Oma Säästöpankit

Versio 1.4

30.10.2026

Palvelukuvaus

Web Service -yhteys

samlink
A Kyndryl Company

samlink
A Kyndryl Company

Sisällys

1 Yleistä 3

2 Web Services 3

2.1 Palvelukuvauksessa käytettyjä lyhenteitä ja termejä 4

3 Sopimus Web Services -yhteyden käytöstä 4

3.1 Varmenteet 4

3.2 WS-yhteyden käytön edellytykset 5

4 Varmenteiden ja PKI avaimien käyttö pankkiyhteyksissä 5

4.1 Asiakkaan tunnistaminen ja palvelun käyttöoikeus 6

4.2 Varmenteiden mitätöinti 7

5 Web Services -yhteyden aineistot 8

5.1 Aineistot 8

6 Yleiskuvaus siirtokäytännöstä 8

6.1 Aineiston luonti ja lähetys pankkiin 9

6.2 Aineiston nouto pankista 10

6.3 Pankkiyhteysohjelmiston tekniset ohjeet 11

7 Pankkiyhteysohjelman Web Service – yhteystestaus 11

8 Aikataulut 11

9 web services -yhteyden osoite 11

10 PKI –varmenteet ja niiden jakelu 12

Samlinkin neuvontanumerot 12

Versioluettelo

Käsikirjan versiotiedot

Versionro	Päiväys	Muutokset
1.0	17.10.2017	alkuperäinen Oma Säästöpankin versio
1.1	17.10.2018	- Poistettu varmenteen noutomahdollisuus turvasähköpostilla - Muutettu neuvonnan aukioloaika
1.2	12.4.2024	Poistettu viittaukset PATU-linjasiirtokanavaan
1.3	04.07.2025	Lisätty filetype VT Verkkolaskun virheilmoituksen lähetys
1.4	30.10.2026	Lisätty aineistotyyppi XI

samlink
A Kyndryl Company

1 Yleistä

Tämä dokumentti kuvaa Samlinkin toteuttaman Web Services-yhteyskäytännön.

Web Services (WS) on Samlinkin pankkien yritysasiakkaille (jäljempänä asiakas) tarkoitettu yhteyskäytäntö asiakkaan ja pankin väliseen eräsiirtoaineistojen välitykseen. Web Services -yhteyskäytäntö perustuu maailmalla yleisesti tunnettuihin standardeihin ja noudattaa W3C-määrityksiä (World Wide Web Consortium, ks. www.W3.org. Tietoliikenne tapahtuu aina SSL-salatun yhteyden kautta Internet (TCP/IP) -verkossa, joten VPN-salausta ei tarvita. Asiakkaan tunnistaminen perustuu Public Key Infrastructure (PKI) -varmenteeseen, jonka asiakas saa pankista. Pankki toimii varmenteiden rekisteröijänä ja Samlink toimii varmentajana (CA, Certificate Authority).

WS-yhteyskäytäntö mahdollistaa yritysten tiedonsiirtoprotokollan, PKI-tunnistamisen ja turvamääritykset Web Services Interoperability Organizationin määritysten mukaisesti (ks. www.ws-i.org). Tämä dokumentti kuvaa standardia siten, kun sitä sovelletaan Samlinkissa.

WS-protokollan tekniset yksityiskohdat on kuvattu muissa dokumenteissa, jotka ovat saatavilla Finanssialan Internet-sivuilta www.finanssiala.fi. Kuvaukset ovat englanninkielisiä.

2 Web Services

WS-tietoliikenne tukee tiedostojen siirtämistä asiakkaalta tai asiakkaalle. Yhteyksissä asiakas on aina aktiivinen osapuoli ja avaa yhteyden sekä lähettäessään aineistoja pankkiin että noutaessaan aineistoja pankista (push-pull).

Käyttäjällä pitää olla WS-yhteyskäytäntöä tukeva pankkiyhteysohjelmisto.

