumeroon 010 252 8470. Varmenteen sulkemiseen tarvitaan 10 numeroa pitkä WS-kanavan käyttäjätunnus tai suljettavan varmenteen sarjanumero. Kun asiakas on sulkenut varmenteen, pankki ei hyväksy allekirjoitusta, joka on tehty kyseistä varmennetta vastaavalla salaisella avaimella.

Pankki julkaisee varmenteiden sulkulistaa. Sulkulista (CRL, Certificate Revocation List) sisältää käytöstä poistettujen varmenteiden sarjanumerot ja käytöstä poiston syykoodin.

Tunnistepalvelu muodostaa sulkulistan vähintään kerran vuorokaudessa ja on voimassa kolme vuorokautta. Tunnistepalvelu muodostaa uuden sulkulistan myös varmenteen sulkemisesta.

Sulkulistan osoitteet löytyvät varmenteiden, joihin luotetaan, CRL Distribution Points –kentästä. Asiakkaan järjestelmän tulee noutaa Tunnistepalvelun sulkulista ja tarkistaa luottamiensa varmenteiden (CA-varmenne ja pankin palveluvarmenteet) voimassaolo sulkulistalta. Käytännössä sulkulistaa vasten tulee tarkistaa pankin vastaussanomassa olevat pankin palveluvarmenteet.

Suljettua varmennetta ei voi enää ottaa uudelleen käyttöön. Jos asiakas ottaa varmenteen sulkemisen jälkeen käyttöön uuden varmenteen, on asiakkaan rekisteröidyttävä uudelleen pankin konttorissa ja tehtävä WS-kanavan kautta uusi varmennepyyntö uuden siirtoavaimen kanssa.

1.8 Termit

Julkinen avain	Julkisen avaimen järjestelmässä epäsymmetrisessä salauksessa käytettävän avainparin julkinen osa. Julkisella avaimella salattu tieto voidaan purkaa vain Avainparin yksityisellä avaimella. Kun Julkisen avaimen haltija on tiedossa, sitä vastaavalla yksityisellä avaimella tehty sähköinen allekirjoitus voidaan tarkistaa. Julkisen avaimen haltija voidaan luotettavasti tunnistaa Varmenteen avulla. Julkisilla avaimilla varmennetaan allekirjoituksia ja toteutetaan salausta.
PKI	Public Key Infrastucture. Kokonaisuus, jonka avulla luodaan, hallinnoidaan, jaetaan, käytetään, varastoidaan ja lakkautetaan Julkisen avaimen Varmenteita. PKI määrittää kontrollit ja standardit, joita Varmentajien tulee noudattaa toiminnassaan varmistaakseen sähköisten varmenteiden yhteensopivuus, tunnistettavuus ja saatavuus ja se perustuu julkisen avaimen salausalgoritmiin.
Siirtoavain	Varmennepyynnön aitouden tarkistaminen perustuu siirtoavaimeen, jonka varmennepyynnön lähettävä tietojärjestelmä laittaa pyynnön mukaan.
Transport Layer Security	TLS eli Transport Layer Security on salausprotokolla, jolla suojataan datan aitous ja siirtyminen kahden sovelluksen välillä.

Varmenne	Varmenne on sähköinen asiakirja, joka kytkee julkisen avaimen ja tiedon sen haltijasta toisiinsa. 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 julkisen avaimen ja asiakkaan tunnisteen. Pankin Tunnistepalvelu muodostaa varmennepyynnön mukaisen varmenteen ja antaa sen asiakkaan tietojärjestelmälle vastaussanomassa.
XML-allekirjoitus	Tekniikka, jolla varmistetaan XML-asiakirjan aitous ja muuttumattomuus. Allekirjoitus tehdään yksityisellä avaimella ja tarkistetaan Julkisella avaimelle.
Yksityinen avain	Avainparin yksityinen osa, jota käytetään PKI-järjestelmässä epäsymmetrisessä salauksessa. Yksityinen avain on määritelty yksikäsitteisesti tietylle taholle. Yksityisellä avaimella voidaan purkaa tietoa, joka on salattu avainparin julkisella avaimella.

2 Salausalgoritmit

Asiakkaan tulee käyttää alla olevia salausalgoritmeja. Ne sisältävät tiivistefunktioita, sähköisiä allekirjoitusalgoritmeja ja salausalgoritmeja.

