Kundanvisning för OP Gruppens kanal Företagets bankförbindelse (Web Services)

Oktober 2024

Innehåll

1 Inledning

Web Services-kanalen (nedan WS-kanalen) är en elektronisk dataöverföringskanal för säker sändning och mottagning av bank- och försäkringsmaterial, meddelanden, order och uppdrag som OP Gruppen tillhandahåller sina företags- och organisationskunder.

Web Services är en teknisk lösning för uppkoppling av kommunikation mellan bankernas och privatkundernas tekniska anordningar, och den bygger på internationella standarder. Gränssnittsbeskrivningarna för WS-kanalen har utarbetats i samarbete mellan flera bankgrupper, och specifikationerna finns att få på Finans Finlands webbplats www.finanssiala.fi.

I den här anvisningen finns information om

- de funktioner som ska vara tillgängliga i den programvara som kunden använder.
- de förfaranden som anknyter till användningen av Web Service-kanalen och som inte beskrivs i bankernas gemensamma meddelandespecifikation.
- funktionerna och meddelandebeskrivningarna i Web Service-kanalen och Identifieringstjänsten.
- hur de certifikat som OP Gruppens Web Service kräver hämtas och används.
- I anvisningen finns också instruktioner för den som implementerar programvaran samt exempelmaterial och meddelanden som kan användas vid implementeringen. I anvisningen beskrivs inte betalningsmaterialens eller kontorapporteringens innehåll. Det finns separata, mer ingående beskrivningar om dem.

Vi rekommenderar att programvaruleverantörerna följer sidan Information till programvaruleverantörer i tjänsten op.fi på adressen https://www.op.fi/sv/foretagskunder/information-till-programvaruleverantorer. På sidan ges information om allmänna ärenden som gäller WS-kanalen. Information om eventuella störningar finns i Servicemeddelandet om Betalningsrörelse.

Banken och kunden ingår avtal om användning av WS-kanalen. Dessutom ska separat avtal ingås om de elektroniska tjänster som används via WS-kanalen.

1.1 Web Service-kanalens Identifieringstjänst

WS-kanalens Identifieringstjänst producerar och administrerar certifikat som används för kontroll av signaturer i WS-kanalen. Den administrerar och publicerar dessutom data om spärrade certifikat.

I WS-kanalen säkerställs integriteten och autenticiteten av meddelanden och tjänstebegäran med XML Digital Signature-teknik. För att mottagaren ska kunna lita på ett meddelande och en tjänstebegäran som mottagaren fått kontrollerar mottagaren deras signatur. Med hjälp av signaturen säkerställs att det undertecknade meddelandet eller tjänstebegäran inte har förändrats efter att det signerades.

De gällande certifikaten som används i WS-kanalen finns i tjänsten op.fi, Företagskunder > Betalning och fakturering, Bankförbindelse Web Services > Certifikatstjänsten (https://www.op.fi/sv/foretagskunder/betalningsrorelse-och-kassahantering/elektroniska-tjanster-for-foretag/foretagets-bankforbindelsekanal/certifikatet-tjanst).

1.2 Registrera certifikat samt överföringsnyckeln

På grund av de åtkomsträttigheter som anknyter till certifikatet ska kunden besöka banken för att identifiera sig, så att certifikatet kan tryggt kopplas till användarkoden för WS-kanalen. Denna första identifiering kan inte utföras elektroniskt.

En förutsättning för användning av WS-kanalen är att kundens programvara använder ett PKI-nyckelpar och ett certifikat som Identifieringstjänsten för WS-kanalen utfärdat.

När avtal tecknats om användning av WS-kanalen får kunden en överföringsnyckel för hämtning av certifikat. På WS-kanalens avtalshandling anges användarkoden för WS-kanalen (10 siffror) och överföringsnyckelns första del (åtta siffror). Överföringsnyckelns andra del (åtta siffror) får kunden efter eget val antingen som sms till sin mobiltelefon eller per post till den adress som kunden uppger.

När kunden har överföringsnyckelns båda delar (sammanlagt 16 siffror), ska kunden mata in överföringsnyckelns båda delar och användarkoden för WS-kanalen i sin programvara och starta processen för att bilda ett certifikat. Kundens programvara skickar en begäran om certifikat till Identifieringstjänsten och får kundcertifikatet i svarsmeddelandet.

1.3 Skapa nyckelpar

Kunden ansvarar för att skapa det nyckelpar som används i WS-kanalen. Banken deltar inte i förfarandet för att skapa nyckelparet och behandlar inte heller kundens nyckelpar.

Kundens programvara skapar nyckelparet med hjälp av ett program för detta ändamål. Programmet som skapar nyckelparet ska se till att algoritmen som används för att skapa nyckelparet är tillräckligt högklassigt och förenligt med kryptografiska förfaranden. Nyckelparet ska skapas med en algoritm och metod som garantera tillräcklig slumpmässighet. Nyckelns längd ska vara 2048 bit och algoritmen ska vara RSA. Signaturens hashalgoritm är sha256RSA.

1.4 Använda nyckel och certifikat

I WS-kanalen signeras både tjänstebegäran (ApplicationRequest) och SOAP-meddelandet separat.

Kundens programvara använder kundens privata nyckel (nyckelparets privata del) för att signera meddelanden och tjänstebegäran elektroniskt i WS-kanalen.

Det signerande systemet ska lägga certifikatet som motsvarar den privata nyckeln till signaturen. Certifikatet innehåller den publika nyckeln med vilken mottagaren kontrollerar signaturen. Den som innehar den privata nyckeln kan genom WS-kanalen sända tjänstebegäran och material till banken, och banken genomför dem åt den kund som kopplats till den privata nyckeln med hjälp av certifikatet.

Certifikatet kopplar den publika nyckeln och genom den hela nyckelparet till innehavaren. I WS-kanalens certifikat finns uppgiften CommonName (CN) på certifikatets ämnesrad. Den anger innehavarens användarkod för WS-kanalen och fungerar som användarens identifikation.

Kunden ansvarar för att förvara den privata – dvs. den hemliga – nyckeln säkert och för att kontrollera dess användning. Den privata nyckeln ska inte förvaras okrypterad och kunden får inte tillåta att den används utan tillräcklig identifiering.

1.5 Certifikatets livslängd och förfarandet för att förnya certifikat

Ett kundcertifikat gäller i högst två år och certifikatet ska förnyas innan det går ut. Kunden ansvarar för att förnya certifikatet i god tid. Kundens programvara förnyar certifikatet automatiskt, och programvaran kan kontrollera certifikatets utgångsdatum varje gång som certifikatet används.

Ett gällande certifikat kan förnyas tidigast 60 kalenderdagar innan certifikatet går ut. Om certifikatet går ut innan ett nytt certifikat har hämtats, ska kunden hämta nya överföringsnycklar från banken.

Därefter ska kunden skapa ett nytt nyckelpar för det nya certifikatet. Om kundens programvara gör en begäran om certifikat som gäller samma nyckelpar som det certifikat som redan är i användning, bildar bankens Identifieringstjänst inte ett nytt certifikat utan returnerar en kopia av det certifikat som bildats tidigare.

Hämtning av ett nytt certifikat medan det föregående certifikatet är aktivt (inom fristen för förnyelse om 60 dagar) förutsätter att nya publika och privata nycklar samt en CSR-begäran (Certificate Signing Request) skapas. Om en ny CSR skapas med samma nycklar, fungerar den fortfarande som ursprunglig, och en kopia av det förra certifikatet är åter i användning. Av säkerhetsskäl ska nya nycklar användas.

Begäran om förnyelse av ett certifikat är likadan som ansökan om ett nytt certifikat, men vid förnyelse används inte överföringsnyckeln (CertApplicationRequest.TransferKey). I stället signeras CertApplicationRequest med en privat nyckel till vilken användarkoden har ett gällande certifikat. Kontrollen av begäran om förnyelse i bankens Identifieringstjänst bygger på användarkodens föregående certifikat, som ska vara i kraft när begäran görs.