2.1 Palvelukuvauksessa käytettyjä lyhenteitä ja termejä

WS	Web Services. De facto -tietoliikennestandardi, joka noudattaa kansainvälisiä määrityksiä, kuten SOAP ja XML.
PKI	Public Key Infrastructure. Kansainvälinen määritys yhteyden osapuolen (tunnuksen omistajan) tunnistamiseksi.
XML	Extensible Markup Language. Formaatti jota käytetään mm. Yrityksen maksut -palvelussa ja SOAP-sanomissa.
CA	Certificate Authority. PKI-varmenteen myöntäjä/julkaisija
SSL	Secure Socets Layer. Internet-yhteyksissä käytetty salaustekniikka
HTTPS	Hypertext Transfer Protocol Secure. http-protokollan salattu versio
SOAP	Standardoitu WS-yhteyden sanomamuoto

3 Sopimus Web Services -yhteyden käytöstä

Asiakas ja pankki tekevät sopimuksen Web Services -yhteyden käytöstä (Web Services -yhteys). Sopimuksessa määritellään asiakas ja asiakasta edustava yhteyshenkilö.

Sopimuksen teon yhteydessä pankki luovuttaa käyttäjää varten varmenteen noutopyyntöön tarkoitetun kertakäyttösalasanan 1-osan sopimuksella ja 2-osa postitetaan suljetussa kirjekuoressa. Kuoren osoiteikkunassa näkyy kuoren kohdistintieto.

3.1 Varmenteet

Sopimuksen teon yhteydessä luovutetuissa sopimuslomakkeessa on tiedot, jotka käyttäjä tarvitsee ladatakseen oman PKI-varmenteen Samlinkista yrityksen järjestelmään.

Tarvittavat tiedot ovat:

- WS-käyttäjätunnus
- kohdistintieto kirjeessä
- kertakäyttöinen salasana.

Varmenne on pankin rekisterissä nimetty aina tietylle organisaatiolle. Jos varmennetta käytetään koneiden välisessä automaattisessa yhteydessä, voi yrityksen varmenne olla jonkun muun kuin

nimetyn henkilön käytettävissä. Asiakkaan vastuulla on huolehtia siitä, että varmenteet säilytetään asianmukaisesti ja siten, että vain niiden luvallinen käyttö on mahdollista.

3.2 WS-yhteyden käytön edellytykset

- Asiakkaalla pitää olla voimassa oleva sopimus pankin kanssa Web Services -yhteyden käytöstä.
- Asiakkaalla pitää olla sopimuksen teon yhteydessä pankista saatu kertakäyttöinen salasana, joilla asiakaskohtainen PKI-varmenne noudetaan Samlinkin palvelusta asiakkaan järjestelmään. PKI-varmenteeseen perustuva digitaalinen allekirjoitus, asiakkaan todennus ja oikeudet käyttää ko. palvelua tarkistetaan pankissa varmenteen perusteella.
- Ohjelmisto digitaalisen allekirjoituksen ja pankkiyhteyden toteuttamiseksi.

Lähetettävä maksuliikeaineisto tai aineiston noutopyyntö allekirjoitetaan digitaalisesti asiakkaan PKI-varmenteeseen kuuluvalla yksityisellä avaimella ennen pankkiyhteyttä. Allekirjoituksen voi tehdä erillisellä ohjelmistolla tai pankkiyhteysohjelmaan integroituna osana.

Digitaalinen allekirjoitus toteutetaan ja pankkiyhteys muodostetaan ohjelmistoilla, jotka tukevat Samlinkin Web Services -kuvauksen mukaista yhteyttä. Yleinen Web Services -kuvaus on suomalaisten pankkien yhdessä määrittelemä ja se on saatavilla Finanssialan Internet-sivuilta, www.finanssiala.fi.

Samlinkin pankkikohtaiset ohjeet kuvauksen soveltamiseksi ovat erillisessä palvelukuvauksessa.

Ohjelmistotaloille on myös erillinen Samlinkin kuvaus Web Services rajapinnasta.

Ennen sanomien lähettämistä pankkiin sanomien rakenteellinen oikeellisuus tulee varmistaa ja sanomat pitää testata.