Salausalgoritmit ja -protokollat suojaavat arkaluontoista, luokittelematonta tietoa.

Salausohjelma salaa siirrettävää dataa ja purkaa sen salauksen. OP tukee aineiston siirtojen salauksessa ja salauksen purkamisessa TLS:n versiota 1.2 tai uudempaa. WS-kanava tukee protokollana vain TLS 1.2:ta tai uudempaa. OP:lle ei voi lähettää aineistoja vanhoilla TLS 1.0- ja TLS 1.1 -versioilla.

OP suosittelee, että asiakkaat käyttävät vähintään SHA-256-algoritmia.

OP:n WS-kanava tukee tällä hetkellä seuraavia salausalgoritmeja:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CB_

Algoritmit tunnetaan nimellä SHA-2, ja ne on nimetty tiivisteen kokojen mukaan bitteinä: SHA-256, SHA-384 ja SHA-512.

3 Web Services -kanavan toiminnot

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 ApplicationRequest:in, joka on varsinainen palvelupyyntö. ApplicationRequest sisältää palveluun liittyvän liiketoiminta-aineiston (esimerkiksi maksuaineiston) ja se on digitaalisesti allekirjoitettu.

Asiakkaan tietojärjestelmä lähettää palvelupyynnön ja saa WS-kanavasta heti vastauksen. Lähetetty aineisto jää pankkiin odottamaan käsittelyä. Käsittelystä saattaa syntyä palauteaineisto, jonka asiakkaan tietojärjestelmän tulee noutaa erikseen.

Ajantasapalveluissa asiakkaan ohjelmisto lataa pankkiin aineiston ja saa heti vastaussanomassa ajantasapalvelun lopullisen vastauksen.

3.1 Aineiston lähettäminen pankkiin

WS-kanava tarkistaa lähetetyn aineiston muodon oikeellisuuden heti lähetyksen yhteydessä ja hylkää aineiston, jos se ei ole muodollisesti oikea. Tällöin 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.

3.2 Aineiston hakeminen pankista

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.

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 uudelleen. Noudetun aineiston tila muuttuu tilasta NEW tilaan DLD, mutta itse aineisto säilyy edelleen näkyvissä ja noudettavissa.

3.3 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.

3.4 Ajantasapalvelut

WS-kanavassa on tarjolla tällä hetkellä alla luetellut ajantasapalvelut.

Palvelun tekninen nimi / FileType	Kuvaus
CustomerCreditTransferInitiantionV02 pain.001.001.02.xsd	C2B SEPA-pikasiirto
CustomerCreditTransferInitiantionV03 pain.001.001.03.xsd	C2B SEPA-pikasiirto
pain.001.001.02 TP4 PS01 ja pain.001.001.03 TP4 PS01	C2B SEPA-pikasiirto
pain.001.001.02 TP4 PS01	POPS–pikamaksu, schema-versio V02. Palaute pain.002.001.02 TP4 PS01.
pain.001.001.03 TP4 PS01	POPS–pikamaksu, schema-versio V03. Palaute pain.002.001.03 TP4 PS01.
TP4 PS01	POPS-pikamaksu
TP1 ES	Tilisiirto omien tilien välillä
TP1 1SS	Tilin saldokysely

TP1 1VA	Valuuttatilien saldoyhteenveto
TP1 2ST	Tilin tapahtumakysely
TP1 2SY	Tilien laajennettu saldoyhteenveto
TP1 2KS	Konsernitilin saldo, otot sekä panot -kysely
TP1 3ST	Tilin tapahtumaotekysely (Tilin kuluvan päivän noutamattomat tiliotetapahtumat)
ORDER TU	Uusintatiliotteen tilaus

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

3.4.1.1 C2B SEPA-pikasiirto ajantasapalveluna

Palvelun tekninen nimi/FileType on TP4 PS01.

CustomerCreditTransferInitiantionV02 pain.001.001.02.xsd tai CustomerCreditTransferInitiantionV03 pain.001.001.03.xsd. Palvelulla voi tehdä yksittäisen ajantasainen SEPA-pikasiirto.

Ajantasaisen yksittäisen SEPA-pikasiirtomaksun voi maksaa Suomessa ja muualla SEPA-alueella toimiviin pankkeihin ja maksupalveluntarjoajille, jotka ovat ottaneet SEPA-pikasiirtopalvelun käyttöön.