1.6 Göra begäran om certifikat och skapa certifikat

När kundens programvara sänder en begäran om certifikat ska den kontrollera SSL-certifikatet för bankens Identifieringstjänst som bildats för domänen wsk.op.fi. Med denna kontroll säkerställer programvaran att begäran om certifikat går till bankens tjänst.

Om den publika nyckeln ska bildas en begäran om certifikat av pkcs10-format.

På ämnesraden för begäran om certifikat ska endast finnas dessa två uppgifter:

- C=FI
- CN= [användarkoden för WS-kanalen, 10 siffror]

När det är fråga om användarkodens första certifikat (första begäran om certifikat som görs utan certifikat), bygger den på den registrering som gjorts i banken, dvs. på överföringsnyckeln. Då ska den 16-siffriga överföringsnyckeln finnas i elementet CertApplicationRequest.TransferKey och den 10 siffror långa användarkoden för WS-kanalen i elementet CertApplicationRequest.CustomerId. Överföringsnyckelns sista siffra är ett kontrollnummer med hjälp av vilken kundens programvara kan säkerställa att överföringsnyckeln matats in rätt. Kontrollnumret har kalkylerats med algoritmen Luhn modulo 10. CertApplicationRequest och SOAP-meddelandet behöver inte vara signerade.

Vid förnyelse av ett gällande certifikat (begäran om certifikat bygger på det tidigare certifikatet) ska CertApplicationRequest signeras med en nyckel som motsvarar det certifikat som används av det användarnamn till vilket nya certifikatet hämtas. Den 10-siffriga användarkoden för WS-kanalen ska finnas i elementet CertApplicationRequest.CustomerId. SOAP-meddelandet behöver inte vara signerat.

Om kundens programvara hämtar ett certifikat med serienummer, ska certifikatets serienummer finnas i elementet CertApplicationRequest.SerialNumber. CertApplicationRequest och SOAP-meddelandet behöver inte vara signerade.

Om den publika nyckeln som finns i begäran om certifikat är samma nyckel som redan finns i något tidigare certifikat för samma användarnamn, returnerar bankens svarsmeddelande det tidigare certifikatet som motsvarar den publika nyckeln även om certifikatet redan gått ut. Inget felmeddelande sänds om detta, utan det begärande programmet ska observera att det fick en kopia av det gamla certifikatet och att inget nytt certifikat bildades.

1.7 Spärra certifikat, hämta och använda data om spärrat certifikat

Om en kund misstänker eller vet att kundens privata nyckel kommit i fel händer, ska kunden spärra certifikatet omedelbart.

Kunden kan spärra sitt certifikat genom att ringa telefonnumret 010 252 8470. För att kunna spärra ett certifikat behövs den 10-siffriga användarkoden för WS-kanalen eller serienumret för det certifikat som ska spärras. När kunden spärrat certifikatet, godkänner banken inte en signatur som gjorts med den hemliga nyckeln som motsvarar certifikatet i fråga.

Banken uppdaterar och publicerar en spärrlista över certifikat. Spärrlistan (CRL, Certificate Revocation List) innehåller serienumren för certifikat som tagits ur bruk samt en orsakskod.

Identifieringstjänsten bildar en spärrlista minst en gång per dygn, och listan gäller i tre dygn. Identifieringstjänsten bildar en ny spärrlista också när ett certifikat spärras.

Spärrlistans adress finns i fältet CRL Distribution Points i anslutning till betrodda certifikat. Kundens system ska hämta spärrlistan från Identifieringstjänsten och kontrollera att de certifikat som är betrodda i systemet (CA-certifikatet och bankens tjänstecertifikat) är i kraft. I praktiken gäller det att kontrollera bankens tjänstecertifikat som finns i bankens svarsmeddelanden mot spärrlistan.

Ett spärrat certifikat kan inte tas i användning igen. Om kunden börjar använda ett nytt certifikat efter att ett certifikat spärrats, ska kunden registrera sig på nytt på bankens kontor och göra en ny begäran om certifikat via WS-kanalen med en ny överföringsnyckel.

1.8 Termer

Begäran om certifikat	En elektronisk handling som kundens datasystem sänder till WS-kanalen. Begäran om certifikat innehåller kundens publika nyckel och kundens identifieringskod. Bankens Identifieringstjänst bildar ett certifikat i enlighet med begäran om certifikat och ger den till kundens datasystem i svarsmeddelandet.
Certifikat	Ett certifikat är en elektronisk handling som kopplar en publik nyckel och nyckelns innehavare till varandra. Certifikatet har signerats av en certifierare. Certifierarens signatur bekräftar att uppgifterna är riktiga och säkerställer samtidigt certifikatets integritet.
PKI	Public Key Infrastucture. En helhet som används för att bilda, administrera, dela, använda, lagra och avlägsna Certifikat för Publika nycklar. PKI specificerar de kontroller och standarder som Certifierare ska använda i sin verksamhet för att säkerställa de elektroniska certifikatens kompatibilitet, identifierbarhet och tillgänglighet. PKI bygger på den publika nyckelns krypteringsalgoritm.
Privat nyckel	Nyckelparets privata del och används för asymmetrisk kryptering i PKI-system. Den privata nyckeln har entydigt utfärdats för en bestämd aktör. Data som krypterats med en publik nyckel kan låsas upp med nyckelparets privata nyckel.

Publik nyckel	Den publika delen av ett nyckelpar som används för asymmetrisk kryptering i system med publika nycklar. Data som krypterats med en publik nyckel kan låsas upp endast med Nyckelparets privata nyckel. När den Publika nyckelns innehavare är känd, är det möjligt att kontrollera en elektronisk signatur som gjorts med den privata nyckeln som motsvarar den publika nyckeln. Den publika nyckelns innehavare kan identifieras pålitligt med ett Certifikat. Publika nycklar används för att auktorisera signaturer och utföra kryptering.
Transport Layer Security	TLS, Transport Layer Security, är ett krypteringsprotokoll som används för att skydda autenticiteten av data och överföringen av data mellan två applikationer.
XML-signatur	En teknisk lösning som säkerställer autenticiteten och integriteten av en XML-handling. Signaturen görs med en privat nyckel och kontrolleras med en Publik nyckel.
Överföringsnyckel	Autenticiteten av en begäran om certifikat kontrolleras med hjälp av överföringsnyckeln som det datasystem som sänder begäran om certifikat fogar till begäran.

2 Krypteringsalgoritmer

Kunden ska använda de krypteringsalgoritmer som anges nedan. I dem ingår hashfunktioner, elektroniska signaturalgoritmer och krypteringsalgoritmer.

Krypteringsalgoritmerna och -protokollen skyddar konfidentiell, oklassificerad information.

Krypteringsprogrammet krypterar data som ska flyttas och låser upp dess kryptering. OP stöder TLS version 1.2 eller senare för kryptering av dataöverföring och låsa upp kryptering. WS-kanalen stöder endast TLS version 1.2 eller senare som protokoll. Det är inte möjligt att sända material till OP med de gamla versionerna TLS 1.0 OCH TLS 1.1.

OP rekommenderar att kunderna använder minst algoritmen SHA256.

OP:s WS-kanal stöder för närvarande de följande krypteringsalgoritmerna:

- 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_

Algoritmerna går under namnet SHA-2 och de har namngetts enligt deras hashvärden i bits: SHA-256, SHA-384 och SHA-512.

3 Web Services-kanalens funktioner

Förbindelsemetoden i WS-kanalen är i första hand SSL-krypterad https över allmänt Internet. Enheten som sänds i kanalen är ett SOAP-meddelande med elektronisk signatur. Meddelandet innehåller en ApplicationRequest-begäran som gäller en XML-handling och är den egentliga tjänstebegäran. ApplicationRequest innehåller det affärsverksamhetsmaterial som anknyter till tjänsten (till exempel betalningsmaterial), och denna begäran är elektroniskt signerad.

Kundens datasystem sänder tjänstebegäran och får genast svar från WS-kanalen. Det sända materialet blir kvar i banken i väntan på behandling. Om behandlingen kan bildas ett returmaterial som kundens datasystem ska hämta separat.