4 Varmenteiden ja PKI avaimien käyttö pankkiyhteyksissä

Web Services -yhteyksissä asiakas tunnistetaan käyttäen PKI-tekniikkaa ja varmenteita (engl. Certificate). PKI eli Public Key Infrastructure on toimintamalli avainten ja varmenteiden käyttöön. Toimintamallissa hyödynnetään avainpareihin perustuvia epäsymmetrisiä salausmenetelmiä siten, että voidaan toteuttaa turvallisen sähköisen asioinnin perusteet, kuten digitaalinen allekirjoitus allekirjoittajan yksityisellä avaimella.

Varmenteella tarkoitetaan nimenomaan X.509-muotoisia varmenteita, jonka myöntäjä (CA) on Samlink. Tässä luottamuksellisessa suhteessa on ainoastaan kaksi osapuolta, pankki ja asiakas. Varmenne myönnetään asiakkaan Web Services -sopimuksen perusteella.

Asiakas käyttää varmennetta, tai pikemminkin sen kuvaamaa salaista ja julkista avainta, aineiston ja sen lähetyksen allekirjoittamiseen ja pankki asiakkaan tunnistamiseen. Allekirjoituksesta pankki voi

todentaa, että aineiston on allekirjoituksellaan hyväksynyt taho, jolla on oikeus kyseisen varmenteen ja vastaavan palvelun käyttöön. Samalla todennetaan, että aineistoa ei ole muunnettu sen allekirjoittamisen jälkeen.

Varmenne on voimassa kaksi vuotta, jonka jälkeen se täytyy uusia.

Digitaalinen allekirjoitus toteutetaan pankkien Web Services -kuvauksessa määritellyllä tavalla, jossa ApplicationRequest-niminen XML-rakenne on allekirjoituksen kohteena. ApplicationRequest on yksinkertainen XML-rakenne, joka sisältää asiakkaan ja aineiston yksilöivät tiedot.

Digitaalinen allekirjoitus on envelope-tyyppinen. Se tarkoittaa, että koko allekirjoitettavan sanoman sisältö, mahdollisine lähetettävine aineistoineen kuuluu allekirjoituksen piiriin. Digitaalinen allekirjoitus kattaa sekä tunnistamisen että aineiston muuntumattomuuden. Mikä tahansa muutos sisältöön, tärvelee allekirjoituksen. Muuttuminen todetaan pankin Web Services -palvelussa ja yhteys hylätään. Vastaavasti pankki allekirjoittaa ApplicationResponse-nimisen sanoman muodostaessaan sanomia asiakkaalle Web Services -yhteydellä. Web Services -yhteyden osapuolet voivat siten varmistaa, että sanoma on tullut sovitulta osapuolelta ja että tieto ei ole muuttunut matkalla.