Erillisinä pikasiirtoaineistotyyppeinä (pain.001.001.02 TP4 PS01 tai pain.001.001.03 TP4 PS01) lähetettävät SEPA-pikasiirrot käsitellään välittömästi ja lähettäjä saa heti liikennöintiyhteyden aikana välittömän online-palautesanoman (ei noudettava aineisto). Yksittäisillä SEPA-pikasiirroilla ei ole eräpäiväkäsittelyä ja niitä voi lähettää 24/7/365. Erillisiä ajantasaisia maksuja ei välitetä koskaan POPS-järjestelmään, vaan ne käsitellään aina SEPA-pikasiirtoina. Jos saajan pankki ei pysty käsittelemään SEPA-pikasiirtoja, maksu hylätään.

3.4.2 Pikamaksu (POPS)

Ajantasainen maksu toiseen suomalaiseen rahalaitokseen-palvelun tekninen nimi/FileType on TP4 PS01.

Pankkiyhteysohjelma laittaa palvelupyynnön 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	sentteineen, 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.....0
0000000000001127.11.20110000000000000001245.....
.....E0.....110727145700000
100000000000000000
```

Vastaanotettava pikamaksukuittaus

Pikamaksukuittaus on tiedosto, jossa on kaksi tietuetta; kuittaustietue ja OP:n tapahtuman päättymistietue ($$EOF). Pikamaksukuittaus saattaa olla myös pelkkä OPn palvelun $$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 OPn palvelusta 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. 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

3.4.3 Ajantasamaksu – tilisiirto omien tilien välillä

Tilisiirto omien tilien välillä-palvelun palvelun tekninen nimi/FileType on TP1 ES.

Pankkiyhteysohjelma laittaa palvelupyynnön 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 sentteineen 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 "Tilisiirto"

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

3.4.4 Saldokysely

Saldokysely-palvelun tekninen nimi/FileType on TP1 1SS.

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

$$TP1 1SS konttorinumero tilinumero X

- 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

3.4.5 Valuuttatilien saldoyhteenveto

Valuuttatilien saldoyhteenveto -palvelun tekninen nimi/FileType on TP1 1VA.

Pankkiyhteysohjelma voi kysyä valuuttatilien saldoyhteenvedon ohjaussanomalla

$$TP1 1VA X tilimuoto valuuttakoodi

missä

- X on merkki X
- tilimuoto on AV-KP (=OP-valuuttatili), MTA (=määräaikainen OP-valuuttatili) tai ALL (=kaikki valuuttatilit)
- valuuttakoodi on valuutan ISO-koodi (esim. USD) tai ALL (=kaikki valuutat)

Saldoyhteenvedon vastausosa muodostuu yhdestä tai useammasta tietueesta, joista vain viimeisessä on mukana rahayksikön koodi.

Tiedon nimi	Pituus	Selitys
Asiakkaan nimi	15	
Tilien lukumäärä tässä tietueessa	3	
Tuleeko saldotietueita lisää	1	0=ei tule, 1=tulee
Tili (0-n kpl)		
Konttorinumero	6	
Tilinumero	8	
Tilimuoto	5	
Valuuttakoodi	3	
Korko %	6	4 des.
Saldot (3 kpl)		
Valuuttamäärä	13	2 des.
Etumerkki	1	+/-
Kirjauspäivä	6	ppkkvv
Vasta-arvo	13	2 des.
Etumerkki	1	+/-
Keskikurssi	10	7 des.
Summien lukumäärä	2	
Summat (0-n kpl)		
Yhteensä euroa	15	
Etumerkki	1	+/-
Kirjauspäivä	6	ppkkvv
Rahayksikön koodi	1	1=euro Tämä kenttä on mukana vain viimeisessä tietueessa.

Tilejä lisää -kenttä saa arvon 1, mikäli sanomassa on lisää tilitietueita. Tietueessa on enintään kolmea tiliä koskevat tiedot. Tilejä koskevat yhteenvedot esitetään tietueittain; viimeisessä tietueessa ei siis ole koko sanoman saldoja yhteensä, vaan ne on laskettava erikseen jokaiselta tietueelta.

Jokaisessa tilitietueessa on kolme saldoa, joissa on esitetty mahdolliset tulevien kirjauspäivien saldot. Puuttuvan saldon kirjauspäivämääräkentässä on nollaa.

3.4.6 Tilin tapahtumakysely

Tilin tapahtumakysely -palvelun tekninen nimi/FileType on TP1 2ST.

Pankkiyhteysohjelma voi kysyä tilin tapahtumia ohjaussanomalla

$$TP1 2ST konttorinumero tilinumero X

missä

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

Tapahtumakyselyn vastausosa

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	
Konttorinumero	6	