I realtidstjänster laddar kundens programvara materialet upp hos banken och får omedelbart realtidstjänstens slutliga svar i svarsmeddelandet.

3.1 Sända material till banken

WS-kanalen kontrollerar att det sända materialet har rätt format genast i samband med sändningen och avvisar materialet om det inte är formellt riktigt. Då ger WS-kanalen omedelbart ett avvisande svar till den sändande programvaran. Svaret innehåller felkoden 12 och förklaringen Schema validation failed.

Det är endast möjligt att skicka ett material i taget, dvs. ett material per meddelande.

3.2 Hämta material från banken

Då material hämtas gäller det att exakt definiera vilket material som ska hämtas. Detta görs med materialets identifikation (FileReference). Materialens identifikationer framgår efter att man kört en lista på materialen. Efter det är det möjligt att hämta material som finns på listan med hjälp av materialets identifikation.

Det är endast möjligt att hämta ett material i taget.

WS-kanalen förvarar material tre månader och tar därefter bort dem automatiskt. Kunden behöver inte ta bort materialen själv.

Även om kunden redan hämtat ett material är det möjligt att hämta materialet på nytt. Status för hämtat material ändras från NEW till DLD, men själva materialet förblir synligt och kan hämtas.

3.3 Komprimera material

Vi rekommenderar att material som sänds till banken alltid komprimeras. Komprimeringsalgoritmen är GZIP enligt RFC1952. Komprimering utförs på det ursprungliga materialet före base64-enkodning och skrivning i elementet ApplicationRequest.Content. Elementet ApplicationRequest.Compression ska ha värdet 'true' när materialet är komprimerat.

Vi rekommenderar att komprimering begärs också i samband med att material hämtas. Genom att ställa in värdet ApplicationRequest.Compression = 'true' i hämtningsbegäran erhålls materialet komprimerat från banken.

3.4 Realtidstjänster

För närvarande tillhandahålls följande realtidstjänster i WS-kanalen

Tjänstens tekniska namn/FileType	Beskrivning
CustomerCreditTransferInitiantionV02 pain.001.001.02.xsd	C2B SEPA-expressbetalning
CustomerCreditTransferInitiantionV03 pain.001.001.03.xsd	C2B SEPA-expressbetalning
pain.001.001.02 TP4 PS01 och pain.001.001.03 TP4 PS01	C2B SEPA-expressbetalning
pain.001.001.02 TP4 PS01	POPS-expressbetalning, schema-version V02. Svarsmeddelande pain.002.001.02 TP4 PS01.

pain.001.001.03 TP4 PS01	POPS-expressbetalning, schema-version V03. Svarsmeddelande pain.002.001.03 TP4 PS01.
TP4 PS01	POPS-expressbetalning
TP1 ES	Girering mellan egna konton
TP1 1SS	Kontots saldoförfrågan
TP1 1VA	Saldosammanfattning av valutakonton
TP1 2ST	Kontotransaktionsförfrågan
TP1 2SY	Utvidgat saldosammandrag för konton
TP1 2KS	Koncernkontots saldo, uttag och insättningar-förfrågan
TP1 3ST	Kontotransaktionsutdragsförfrågan (Ohämtade transaktionsutdrag över kontotransaktionerna innevarande dag)
ORDER TU	Beställa upprepningskontoutdrag

Realtidstjänsterna fungerar med operationen UploadFile. Begäran laddas upp i WS-kanalen i elementet ApplicationRequest.Content, och ApplicationRequest.FileType är realtidstjänstens tekniska namn/File type, t.ex. "TP1 1SS".

3.4.1.1 C2B SEPA-expressbetalning som realtidstjänst

Tjänstens tekniska namn/FileType är TP4 PS01.

CustomerCreditTransferInitiantionV02 pain.001.001.02.xsd eller CustomerCreditTransferInitiantionV03 pain.001.001.03.xsd. Det är möjligt att göra en enskild SEPA-expressbetalning i realtid med tjänsten.

En enskild SEPA-expressbetalning i realtid kan göras i banker som är verksamma i Finland eller på annat håll i SEPA-området och till leverantörer av betalningstjänster som använder SEPA-expressbetalningstjänsten.

SEPA-expressbetalningar som skickas som separata expressbetalningstyper (pain.001.001.02 TP4 PS01 eller pain.001.001.03 TP4 PS01) behandlas omedelbart och avsändaren får ett omedelbart online-svarsmeddelande genast under överföringsförbindelsen (material som inte kan hämtas). Enskilda SEPA-expressbetalningar har ingen förfallodagsbehandling och de kan sändas 24/7/365. Separata realtidsbetalningar förmedlas aldrig till POPS-systemet, utan de behandlas alltid som SEPA-expressbetalningar. Om mottagarens bank inte kan behandla SEPA-expressbetalningar, avvisas betalningen.

3.4.2 Expressbetalning (POPS)

Det tekniska namnet/FileType för tjänsten för realtidsbetalning till ett annat finansinstitut är TP4 PS01.

Bankförbindelseprogrammet lägger en base64-enkodad begäran av följande form i elementet ApplicationRequest.Content:

Uppgiftens namn	Längd	Förklaring
Styrkommando	11	"$$TP4 PS01 "
Betalarens kontor	6	5nnnnn
Betalarens kontonummer	8	
Betalarens namn	30	
Mottagarens kontor	6	
Mottagarens kontonummer	8	
Mottagarens namn	30	

Penningbelopp som överförs	14	i cent, se nedan
Myntenhetskod	1	1 euro
Förfallodag	10	dd.mm., tills vidare tomt
Referens	20	Infogade inledande nollor
Meddelande	140	
Papperskvitto till betalaren	1	"E", inga kvitton tills vidare
Avisering till mottagaren	1	0 ingen avisering 1 telefon 2 fax 9 annan
Mottagarens kontaktinformation	70	Mottagarens kontaktinformation när mottagaren aviseras, annars tomt
Tidsstämpel	15	Ååmmddttmmnnn, individuell
Meddelandeversion	1	”1”
Användarnyckelns generation	1	0 ... 9
Kontrolltal	16	används inte, ska fyllas i med nollor

Exempel på begäran om expressbetalning. Mellanslag har ersatts med punkter, så att deras antal och läge syns. Ett riktigt meddelande med begäran ska ha mellanslag.

```
$$TP4.PS01.57803820021333Saku.Eeroila.....13934600001181Simo.Sammila.....0
0000000000001127.11.201100000000000000001245.....
.....E0.....110727145700000
100000000000000000
```

Expressbetalningskvittering för mottagning

En expressbetalningskvittering är en fil med två poster: en kvitteringspost och en avslutningspost för OP:s transaktion ($$EOF). Expresskvitteringen kan också vara endast ett $$ERROR-felmeddelande från OP:s tjänst, t.ex. PERMISSION ERROR eller NO RESPONSE FROM HOST. I fråga om expressbetalning ska bankförbindelseprogrammet förbereda sig på en längre svarstid än normalt: cirka 120 sekunder (det är möjligt att transaktionen behandlas vid ett annat finansinstitut). Om en kvittering inte erhålls från OP:s tjänst eller om den är ett $$ERROR - NO RESPONSE FROM HOST-felmeddelande, ska bankförbindelseprogrammet be att användaren kontaktar sin egen bank eller kontrollerar t.ex. med en transaktionsförfrågan om expressbetalningen lyckades. Om det finns en transaktion som motsvarar expressbetalningen på kontot, har expressbetalningen lyckats.

Ett MAC-kontrollnummer har kalkylerats för kvitteringsposten i enlighet med standarden PATU. Kontrollnumret kalkyleras med användarnyckeln från kvitteringspostens början till kontrollnummerfältet på samma sätt som i fråga om andra PATU-standarder (ESI, SUO, VAR och PTE).