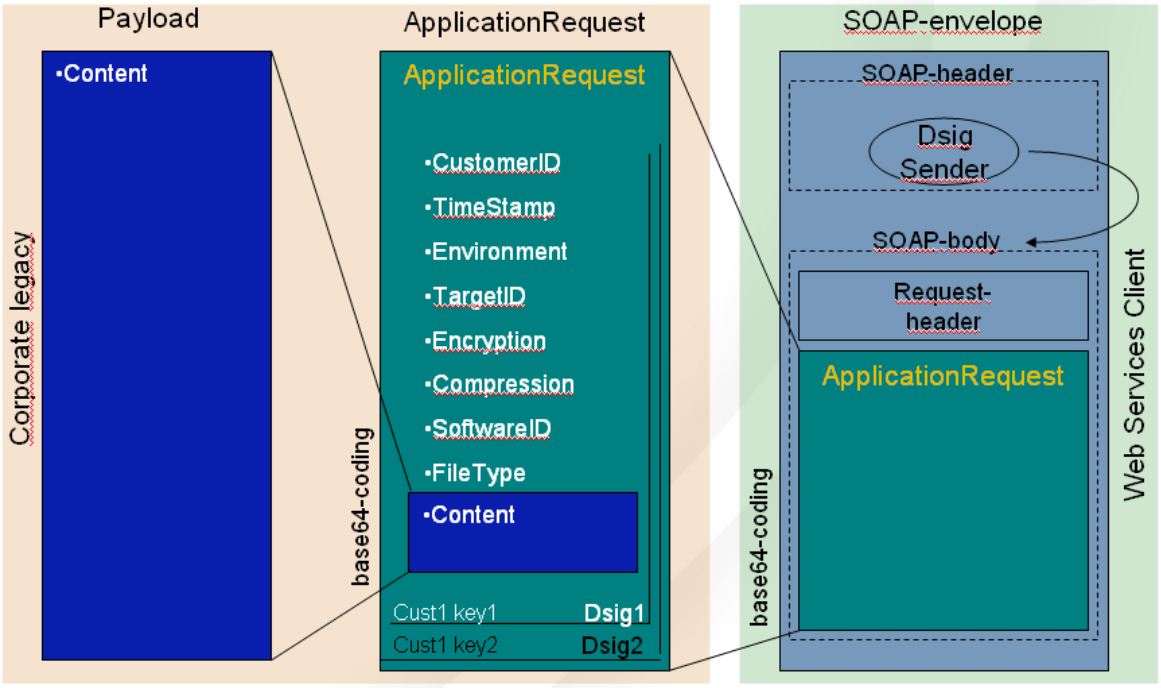
Envelope-tyyppinen allekirjoitus on mahdollista kahdentaa, jolloin jälkimmäinen allekirjoittaja allekirjoittaa koko sisällön ja myös edellisen allekirjoituksen. Kahdenkertainen ApplicationRequestin allekirjoitus ei ole käytettävissä Samlinkin Web Services -yhteyskäytännössä.

4.1 Asiakkaan tunnistaminen ja palvelun käyttöoikeus

Valtuutus palvelun käyttöön perustuu ApplicationRequest-sanoman digitaaliseen allekirjoitukseen ja siten asiakkaan tunnistamiseen sekä valtuutuksen tarkistamiseen pankin palvelusopimusjärjestelmästä. Ennen pankkiyhteyttä allekirjoitettu ApplicationRequest-sanoma välitetään SOAP-sanoman sisällä, sen body-elementissä. ApplicationRequestin allekirjoitus voi tapahtua ennakkoon ennen lähetystä.

SOAP-sanoma allekirjoitetaan aineiston toimittajan omalla PKI-avaimella. Tämä allekirjoitus on vain valtuus Web Services -yhteyden käyttöön, ei minkään palvelun aineiston allekirjoitukseen. SOAP-sanoman allekirjoituksella varmistetaan ainoastaan, että aineiston toimittajalla on oikeus olla yhteydessä pankin eräsiirtopalveluun Web Services -yhteydellä ja lähettää asiakkaan allekirjoittamia ApplicationRequest-sanomia ja vastaanottaa käyttäjälle tarkoitettuja, pankissa allekirjoitettuja ApplicationResponse-sanomia.

Seuraava kuvio 1 esittää lähetettävän aineiston (Payload), allekirjoitettavan ApplicationRequest-sanoman ja pankkiin lähetettävän SOAP-sanoman välisiä suhteita. Jotta vältytään sisäkkäisten XML-rakenteiden välisiltä riippuvuussuhteilta, sanomat täytyy kuitenkin base64-koodata ennen kuin ne sijoitetaan kentän sisällöksi.



Kuvio 1. WS Sanoman rakenne

Yleensä asiakas toimii itse myös pankkiyhteysohjelmistonsa aineiston toimittajan roolissa, jolloin SOAP-sanoman voi allekirjoittaa käyttäen samaa PKI-avainta, jolla ApplicationRequest-sanoma allekirjoitettiin.

Kun käyttäjä pyytää aineistoa pankista, ei ApplicationRequestin Content-kenttään tule sisältöä. Tässäkin tapauksessa ApplicationRequest on allekirjoitettava samalla tavalla kuin lähetettäessä aineistoa pankkiin.