Tilinumero	8	
Päivämäärä	6	ppkkvv
Tapahtumat (10 kpl)		
Tapahtumapäivä	6	ppkkvv
Selite	12	
Rahamäärä	11	2 des.
Etumerkki	1	+/-
Saldo	11	2 des.
Etumerkki	1	+/-
Luottoraja	11	2 des.
Etumerkki	1	+/-
Katevaraukset	11	2 des.
Etumerkki	1	+/-
Nostovara	11	2 des.
Etumerkki	1	+/-
Rahayksikön koodi	1	1=euro

3.4.7 Tilien laajennettu saldoyhteenveto

Tilien laajennettu saldoyhteenveto -palvelun tekninen nimi/FileType on TP1 2SY.

Pankkiyhteysohjelma voi kysyä tilien laajennettua saldoyhteenvetoa ohjaussanomalla

$$TP1 2SY

Saldoyhteenvedon vastausosa muodostuu yhdestä tai useammasta tietueesta.

Tiedon nimi	Pituus	Selitys
Asiakkaan nimi	40	
Tilien lukumäärä tässä tietueessa	3	

Tuleeko saldotietueita lisää	1	0=ei tule, 1=tulee
Tili ja saldo (0-n kpl)		
Konttorinumero	6	
Tilinumero	8	
Saldo	13	11 kok. + 2 des.
Etumerkki	1	+/-
Nostovara	13	11 kok. + 2 des.
Etumerkki	1	+/-
Korkoprosentti	6	4 des.
Saldon pvm.	8	vvvvkkpp

Sanoman tietuepituus vaihtelee.

3.4.8 Konsernitilikysely

Konsernitilin saldon, otot sekä panot-palvelun tekninen nimi/FileType on TP1 2KS.

Pankkiyhteysohjelma laittaa palvelupyynnön 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

3.4.9 Tapahtumaotekysely

Tilin kuluvan päivän noutamattomat tiliotetapahtumat-palvelun tekninen nimi/FileType on TP1 3ST.

Pankkiyhteysohjelma laittaa palvelupyynnön 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 tapahtumaotteeseen
13	Välitystapa	AN1	
14	Saaja/Maksaja .1 Nimi .2 Nimen lähde	 AN35 AN1	 tyhjä., A, J tai K
15	Saajan tili .1 Tilinumero .2 Tili muuttunut -tieto	 AN14 AN1	 tyhjä merkki, *
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, mutta selitetekstit ovat pankkikohtaisia. Korjauksissa koodeja käytetään sekä pano- että ottotapahtumalla.

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
- 720 = otto
- 721 = korttimaksu otto
- 722 = shekki otto
- 723 = taksibussiseteli otto
- 730 = palkkio otto
- 740 = korkoveloitus otto
- 750 = korkohyvitys pano
- 760 = laina (sisältäen lyhennyksen, koron ja palkkion) otto
- 761 = lainan lyhennys otto

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

Kuittikoodin arvot ovat:

- tyhjä = 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 alun perin antaneen tilin muuttuneen pankin järjestelmissä.

Tili muuttunut -tiedon arvot ovat:

- tyhjä = 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	

Nimi tarkenteen 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 välitetään asiakkaalle vain, jos kysely ei onnistu tai häiriöiden takia tiedot eivät ole ajan tasalla.

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	

3.4.10 Uusintatiliotteen tilaus

Uusintatiliotteen tilaus -palvelun tekninen nimi/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 muodostumisaikataulussa seuraavaksi aamuksi.

3.5 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)
    - 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.

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.

3.6 Aineiston poistaminen

Asiakas voi poistaa pankkiin lähettämänsä aineisto deleteFile-operaatiolla. Aineiston poistaminen muuttaa aineiston tilan tilasta WFP tilaan DEL. Tämä tilamuutos estää aineiston viemisen jatkokäsittelyyn, muuta vaikutusta sillä ei ole. Poistetut aineistot eivät näy getFileList-operaatiolla.

Aineiston poistaminen on mahdollista tehdä aineiston pankkiin lähettämisen ja sen käsittelyyn ottamisen välillä. Jo käsittelyyn laitettua aineistoa ei voi enää poistaa.

Aika, jonka aineisto odottaa WS-kanavassa jatkokäsittelyyn laittamista riippuu palvelusta ja aineistotyypistä. Esimerkiksi C2B-maksuaineistot käsitellään pankkipäivinä klo 02:30 ja 7:00-18:00 puolen tunnin välein.

3.7 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.

3.8 Esimerkkisanomia ja palvelupyyntöjäPyyntösanoma

Esimerkki getFileList –operaation SOAP-pyyntösanomasta. 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>
```