Uppgiftens namn	Längd	Förklaring
Kod för genomförande	2	"00" Lyckades Andra siffervärden är fel, och då anger den förklarande texten orsaken, t.ex. om betalningen är avvisad på grund av brist på täckning ("HYLÄTTY, KATE El RIITÄ").
Förklarande text	80	Förklarande text, på kundens språk
Arkiveringskod	22	Om lyckades, i annat fall tomt
Tidsstämpel	15	Ååmmddttmmssnnn
Meddelandeversion	1	”1”
Användarnyckelns generation	1	0 ... 9
Kontrolltal	16	Används inte, nollor

3.4.3 Realtidsbetalning – girering mellan egna konton

Det tekniska namnet/File type för tjänsten Girering mellan egna konton är TP1 ES.

Bankförbindelseprogrammet lägger en base64-enkodad begäran av följande form i elementet ApplicationRequest.Content:

$$TP1 ES X vknro vtnro hknro htnro eurobelopp meddelande

där

- X är tecknet X
- vknro veloitettava konttorinumero (kontorsnummer som debiteras), längd 6 tecken
- vtnro veloitettava tilinumero (kontonummer som debiteras) 8 tecken
- hknro hyvitettävä konttorinumero (kontorsnummer som krediteras), 6 tecken
- htnro hyvitettävä tilinumero (kontonummer som krediteras), 8 tecken
- eurobelopp, penningbelopp som överförs inkl. cent, utan decimaltecken, max. 11 tecken
- meddelande max. längd 70 tecken, mellan citattecken

Exempel: överföring av 1500 euro från konto 500015-118 till konto 500015-22228 med meddelandet Modellgirering

- $$TP1 ES X 500015 10000018 500015 20002228 150000 "Girering"

Svarsmeddelande på girering

Uppgiftens namn	Längd	Förklaring
Postens ordningsnummer	1	1
Svarstyp	1	1=OK, annat=fel*
Reserv	3	
Transaktionskontor	6	
Terminalnummer	2	
Transaktionsnummer	4	
Kontohavarens namn	15	
Datum	6	ddmmåå
Debiterat kontorsnummer	6	
Debiterat kontonummer	8	
Det debiterade kontorets saldo	11	inkl. cent, utan decimaltecken
Saldots förtecken	1	+/-
Krediterat kontorsnummer	6	
Krediterat kontonummer	8	
Reserv	12	
Girerat eurobelopp	11	inkl. cent, utan decimaltecken
Förtecken	1	+
Myntenhetens kod	1	1=euro

3.4.4 Saldoförfrågan

Det tekniska namnet/FileType för tjänsten Saldoförfrågan är TP1 1SS.

Bankförbindelseprogrammet lägger en base64-enkodad begäran av följande form i elementet ApplicationRequest.Content:

$$TP1 1SS kontorsnummer kontonummer X

- kontorsnummer, 6 tecken
- kontonummer, 8 tecken
- X är tecknet X.

Svaret på saldoförfrågan finns i elementet ApplicationResponse.Content och har följande struktur.

Uppgiftens namn	Längd	Förklaring
Postens ordningsnummer	1	=1
Svarstyp	1	1=OK, annat=fel*
Reserv	3	
Transaktionskontorets nummer	6	
Terminalnummer	2	
Transaktionsnummer	4	
Kontohavarens namn	15	
Kontorsnummer	6	
Kontonummer	8	
Datum	6	ddmmåå
Saldo	11	2 dec,
Saldots förtecken	1	+/-
Kreditgräns	11	2 dec,
Kreditgränsens förtecken	1	+/-
Disponibelt belopp	11	2 dec,
Det disponibla beloppets förtecken	1	+/-
Myntenhetens kod	1	1=euro

3.4.5 Saldosammanfattning av valutakonton

Det tekniska namnet/FileType för tjänsten Saldosammandrag för valutakonton är TP1 1VA.

Bankförbindelseprogrammet kan begära ett saldosammandrag för valutakonton med styrmeddelandet

$$TP1 1VA X kontoform valutakod

där

- X är tecknet X
- kontoformen är AV-KP (=OP-valutakonto), MTA (=tidsbestämt OP-valutakonto) eller ALL (=alla valutakonton)
- valutakoden är valutans ISO-kod (t.ex. USD) eller ALL (=alla valutor)

Saldosammandragets svarsdel består av en eller flera poster. Myntenhetens kod finns endast i den sista posten.

Uppgiftens namn	Längd	Förklaring
Kundens namn	15	
Antalet konton i denna post	3	
Kommer det fler saldoposter	1	0=nej, 1=ja
Konto (0-n st.)		
Kontorsnummer	6	
Kontonummer	8	
Kontoform	5	
Valutakod	3	
Ränta, %	6	4 dec.
Saldon (3 st.)		
Valutabelopp	13	2 dec,

Förtecken	1	+/-
Registreringsdag	6	ddmmåå
Motvärde	13	2 dec,
Förtecken	1	+/-
Mittkurs	10	7 dec.
Antal belopp	2	
Summor (0-n st.)		
Totalt euro	15	
Förtecken	1	+/-
Registreringsdag	6	ddmmåå
Myntenhetens kod	1	1=euro Detta fält finns med endast i den sista posten.

Fältet Fler konton (Tilejä lisää) får värdet 1, om det finns fler kontoposter i meddelandet. I posten finns uppgifter om högst tre konton. Sammandragen över konton presenteras per post; i den sista posten anges således inte hela meddelandets sammanlagda saldon, utan de ska räknas separat från varje post.

I varje kontopost finns tre saldon, i vilka presenteras de kommande registreringsdagarnas eventuella saldon. I fältet för registreringsdatum som gäller ett saldo som saknas finns nollor.

3.4.6 Kontotransaktionsförfrågan

Det tekniska namnet/FileType för tjänsten Kontotransaktionsförfrågan är TP1 2ST.

Bankförbindelseprogrammet kan fråga efter kontots transaktioner med styrmeddelandet

$$TP1 2ST kontorsnummer kontonummer X

där

- kontorsnummer, 6 tecken
- kontonummer, 8 tecken
- X är tecknet X.

Transaktionsförfrågan, svarsdel

Uppgiftens namn	Längd	Förklaring
Postens ordningsnummer	1	=1
Svarstyp	1	1=OK, annat=fel
Reserv	3	
Transaktionskontor	6	
Terminalnummer	2	
Transaktionsnummer	4	
Kontohavarens namn	15	
Kontorsnummer	6	
Kontonummer	8	
Datum	6	ddmmåå
Transaktioner (10 st.)		
Transaktionsdag	6	ddmmåå
Förklaring	12	
Penningbelopp	11	2 dec,
Förtecken	1	+/-
Saldo	11	2 dec,
Förtecken	1	+/-
Kreditgräns	11	2 dec,
Förtecken	1	+/-

Täckningsreserveringar	11	2 dec,
Förtecken	1	+/-
Disponibelt belopp	11	2 dec,
Förtecken	1	+/-
Myntenhetens kod	1	1=euro

3.4.7 Utvidgat saldosammandrag för konton

Det tekniska namnet/FileType för tjänsten Utvidgat saldosammandrag för konton är TP1 2SY.

Bankförbindelseprogrammet kan fråga efter ett utvidgat saldosammandrag för konton med styrmeddelande

$$TP1 2SY

Saldosammandragets svarsdel består av en eller flera poster.

Uppgiftens namn	Längd	Förklaring
Kundens namn	40	
Antalet konton i denna post	3	
Kommer det fler saldoposter	1	0=nej, 1=ja
Konto och saldo (0-n st.)		
Kontorsnummer	6	
Kontonummer	8	
Saldo	13	11 heltal + 2 dec.
Förtecken	1	+/-
Disponibelt belopp	13	11 heltal + 2 dec.
Förtecken	1	+/-
Räntesats	6	4 dec.
Saldots datum	8	ååååmmdd

Meddelandets postlängd varierar.

3.4.8 Koncernkontoförfrågan

Det tekniska namnet/FileType för tjänsten Koncernkontots saldo, uttag och insättningar är TP1 2KS.

Bankförbindelseprogrammet lägger en base64-enkodad begäran av följande form i elementet ApplicationRequest.Content:

$$TP1 2KS kontorsnummer kontonummer X

där

- kontorsnummer, 6 tecken
- kontonummer, 8 tecken
- X är tecknet X.