4.2 Varmenteiden mitätöinti

Jos asiakas epäilee yksityisen avaimensa joutuneen vääriin käsiin tai haluaa muista syistä mitätöidä varmenteen, varmenteen mitätöinnin jälkeen tarvittaessa tilattava uusi varmenne pankista.

Toimenpide on asiakkaan vastuulla ja edellyttää sopimuksen uusimista pankissa.

Sopimuksen lopettaminen sulkee varmenteen eikä sitä voi ottaa uudelleen käyttöön.

5 Web Services -yhteyden aineistot

5.1 Aineistot

Taulukossa 1. ovat lueteltuna maksuliikeaineistot, joita voidaan joko lähettää tai noutaa Web Services -yhteydellä:

Aineiston nimi	Aineistotyyppi	Selitys
SEPA-XML –tilisiirto (lähetys)	XL	pain.001.001.02 ja .03
SEPA-XML -virhepalaute (nouto)	XP	pain.002.001.02 ja .03
SEPA-XML – POPS pikasiirto (lähetys)	XF	pain.001.001.02 ja .03
SEPA-XML – SEPA pikasiirto (lähetys)	XI	pain.001.001.03
Saapuvat viitemaksut (nouto)	OP	
XML-viiteluettelo (nouto)	XE	camt.054.001.02
XML-maksuluettelo (nouto)	XM	camt.054.001.02
Tiliote (nouto)	TO	
XML-tiliote (nouto)	XT	camt.053.001.02
Konsernitiliote (nouto)	TK	
Konsernitiliote tapahtumilla (nouto)	TT	
Tilitapahtumakysely (nouto)	RA	
Verkkolaskujen lähetys (lähetys)	VL	
Verkkolaskujen nouto (nouto)	VN	
Verkkolaskun virheilmoituksen nouto (nouto)	VP	
Verkkolaskun virheilmoituksen lähetys (lähetys)	VT	
Laskuttajailmoituksen lähetys (lähetys)	VS	
E-laskuosoiteilmoituksen nouto (nouto)	VR	
Vastaanottoehdotuksen lähetys (lähetys)	VE	
Finvoice-liite (lähetys)	VA	
Finvoice-liite (nouto)	VB	
Valuuttakurssit (nouto)	WK	

Taulukko 1. Web Services kanavassa välitettävä aineisto ja niiden aineistotyypit

6 Yleiskuvaus siirtokäytännöstä

Web Services -yhteys on niin sanottu sessionless request-reply -sanomien välitystä. Web Services -yhteydessä asiakkaan tunnistetiedot seuraavat mukana jokaisessa yksittäisessä yhteydessä.

Tiedonsiirtoyhteys tapahtuu Web Services -standardiin perustuvalla tavalla; lähettämällä ja vastaanottamalla SOAP-määrityksen mukainen XML-rakenne (SOAP= Standardoitu WS -yhteyden

sanomamuoto). SOAP-sanomassa on header- ja body-osat, jotka allekirjoitetaan asiakkaan varmenteella ennen lähetystä.

Jokaisessa yhteydessä on mukana oma digitaalisesti allekirjoitettu ApplicationRequest-sanoma, jossa on haluttu toimenpidepyyntö (Command). ApplicationRequest on aina allekirjoitettu asiakkaan yksityisellä avaimella. ApplicationRequest sijoitetaan SOAP-sanoman body-osaan base64-koodattuna.

Toimenpidepyyntö (Command) on joko aineiston lähetys pankkiin (UploadFile) tai pyyntö noutaa aineisto (DownloadFile) pankista. Lisäksi on kaksi muuta pyyntöä:

- DownloadFileList, jolla saa listan noudettavissa olevista aineistoista
- DeleteFile, jolla saa asiakas voi poistaa lähettämänsä aineiston.

ApplicationRequest kohdistuu aina johonkin aineistotyyppiin. Kentässä Filetype on mainittava halutun aineiston tyyppi.