3.8.2 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>IkuQU09sgqWIp02wRR1BDxCrxyk=</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>
```

3.8.3 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>alqreFNkxuy...nM4SXE8g==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIC9TCCA...Iv3xpHPU=</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ApplicationRequest>
```

3.8.4 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>LlpU5jyiDd5kO5FjJDlL7AWZyBQ=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>WKtQ1t8V1...LkGV9DMz0cQ==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIID1zCCAr...JKaoOlc5gLu</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ApplicationResponse>
```

3.8.5 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>
```

3.8.6 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>
```

3.8.7 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>
```

3.8.8 Palveluvastaus uploadFile

Esimerkki validointivirheestä 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>2018-03-16T17:14:38+02:00</Timestamp>
<ResponseCode>12</ResponseCode>
<ResponseText>Schema validation failed. - Tranid = 661232927</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>TIA6ACHFI9HVswrPCi6jhA10G14=</DigestValue>
        </Reference>
    </SignedInfo>
<SignatureValue>o9F1TZvdEFTeb09aBSf6TzGmCE/F09jd...S5YAiEGZtxvfR/FqO3i6u5P9VfK0cCy6czYqJs9Ew==</Signature
Value>
    <KeyInfo>
        <X509Data>
            <X509Certificate>MIIGLzCCBBegAwIBAgIDKCf...POM88+Y+luwn7HmqB</X509Certificate>
            <X509IssuerSerial>
                <X509IssuerName>C=FI, CN=CUSTOMER TEST OP Services CA V2</X509IssuerName>
                <X509SerialNumber>2631673</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 virhe-esimerkissä elementti ApplicationResponse.Content sisältää seuraavan pain.002.001.02 –aineiston (Base64-enkoodattuna). Katso maksupalautteiden sisältö ja käyttö erillisestä C2B-maksujen asiakasohjeesta.

```
<?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>
```