Koncernkontoförfrågan, svarsdel

Uppgiftens namn	Längd	Förklaring
Postens ordningsnummer	1	1
Svarstyp	1	1=OK, annat=fel*
Reserv	3	
Transaktionskontor	6	
Terminalnummer	2	
Transaktionsnummer	4	

Kontoinnehavarens namn	15	
Koncernkontorsnummer	6	
Koncernkontonummer	8	
Datum	6	ddmmåå
Saldo	13	2 dec,
Förtecken	1	+/-
Dagens uttag	13	2 dec,
Förtecken	1	+/-
Dagens insättningar	13	2 dec,
Förtecken	1	+/-
Myntenhetens kod	1	1=euro

3.4.9 Transaktionsutdragsförfrågan

Det tekniska namnet/FileType för tjänsten Kontots ohämtade kontoutdragstransaktioner för innevarande dag är TP1 3ST.

Bankförbindelseprogrammet lägger till en base64-enkodad begäran av följande form i elementet ApplicationRequest.Content:

$$TP1 3ST kontorsnummer kontonummer X

där

- kontorsnummer, 6 tecken
- kontonummer, 8 tecken
- X är tecknet 1 om man på nytt vill ha alla transaktioner från dagens början. I annat fall returneras endast nya kontotransaktioner som ännu inte hämtats med samma användarkod (CustomerId) för WS-kanalen.

Beskrivning av posterna i svarsmeddelandet
Posterna avgränsas från varandra med postavgränsare. Varje post slutar med carriage return- och line feed-tecken.

Baspost, transaktionsutdrag

Fält	Uppgiftens namn	Form	Beskrivning
1	Materialkod	AN1	S
2	Postkod	AN2	00
3	Postens längd	N3	322
4	Versionsnummer	AN3	001
5	Kontonummer	AN14	
6	Transaktionsutdragets nr	AN3	Tomt
7	Datum för förfrågan		
	.1 Startdag	N6	ÅÅMMDD
	.2 Slutdag	N6	ÅÅMMDD
8	Tidpunkt för bildande		
	.1 Innevarande dag	N6	ÅÅMMDD
	.2 Klockslag	N4	HHMM
9	Kundkod	AN17	
10	Används inte	N6	
11	Används inte	AN19	
12	Används inte	N6	
13	Kod för kontots valuta	AN3	ISO-kod
14	Kontots namn	AN30	
15	Kontots limit	AN18	16 heltal + 2 dec.
16	Kontohavarens namn	AN35	

17	Bankens namn	AN40	
18	Används inte	AN40	
19	Används inte	AN30	
20	Används inte	AN30	
	TOTALT	322	

Fält 4 anger versionen av det program som använts för att bilda transaktionsutdraget.

Fält 7 Startdatum och slutdatum är samma datum, dvs. datum för förfrågan.

Fält 9 anger bankens kundkod används för kontohavaren och dess eventuella kontrollnummer (i det inledande skedet är landskoden eller standarduppgiften och specifikationen tomma).

- landskod X(4) eller .1 standard X(4)
- kundkod X(8) .2 kundkod X(10)
- kundspecifikation X(5) .3 kundspecifikation X(3)

Fält 15 I fältet finns kontots limit på ett checkkonto med kredit. Kontot har ingen limit om fältet innehåller nollor. I fråga om koncernkontotjänstens enhetskonto förmedlas kontots interna limit i fältet.

Baspost, transaktion

Fält	Uppgiftens namn	Form	Beskrivning
1	Materialkod	AN1	S
2	Postkod	AN2	10
3	Postens längd	N3	188
4	Klockslag, transaktionens uppkomsttid	N6	HHMMSS
5	Urspr. arkiveringskod	AN18	
6	Registreringsdag	N6	ÅÅMMDD
7	Valuteringsdag	N6	ÅÅMMDD
8	Betalningsdag	N6	ÅÅMMDD
9	Transaktionskod	AN1	1, 2, 3, 4
10	Registreringsspecifikation .1 Kod .2 Förklarande text	 AN3 AN35	
11	Transaktionens belopp .1 Förtecken .2 Belopp	 AN1 N18	 16 heltal + 2 dec.
12	Kvittokod	AN1	E = Specifikationerna kommer inte på transaktionsutdraget
13	Förmedlingssätt	AN1	
14	Mottagare/Betalare .1 Namn .2 Namnkälla	 AN35 AN1	 tomt, A, J eller K
15	Mottagarens konto .1 Kontonummer .2 Ändrat konto	 AN14 AN1	 tomt tecken, *
16	Referens	AN20	
17	Formulärets namn	AN8	
18	Nivåkod	AN1	0
	TOTALT	188	

Fält 5 I fältet anges arkivkoden som banken som bildat transaktionen gett. Med arkivkoden är det möjligt att spåra det ursprungliga betalningsuppdraget.

Arkiveringskoden anger på vilken dag banken behandlat betalningsuppdraget och vilken banks kontor eller system behandlat transaktionen.

ÅÅMMDD XXXXXXXXXXX
^_____identifieringsuppgift
^_____ datum

Arkiveringskodens identifieringsuppgift är bankspecifik. De första tecknen i koden består av bankgruppens kod.

Fält 9 I fält 9 finns en transaktionskod, vars värden är:

- 1 = insättning
- 2 = uttag
- 3 = korrigering av insättning
- 4 = korrigering av uttag

Obs. Korrigeringar av korrigeringar ges transaktionskoden 1 (insättning) eller 2 (uttag).

Fält 10 Registreringsspecifikationen i fält 10 anger genom vilken tjänst eller hur transaktionen registrerats i kontobanken. Det främsta syftet med koden i registreringsspecifikationen är att göra det möjligt för kunderna att automatiskt kontera kontotransaktionerna i sin bokföring. Transaktioner som ska konteras automatiskt har getts specificerande koder. De övriga transaktionerna ges allmänna koder. Alla banker har samma värden för koderna, men de förklarande texterna är bankspecifika. Vid korrigeringar används koderna för både insättnings- och uttagstransaktioner.

Registreringsspecifikationens kod har följande värden:

- 700 = betalningstjänster insättning/uttag
- 701 = tjänsten för periodiska betalningar insättning/uttag
- 702 = fakturabetalningstjänst uttag
- 703 = betalterminaltjänst insättning
- 704 = direktdebiteringstjänst/automatisk betalningstjänst insättning/uttag
- 705 = referensbetalningstjänst insättning
- 706 = betalningstjänst uttag
- 710 = insättning
- 720 = uttag
- 721 = kortbetalning uttag
- 722 = check uttag
- 723 = taxibussedel uttag
- 730 = provision uttag
- 740 = räntedebitering uttag
- 750 = räntegottgörelse insättning
- 760 = lån (inkl. amortering, ränta och provision) uttag
- 761 = amortering av lån uttag

Fält 12 I fältet finns en kvittokod som anger huruvida verifikatuppgifterna finns på kontoutdraget eller om transaktionen också förknippas med ett separat papperskvitto eller en specifikation av de enskilda transaktionerna i maskinläsbart format.

Kvittokoden har följande värden:

- tomt = Banken ger inte kunden ett papperskvitto på transaktionen.
- E = Transaktionen har en specifikation.
- P = Banken ger kunden ett papperskvitto på transaktionen.

Fält 13 I fält 13 finns förmedlingssättskod som den bank som tagit emot betalningsuppdraget ger. Denna kod anger hur betalningsuppdraget förmedlats till banken och var det ursprungliga betalningsuppdraget finns. Vid utredning används förmedlingssättet för att ta reda på vilken instans som ska kontaktas, om det behövs mer information om transaktionen. Då förmedlingssättet har värdet A riktas begäran om utredning alltid direkt till uppdragsgivaren. I annat fall ska kontokontoret kontaktas.

Förmedlingssättskoden har följande värden:

- A = Kunden har sänt betalningen i maskinläsbart format eller betalat den som självtjänst. Det ursprungliga betalningsuppdraget finns hos kunden.
- J = Transaktionen har bildats i bankens system. Grunderna för dess uppkomst kan utredas på utredningsstället för det system som arkiveringssystemet anger.
- K = Transaktionen har bildats på bankens kontor när en tjänsteman registrerat den. Betalningsuppdraget går att söka med arkiveringskoden.