Pankki vastaa jokaiseen Request-sanomaan Response-sanomalla. ApplicationResponse-sanoma sisältää Upload-käyttötapauksessa kuittauksen, että aineisto on vastaanotettu tai hylätty. Eri palvelut tuottavat status- tai palautesanomia omien aikataulujensa mukaisesti. On huomattava, että lähetetty aineisto voidaan hylätä myöhemmin, esimerkiksi tilillä olevan katteen puuttumisen vuoksi.

Virheilmoitus tuotetaan SOAP fault -sanomalla esimerkiksi silloin kun ApplicationRequest-sanomaa tai allekirjoitusta ei ole voitu varmistaa

Vastaavasti Download request -pyyntöön vastataan palauttamalla pyydetty aineisto ApplicationResponse-sanomalla, sen Content-kentässä, base64-koodattuna. Jos pyydettyä aineistoa ei ole saatavilla, on Response-sanomalla asiaa selventävä virheilmoitus. Pankin vastauksessa on aina mukana ApplicationResponse-sanoma, jossa on vastaavia kenttiä kuin Request-sanomassa, mm. Content, jossa on vastaanotettava tiedosto.

ApplicationResponse-sanoma on aina digitaalisesti allekirjoitettu pankissa, joten asia-kas/asiakkaan ohjelmisto voi tarkistaa, että sanoma on tullut sovitulta osapuolelta ja ettei se ole muuttunut allekirjoituksen jälkeen.

ApplicationRequest-, ApplicationResponse- ja SOAP-sanomien rakenne on kuvattu tarkemmin englanninkielisessä dokumentissa Web Services Security and Communication Description, sekä muissa dokumenteissa, jotka ovat saatavilla Finanssialan Internet-sivuilla www.finanssiala.fi

6.1 Aineiston luonti ja lähetys pankkiin

Seuraavassa on esitetty tarvittavat vaiheet sanoman muodostamiseksi ja lähettämiseksi.

Pankkiyhteysohjelma suorittaa nämä toimet yleensä käyttäjän niitä näkemättä. Jos aineisto allekirjoitetaan ja lähetetään eri ohjelmistoilla, toteutetaan sanoman allekirjoitus kohtien 1–5 mukaisesti ja sanoman lähetys vastaavasti kohtien 6–8 mukaisesti.

Katso myös kuvaa 1 kohdassa 4.1 sanomien yhteydestä toisiinsa.

Aineiston allekirjoitus:

1. Luo maksuliikeaineisto (esim. SEPA-XML -aineisto) yrityksen järjestelmässä. Aineisto on muunnettava base64-koodauksella lähettämisen ajaksi. Aineistoa kutsutaan nimellä Payload.
2. Luo XML-rakenne nimeltään ApplicationRequest, jossa on mm. elementit Content ja Signature.
3. Sijoita Payload/aineisto ApplicationRequestin Content-elementtiin
4. Allekirjoita digitaalisesti koko ApplicationRequest käyttäen asiakaskohtaista varmennetta ja sen yksityistä avainta. Muunna allekirjoitettu sanoma base64-koodattuun muotoon.
5. Siirrä sanoma tietoliikenne-ohjelmalle tai tallennusmedialle.

Aineiston toimitus

6. Sijoita allekirjoitettu ja base64-koodattu ApplicationRequest uuden SOAP-sanoman body-osaan, sen ApplicationRequest-kenttään
7. Allekirjoita SOAP-sanoma digitaalisesti aineiston toimittajan varmenteen yksityisellä avaimella. Avain voi olla sama kuin edellä mainittu avain, jolla allekirjoitettiin ApplicationRequest-sanoma.
8. Lähetä SOAP-sanoma WS-protokollaa käyttäen ja odota pankista vastausta. Tarkista vastauksen allekirjoitus ja näytä ApplicationResponse-sanoman sisältö käyttäjälle.

Vastaus pankista noudattaa ApplicationResponse-sanomaa, joka on määritelty pankkien Web Services -kuvauksessa. Vastauksessa on tilakoodi, joka kertoo lähetyksen onnistuneen (= 0) tai virheestä (suurempi kuin 0).