3.8.9 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/nfTlGGFGIHL43pl=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>dgUhp4b...qelFFvQ==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIC9TCCAd2g...Iv3xpHPU=</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ApplicationRequest>
```

3.8.10 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 Tunnistepalvelun sanomat ja palvelupyynnöt

4.1 SHA1-varmenne korvataan SHA256 varmenteella

OP Ryhmä lopettaa SHA1-varmenteen ja digitaalisen allekirjoituksen tuen ja korvaa sen SHA256-varmenteella.

Vanha SHA1-palvelu suljetaan 31.8.2025 ja tämän jälkeen asiakkaiden tulee käyttää SHA256-algoritmiä. Aineistot eivät välity eteenpäin Web Services-kanavassa 1.9.2025 alkaen, jos pankkiyhteysohjelmisto muodostaa yhteyden vanhentuneella varmenteella / TLS-salausmenetelmillä.

Asiakkaiden tulee tehdä muutokset ohjelmistoonsa SHA256 algoritmin käyttöönottoon palvelupyynnöissä (ApplicationRequest) sekä SOAP-pyyntösanomassa (SOAPRequest).

- SignatureMethod Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-sha256
- DigestMethod Algorithm=http://www.w3.org/2001/04/xmlenc#sha256

Vastaavasti vastaussanomat on allekirjoitettu SHA256 certifikaatilla ja algoritmillä.

Osoitteet Yrityksen pankkiyhteyden tuotantoympäristöön:

- https://wsk.op.fi/services/OPCertificateServiceV2
- https://wsk.op.fi/services/CorporateFileServiceV2