Fält 14 I en enskild transaktion förmedlas den andra partens namn i fält 14 alltid när den är tillgänglig. Uppgiften finns inte på en sammandragstransaktion. Namnet är antingen mottagarens namn i fråga om betalarens enskilda transaktion, eller betalarens namn i fråga om mottagarens enskilda transaktion. Namnkällan anges endast för transaktioner som har uppgiften Mottagare/Betalare och den anger ursprunget till mottagarens eller betalarens namn som förmedlats.

Uppgiften Namnkälla har värdena:

- A = Namnet har fåtts från kundens material i maskinläsbart format eller kunden har sparat det som självtjänst.
- J = Namnuppgiften har fåtts från bankens register utifrån kontonumret.
- K = En tjänsteman på bankens kontor har sparat namnet.

Fält 15 I fält 15 finns i fråga om betalarens transaktion mottagarens kontonummer som betalarens bank angett då den förmedlat transaktionen. Med hjälp av uppgiften kan betalaren kontrollera till vilket konto betalningen riktats. Uppgiften Ändrat konto gäller endast mottagarens kontonummer och den anger att det kontonummer som betalaren ursprungligen angett ändrats i bankens system.

Uppgiften Ändrat konto har följande värden:

- tomt = har inte ändrats
- * = har ändrats

Tilläggspost för transaktion

Fält	Uppgiftens namn	Form	Beskrivning
1	Materialkod	AN1	S
2	Postkod	AN2	11
3	Postens längd	N3	
4	Typ av tilläggsuppgift	AN2	
5	Tilläggsuppgift	ANnnn	
	TOTALT	8+nnn	

Tilläggsposten för en transaktion består av en inledande del som är gemensam för alla tilläggsposter samt av en tilläggsuppgift, vars längd varierar beroende på tilläggsuppgiftens typ.

Fritt formulerat meddelande, typ = 00			
5.1	Meddelande - 1	AN35	
5.2	Meddelande - 2	AN35	
...	.....		
5.12	Meddelande - 12	AN35	

	TOTALT	Max 420	

St.-antal, typ = 01			
5.1	Antalet transaktioner, st.	N8	
	TOTALT	8	

Uppgifter om fakturatransaktion, typ = 02			
5.1	Kundnummer	AN10	
5.2	Tomt	AN1	
5.3	Fakturanummer	AN15	
5.4	Tomt	AN1	
5.5	Fakturans datum	AN6	ÅÅMMDD
	TOTALT	33	

Uppgifter om korttransaktion, tilläggsuppgiftens typ = 03			
5.1	Kortets nummer	AN19	
5.2	Tomt	AN1	
5.4	Affärens arkivreferens	AN14	
	TOTALT	34	

Uppgifter om korrigeringstransaktion, typ = 04			
5.1	Den ursprungliga arkiveringskoden för den transaktion som korrigeras	AN18	
	TOTALT	18	

Uppgifter om valutatransaktion, tilläggsuppgiftens typ = 05			
5.1	Motvärde		
	.1 Förtecken	AN1	
	.2 Belopp	N18	16 heltal + 2 dec.
5.2	Tomt	AN1	
5.3	Valutans ISO-kod	AN3	
5.4	Tomt	AN1	
5.5	Valutakurs	N11	4 heltal + 7 dec.
5.6	Kursreferens	AN6	
	TOTALT	41	

Uppgifter om uppdragsgivaren, typ = 06			
5.1	Uppgift om uppdragsgivaren-1	AN35	
5.2	Uppgift om uppdragsgivaren-2	AN35	
	TOTALT	70	

Tilläggsuppgifter om banken, typ = 07			
5.1	Tilläggsuppgift-1	AN35	
5.2	Tilläggsuppgift-2	AN35	
...	.....		
5.12	Tilläggsuppgift-12	AN35	
	TOTALT	Max 420	

Uppgifter om betalningsgrund, typ = 08			
5.1	Betalningsgrundkod	N3	
5.2	Tomt	AN1	

5.3	Betalningsgrundens förklaring	AN31	
	TOTALT	35	

Uppgifter om specifikationen namn, typ = 09			
5.1	Specifikation för mottagarens/betalarens namn	AN35	
	TOTALT	35	

Saldopost

Fält	Uppgiftens namn	Form	Beskrivning
1	Materialkod	AN1	S
2	Postkod	AN2	40
3	Postens längd	N3	50
4	Datum för förfrågan	N6	ÅÅMMDD
5	Saldo vid tidpunkten för förfrågan .1 Förtecken .2 Belopp	 AN1 N18	 16 heltal + 2 dec.
6	Disponibelt saldo .1 Förtecken .2 Belopp	 AN1 N18	 16 heltal + 2 dec.
	TOTALT	50	

Meddelandeposten förmedlas till kunden endast om förfrågan inte kan göras eller om uppgifterna inte är aktuella på grund av störningar.

Fält	Uppgiftens namn	Form	Beskrivning
1	Materialkod	AN1	S
2	Postkod	AN2	70
3	Postens längd	N3	
4	Bankgruppens kod	AN3	
5	Meddelande .1 Rad - 1 (t.ex. störningens orsak) ... .6 Rad - 6	 AN80 AN80	
	TOTALT	Max 489	

3.4.10 Beställa upprepningskontoutdrag

Det tekniska namnet/FileType för tjänsten Beställning av upprepningskontoutdrag är ORDER TU.

Beställningen har formen:

$$ORDER TU startdatum slutdatum kontorsnummer kontonummer

där

- startdatum är kontoutdragsperiodens startdatum i formen ååååmmdd
- slutdatum är kontoutdragsperiodens slutdatum i formen ååååmmdd
- kontorsnummer, 6 tecken
- kontonummer, 8 tecken

Om beställningen lyckades, är returkoden 00 OK. Ett upprepningskontoutdrag bildas enligt schemat för kontoutdrag till nästa morgon.

3.5 Beställa material

Kundens system kan hämta en lista över material från WS-kanalen. Följande sökkriterier kan användas då listan söks:

- Materialets registreringstidpunkt i kanalen med avgränsning till ett bestämt tidsintervall med en dags precision.

- Uppgift om materialets status

    - i fråga om material som kunden skickat
        - WFP – väntar på behandling (Waiting for Processing)
        - FWD – har skickats till fortsatt behandling (Forwarded)

    - i fråga om material som kunden kan hämta
        - DLD – har hämtats (Downloaded)
        - NEW – har inte hämtats (New)

- Materialets typ, t.ex. pain.001.001.02, pain.002.001.02.

Material som kunden själv tagit bort med funktionen deleteFile visas inte på listan.

Både material som kunden skickat till banken och material som banken skickat för avhämtning av kunden visas i listan över material. Med lämpliga filter i getFileList-operationen kan kundens programvara välja vilka material som visas på listan.

3.6 Ta bort material

Kunden kan ta bort material som kunden skickat till banken med funktionen deleteFile. När material tas bort, ändras materialets status från WFP till DEL. Denna ändring av status förhindrar att material förs till fortsatt behandling. Den har ingen annan inverkan. Borttagna material syns inte i operationen getFileList.

Borttagning av material kan göras efter att materialet sänts till banken och före den tagits till behandling. Material som tagits till behandling kan inte längre tas bort.

Hur länge materialet väntar i WS-kanalen innan den tas till fortsatt behandling beror på tjänst och materialtyp. Till exempel C2B-betalningsmaterial behandlas på bankdagar kl. 02:30 och varje halvtimme kl. 7:00–18:00.

3.7 Materialhanterare och fullmakter

Fullmakten till betalningsrörelsematerial bygger på användarkodens roll Bildat av i WS-kanalen. Kundkoden i den aktuella användarkodens avtal om WS-kanalen och kontorsnumret som används som en parameter för användarkoden bildar den så kallade materialhanterarkoden. Materialhanterarkoden, dvs. kontoret, ska anges som tillåten avsändare eller som mottagare av material som ska avhämtas i det betalningsrörelseavtal i enlighet med vilken material behandlas och bildas.