6.2 Aineiston nouto pankista

Aineiston nouto tapahtuu pääosin kuten edellä, mutta koska lähetettävää aineistoa ei ole, jää Content-kenttä tyhjäksi (kohdat 1, 2 ja 4 jäävät pois). Kentän Command sisältönä on DownloadFile tai DownloadFileList.

Vastaus pankista noudattaa ApplicationResponse-sanomaa, joka on määritelty pankkien yhteisessä Web Services -kuvauksessa. Jos vastauksessa on pyydetty tiedosto, se on ApplicationResponse/Content-kentässä base64-koodattuna. ApplicationResponse-sanoma on aina allekirjoitettu pankissa, joten asiakas/asiakkaan ohjelmisto voi tarkistaa, että sanoma on tullut sovitulta osapuolelta.

6.3 Pankkiyhteysohjelmiston tekniset ohjeet

Samlinkin Web Services -yhteyskäytäntö on kuvattu tarkemmin ja yksityiskohtaisemmin erillisessä ohjeistossa. Tekniset ohjeet on tarkoitettu pääosin pankkiyhteysohjelmistoja tekevien yritysten käyttöön, jotta kaikkia palvelun piirteitä ja turvaominaisuuksia voitaisiin noudattaa tarkasti määritysten mukaan.

7 Pankkiyhteysohjelman Web Service – yhteystestaus

Pankkiyhteysohjelmiston yhteysasetukset on hyvä testata ennen ensimmäisen maksuaineiston lähetystä käyttäen erillistä Web Service –yhteyden erillistä testiominaisuutta.

Testaus tapahtuu pankkiyhteysohjelmiston avulla kuten varsinainenkin maksuaineiston lähetys, mutta ohjelmiston testitilassa. Tällöin pankkiyhteysohjelmisto asettaa ApplicationRequest-sanoman Environment-kenttään arvon TEST. Testiomainaisuudella lähetyt maksut eivät kirjaudu tilille.

Kun yhteysasetukset on todettu toimivaksi ja virheettömäksi, voi sitä käyttää pankin Web Services -yhteyksiin.

8 Aikataulut

Aineistoja voi lähettää ja noutaa ympäri vuorokauden viikon jokaisena päivänä. Pankkiin lähetettävien ja pankista noudettavien XML-aineistojen käsittely- ja valmistumisaikataulut löytyvät erillisestä palvelukuvauksesta.

Hyväksyttyjen aineistojen uusintalähetyksistä tai niiden poistoista on sovittava erikseen Yritysten maksuliikenneselvittelyn kanssa.

9 web services -yhteyden osoite

Oma Säästöpankit

Tiedostojen siirto: https://ws.samlink.fi/services/CorporateFileService

Varmennepalvelu: https://ws.samlink.fi/wsdl/CertificateService.xml

Yhteys on aina SSL-suojattu.

10 PKI –varmenteet ja niiden jakelu

Yhteyskäytännöstä sovittaessa asiakkaan yhteyshenkilölle luovutetaan kaksiosainen kertakäyttösalasana, jolla on oikeus lähettää varmennepyyntö pankin järjestelmään, ja noutaa allekirjoitetun varmenteen WS-yhteydellä. Asiakas saa varmenteen, jolla aineisto tai pyyntö (ApplicationRequest) allekirjoitetaan digitaalisesti ennen pankkiyhteyttä.

Varmennepyynnön voi toimittaa myös muulla tavalla pankkiin, mikäli asiakkaan sovellus ei tue toimintoa.

Varmentajan varmennekäytäntö on kuvattu erillisissä dokumenteissa:

- Samlink Customer CA varmenneperiaatteet WS-aineistopalvelut varmenteita varten
- Samlink Customer CA varmennuskäytäntö

Samlinkin neuvontanumerot

Kysymyksiinne testauksesta, aineistojen tarkistuksesta sekä konekielisten palveluiden käytöstä vastaa maksuliikennepalveluiden puhelinpalvelu numerossa 0100 4050 (1,17 eur + pvm) pankkipäivinä klo. 8.30–16.30.