4.2 Tunnistepalvelun sanomakuvaukset

SOAP-sanomien rakenne ja Tunnistepalvelun osoite on kuvattu WSDL-tiedostossa.

Tunnistepalvelussa SOAP-sanomaa ei allekirjoiteta, aitouden varmistaminen allekirjoituksella tehdään vain palvelupyynnön (CertApplicationRequest) tasolla.

WSDL-tiedosto on noudettavissa osoitteesta

- SHA1: https://wsk.op.fi/wsdl/MaksuliikeWS.xml.
- SHA256: https://wsk.op.fi/wsdl/MaksuliikeWSV2.xml

4.3 Palvelupyynnöt ja schemat

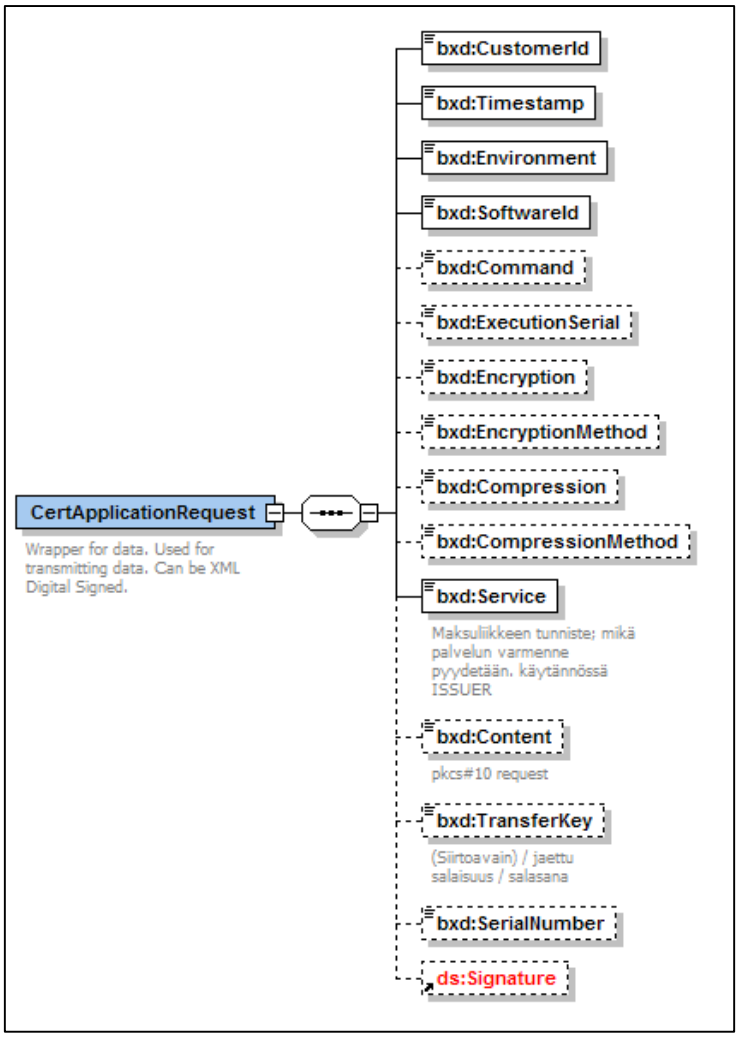
XML Schema-tiedostot kuvaavat sanoman sisältämän palvelupyynnön ja palveluvastauksen.

Tunnistepalvelun WSDL on osoitteessa

- SHA1: https://wsk.op.fi/wsdl/MaksuliikeCertService.xml
- SHA256: https://wsk.op.fi/wsdl/MaksuliikeCertServiceV2.xml

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

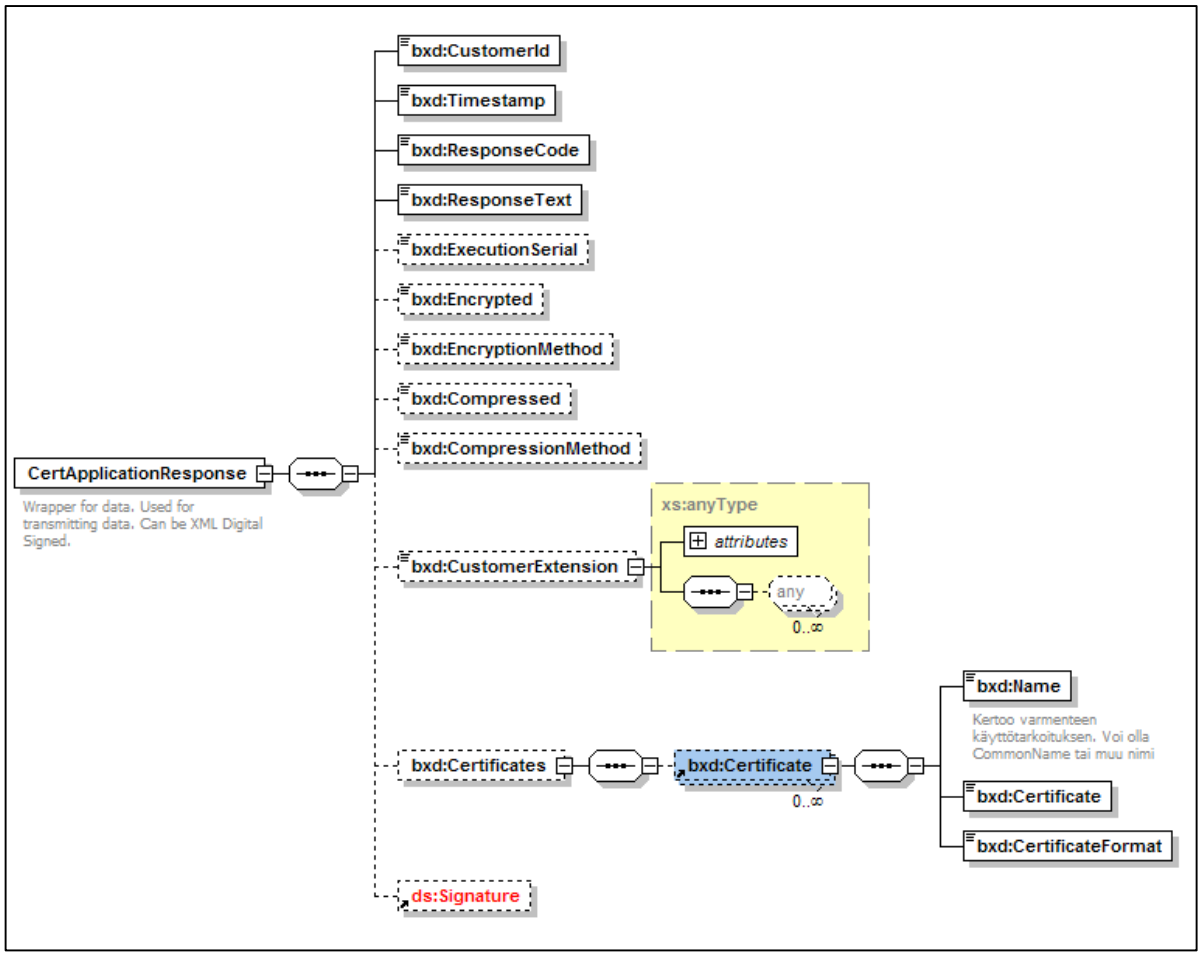
4.3.1 CertApplicationRequest



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
- Pakolliset tiedot:
    - Timestamp – palvelupyynnön muodostushetken aikaleima, käytetään lähinnä selvittelyn apuna
    - Environment – tuotannossa oltava PRODUCTION, muuten pyyntö hylätään.
    - SofwareId – palvelupyynnön tehneen ohjelmiston nimi ja versio, käytetään lähinnä selvittelyn apuna
    - Service – MATU

4.3.2 CertApplicationResponse



4.4 Tunnistepalvelun esimerkkipyyntöjä 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>
```