Materialhanteraren är den tillåtna avsändare eller materialets mottagare som antecknats i betalningsrörelseavtalet. Materialhanteraren har ett eget avtal om WS-kanalen, tillsammans med anknytande användarkoder och certifikat till användarkoderna.

3.8 Exempel på meddelanden och tjänstebegäran

3.8.1 Meddelande om begäran

Exempel på ett SOAP-meddelande om begäran av operationen getFileList. Base64-enkodade elementinnehåll är förkortade och utelämnade delar har ersatts med tre punkter för bättre läsbarhet.

```
<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 Svarsmeddelande

```
<?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 Tjänstebegäran getFilelist

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

3.8.4 Tjänstesvar getFileList

```
<?xml version="1.0" encoding="UTF-8"?>
<ApplicationResponse xmlns="http://bxd.fi/xmldata/" xmlns:ns2="http://www.w3.org/2000/09/xmldsig#">
    <CustomerId>1000000000</CustomerId>
    <Timestamp>2011-08-15T09:48:33.668+03:00</Timestamp>
    <ResponseCode>00</ResponseCode>
    <ResponseText>OK.</ResponseText>
    <FileDescriptors>
        <FileDescriptor>
            <FileReference>5802</FileReference>
            <TargetId>MLP</TargetId>
            <ParentFileReference>5801</ParentFileReference>
            <FileType>pain.002.001.02</FileType>
            <FileTimestamp>2011-07-29T12:00:16.483+03:00</FileTimestamp>
            <Status>NEW</Status>
        </FileDescriptor>
        <FileDescriptor>
            <FileReference>5803</FileReference>
            <TargetId>MLP</TargetId>
            <ParentFileReference>5801</ParentFileReference>
            <FileType>pain.002.001.02</FileType>
            <FileTimestamp>2011-07-29T12:01:16.971+03:00</FileTimestamp>
            <Status>NEW</Status>
        </FileDescriptor>
    </FileDescriptors>
    <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
        <SignedInfo>
```

```
            <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
            20010315#WithComments"/>
            <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
            <Reference URI="">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                <DigestValue>LlpU5jyiDd5kO5FjJDIL7AWZyBQ=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>WKtQ1t8V1...LkGV9DMz0cQ==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIID1zCCAr...JKaoOlc5gLu</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ApplicationResponse>
```

3.8.5 Tjänstebegäran 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>OQA4fiudfd6KJKR0KlNTsE9Fyxc=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>c2RzFUa...9VBAnMQ==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIC9TC....v3xpHPU=</X509Certificate>
            </X509Data>
        </KeyInfo>
    </Signature>
</ApplicationRequest>
```

3.8.6 Tjänstesvar 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 Tjänstebegäran 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 Tjänstesvar uploadFile

Exempel på valideringsfel i pain.001.001.02-material som kunden skickat.

```
<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>
```

Svaret på ett annorlunda schema-fel ser ut på det här sättet:

```
<?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>
```

I detta exempel på fel innehåller elementet ApplicationResponse.Content följande pain.002.001.02-material (base64-enkodat). För information om innehållet och användningen av svarsmeddelanden som gäller betalningsrörelsen se den separata kundanvisningen om C2B-betalningar.

```
<?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 Tjänstebegäran 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/nfTlGGFGIHL43pI=</DigestValue>
            </Reference>
        </SignedInfo>
        <SignatureValue>dgUhp4b...qelFFvQ==</SignatureValue>
        <KeyInfo>
            <X509Data>
                <X509Certificate>MIIC9TCCAd2g...Iv3xpHPU=</X509Certificate>
            </X509Data>
```

```
        </KeyInfo>
    </Signature>
</ApplicationRequest>
```

3.8.10 Tjänstesvar 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 Meddelanden och tjänstebegäran i Identifieringstjänsten för Web Service-kanalen

4.1 SHA1-certifikatet ersätts med SHA256

OP Gruppen slutar stöda certifikat och elektronisk signatur enligt SHA1 och ersätter det med SHA256.

Den gamla SHA1-tjänsten stängs 31.8.2025 och efter detta ska kunderna använda algoritmen SHA256. Materialen förmedlas inte vidare i Web Service-kanalen fr.o.m. 1,9.2025, om bankförbindelseprogrammet bildar förbindelsen med ett certifikat/TLS-krypteringsmetoder som gått ut.

Kunderna ska göra de nödvändiga ändringarna i sina programvaror för att kunna börja använda algoritmen SHA256 i tjänstebegäran (ApplicationRequest) och SOAP-begäran (SOAPRequest).

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

Svarsmeddelanden undertecknas på motsvarande sätt med SHA256-certifikat och algoritm.

Adresserna till driftmiljön för Företagets bankförbindelse:

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

4.2 Meddelandebeskrivningarna för Identifieringstjänsten

SOAP-meddelandenas struktur och Identifieringstjänstens adress beskrivs i en WSDL-fil.

SOAP-meddelanden signeras inte i Identifieringstjänsten. Autenticiteten kontrolleras med signatur endast på nivån för tjänstebegäran (CertApplicationRequest).

WDSL-filen finns att hämta på adressen

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

4.3 Tjänstebegäran och scheman

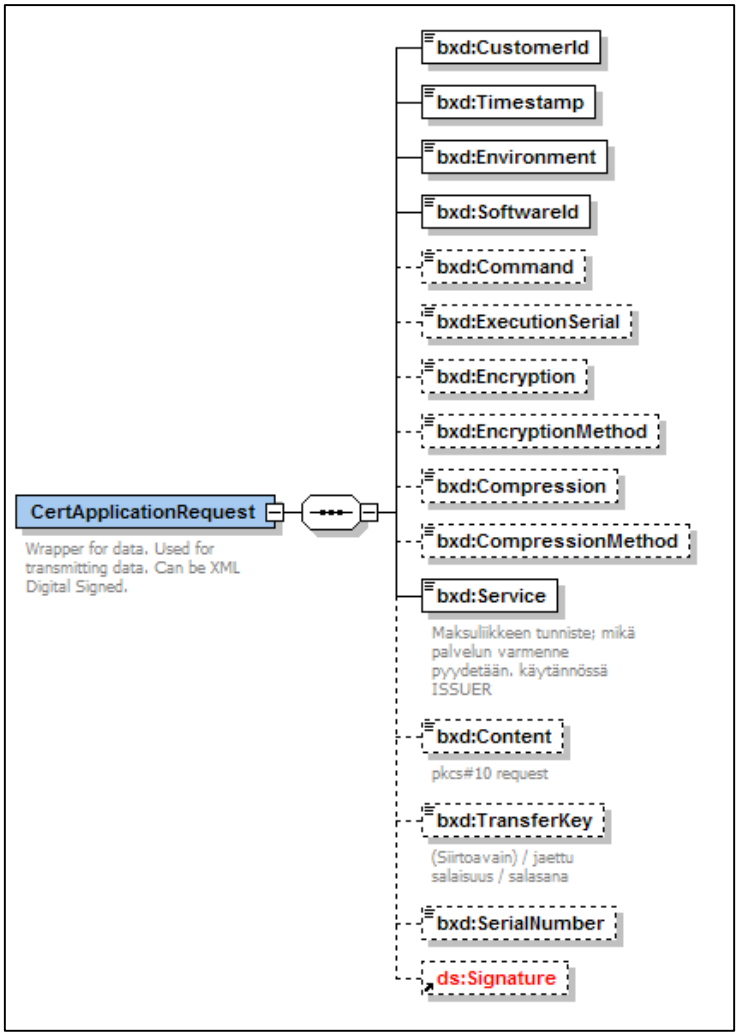
XML Schema-filerna beskriver den tjänstebegäran som finns i meddelandet och tjänstesvaret.

Identifieringstjänstens WSDL finns på adressen

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

Tjänstebegäran som kunden sänder heter CertApplicationRequest och tjänstesvaret som bankens Identifieringstjänst sänder heter CertApplicationResponse.

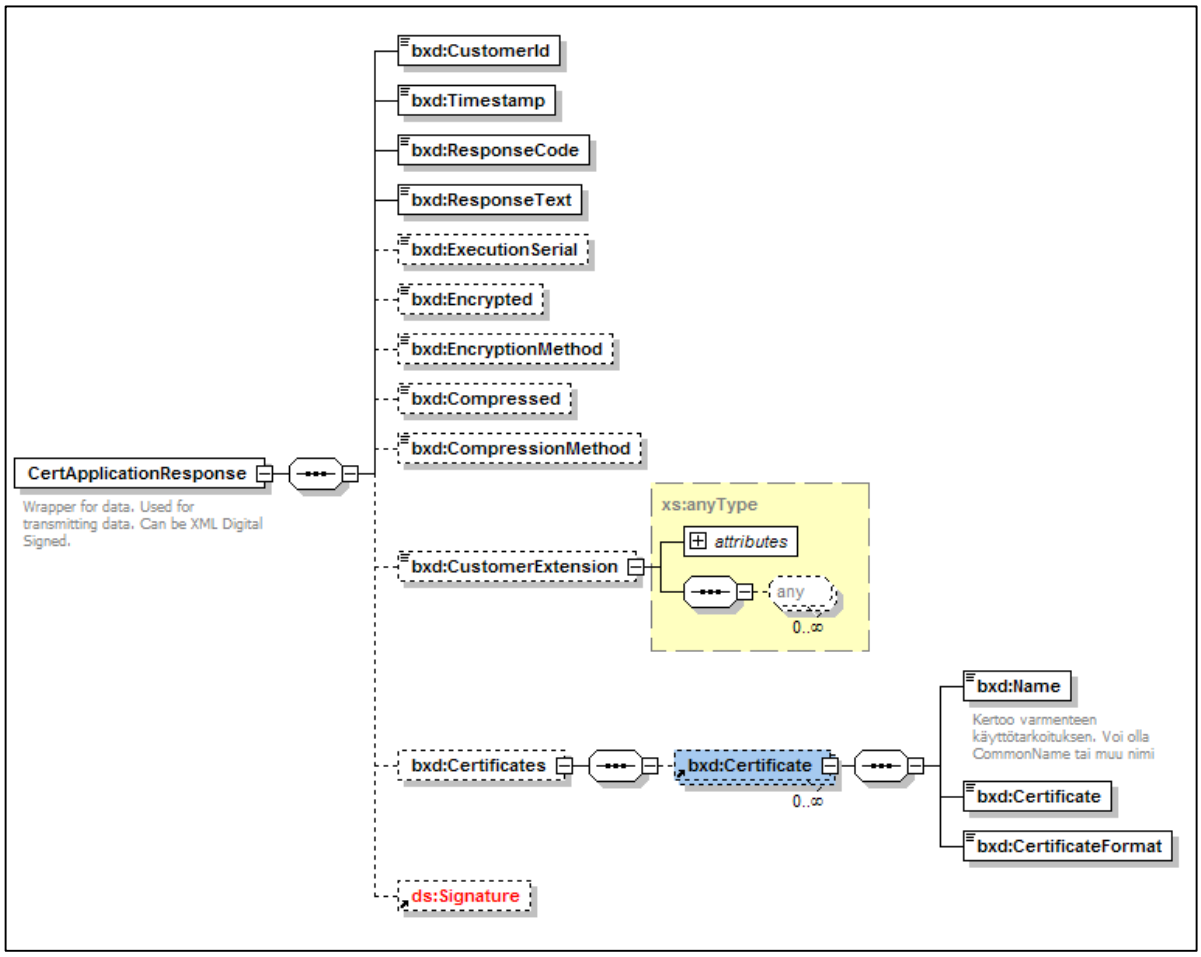
4.3.1 CertApplicationRequest



De viktigaste elementen som ska ifyllas i tjänstebegäran Begäran om certifikat är:

- CustomerId – användarkoden för WS-koden för den som begär certifikat, 10 siffror
- Content – base64-enkodad begäran om certifikat av formatet pkcs10
- TransferKey – överföringsnyckel, 16 siffror, om användaren gör den första begäran om certifikat med användarkod
- Signature – XML-signatur, om användaren förnyar ett certifikat
- Obligatoriska uppgifter:
    - Timestamp – tidsstämpel för klockslaget då tjänstebegäran bildades, används främst som hjälp vid utredning
    - Environment – vid produktion ska värdet vara PRODUCTION, i annat fall avvisas begäran.
    - SofwareId – namn- och versionsuppgift för programvaran som gjort tjänstebegäran, används främst som hjälp vid utredning
    - Service – MATU

4.3.2 CertApplicationResponse



4.4 Exempelbegäran i Identifieringstjänsten

4.4.1 Meddelande om begäran

```
<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 Svarsmeddelande

```
<?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 Tjänstebegäran Förnyelse av certifikat

I exemplet presenteras begäran om förnyelse av certifikat med användarkoden 1000000047. Tjänstebegäran har signatur eftersom identifieringen och kontrollen av autenticiteten bygger på ett gällande certifikat för samma användarkod.

```
<?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 Tjänstesvar Förnyelse av certifikat

```
<?xml version="1.0" encoding="UTF-8"?>
<xd:CertApplicationResponse xmlns:xd="http://op.fi/mlp/xmldata/">
```

```
        <xd:CustomerId>1000000047</xd:CustomerId>
        <xd:Timestamp>2010-01-26T14:32:51.808+02:00</xd:Timestamp>
        <xd:ResponseCode>00</xd:ResponseCode>
        <xd:ResponseText>OK.</xd:ResponseText>
        <xd:Certificates>
                <xd:Certificate>
                        <xd:Name>CN=1000000047,C=FI</xd:Name>
                        <xd:Certificate>MIICvTCCAa... Ne+0U19z3z25nFb</xd:Certificate>
                        <xd:CertificateFormat>X509v3</xd:CertificateFormat>
                </xd:Certificate>
        </xd:Certificates>
        <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
                <SignedInfo>
                        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-
                        20010315#WithComments"/>
                        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                        <Reference URI="">
                                <Transforms>
                                        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-
                        signature"/>
                                </Transforms>
                                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                <DigestValue>ZdaOhjgcjfFb5aRwgMeWtlR5Oj0=</DigestValue>
                        </Reference>
                </SignedInfo>
                <SignatureValue>PXPPXC... +TLjnO2g==</SignatureValue>
                <KeyInfo>
                        <X509Data>
                                <X509Certificate>MIIDnDCCAo... A7xVA==</X509Certificate>
                        </X509Data>
                </KeyInfo>
        </Signature>
</xd:CertApplicationResponse>
```

4.4.5 Tjänstebegäran Begäran om certifikat med överföringsnyckel

```
<?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 Detaljerade anvisningar för att skapa en getCertificate-begäran med överföringsnycklar

a. Ett CSR-meddelande (Certificate Signing Request) som använder nyckelparet med en publik och en privat nyckel ska se ut så här:

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

b. När CSR har skapats, tas dess start- och sluttaggar bort och binärvärdet läggs till på samma sätt som i fråga om punkt 4.4.5 Tjänstebegäran Begäran om certifikat med överföringsnyckel:

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

c. Tjänstebegäran Begäran om certifikat med överföringsnyckel som skapats i enlighet med punkt 4.4.5 ska, när den är base64-enkodad, ge följande värden:

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

e. Den base64-kodade tjänstebegäran ska upptas i meddelandet för begäran på samma sätt som i punkt 4.4.1:

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

f. Den ursprungliga getCertificate-begäran med överföringsnycklar är nu färdig, och den kan skickas till banken för hämtning av ett nytt certifikat.

4.4.6 Tjänstesvar Begäran om certifikat med överföringsnyckel

```
<?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 Tjänstebegäran Hämta certifikat med serienummer

```
<?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 Tjänstesvar Hämta certifikat med serienummer

```
<?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 Tjänstebegäran Hämta tjänstecertifikat

```
<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 Tjänstesvar Hämta tjänstecertifikat

```
<?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>
```