4.4.2 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>
```

4.4.3 Palvelupyyntö Varmenteen uusiminen

Esimerkissä on varmenteen uusintapyyntö käyttäjätunnuksella 1000000047. Palvelupyyntö on allekirjoitettu, koska tunnistaminen ja aitouden tarkistaminen perustuu voimassa olevaan 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>
```

4.4.4 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>ZdaOhjgcjfFb5aRwgMeWtIR5Oj0=</DigestValue>
                </Reference>
        </SignedInfo>
        <SignatureValue>PXPPXC... +TLjnO2g==</SignatureValue>
        <KeyInfo>
                <X509Data>
                        <X509Certificate>MIIDnDCCAo... A7xVA==</X509Certificate>
                </X509Data>
        </KeyInfo>
    </Signature>
</xd:CertApplicationResponse>
```

4.4.5 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>
```

4.4.5.1 Yksityiskohtaiset ohjeet getCertificate-pyynnön luomiseen siirtoavaimilla

a. Yksityistä ja julkista avainparia käyttävän CSR:n (Certificate Signing Request) tulee näyttää tältä:

```
-----BEGIN CERTIFICATE REQUEST-----
MIICZz... Vr5kiQ==
-----END CERTIFICATE REQUEST-----
```

b. Luodun CSR:n alku- ja lopputagit poistetaan ja binääriarvo lisätään samoin kuin kohdassa 4.4.5 Palvelupyyntö Varmennepyyntöön siirtoavaimella:

```
...
<Content>MIICZz... Vr5kiQ==</Content>
...
```

c. Kohdassa 4.4.5 luodun pyynnön Varmennepyyntö siirtoavaimella pitää base64-koodattuna antaa seuraavat arvot:

```
PD94bWwgdmVy.....GlvblJlcXVlc3Q+
```

e. Base64-koodattu Palvelupyyntö pitää sisällyttää Pyyntösanomaan kuten osiossa 4.4.1:

```
<opc:ApplicationRequest>PD94bWwgdmVy...
GlvblJlcXVlc3Q+</opc:ApplicationRequest>
```

f. Alkuperäinen getCertificate-pyyntö Siirtoavaimilla on nyt valmis, ja sen voi lähettää pankkiin uuden Varmenteen noutamista varten.

4.4.6 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>
```

4.4.7 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>
```

4.4.8 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>
```

4.4.9 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>
```

4.4.10 Palveluvastaus Hae palveluvarmenteet

```
<?xml version="1.0" encoding="UTF-8"?>
<CertApplicationResponse xmlns="http://op.fi/mlp/xmldata/"xmlns:ns2=
"http://www.w3.org/2000/09/xmldsig#">
        <CustomerId>1000000047</CustomerId>
        <Timestamp>2018-0319T09:43:33.504+02:00</Timestamp>
        <ResponseCode>00</ResponseCode>
        ResponseText>OK.</ResponseText>
        <Certificates>
                <Certificate>
                        <Name>CN=CUSTOMER TEST OP-Pohjola Services CA, C=FI</Name>
                        <Certificate>MIIGIDCCBAigAwI...kVj8Sv1dNBrnd52LISFjx2wCXud</Certificate>
                        <CertificateFormat>X509v3</CertificateFormat>
                </Certificate>
                <Certificate>
                        <Name>CN=CUSTOMER TEST OP-Pohjola WS CA, C=FI</Name>
                        <Certificate>MIIGGjCCBAKgAwIBAgIDAT5bMA0G...dMwP+ujyr/EoHCNOrGcpAs</Certi
                        ficate>
                        <CertificateFormat>X509v3</CertificateFormat>
                </Certificate>
                <Certificate>
                        <Name>C=FI, CN=CUSTOMER TEST OP Services CA V2</Name>
                        <Certificate>MIIGGzCCBAOgAwIBAgIDKCJGMA0GCSqGS...3U+YS9431RzBqGk48uE5KSxAcUZ
                        vLnc6372j0a7WsISQ==</Certificate>
                        <CertificateFormat>X509v3</CertificateFormat>
                </Certificate>
                <Certificate>
                        <Name>C=FI, CN=CUSTOMER TEST OP WS CA V2</Name>
                        <Certificate>MIIGFTCCA/2gAwIBAgIDKBo1M...tkoEmxWW1K8rootLAROAf+a
                        2K13wgSwOA==</Certificate>
                        <CertificateFormat>X509v3</CertificateFormat>
                </Certificate>
        </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>VyXRntiU4/X/h1GOGj0Tjtt7wlc=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>RR5AfAz0Rt7NPUQnnTJA0IuRUtZ9cQUIZRq0DN....sp
                VilxA==</SignatureValue>
                <KeyInfo>
                        <X509Data>
                         <X509Certificate>MIIGKjCCBBKgA...HsHt8Os4G7ov7mhKYQ==</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
</CertApplicationResponse>
```