Aktia, SP, POP

Version 1.2

02.05.2014

**Service Description**

# Web Services - connection

SAMLINK

# Table of contents

# VERSION CATALOGUE

### Documents version information

| Version nr. | Date | Muutokset |
|---|---|---|
| 1.2 | 02. May 2014 | New file types added: XT, XE, XM, VE, VA, VB, WK |
| | | |

# 1 GENERAL

This document describes the Web Services connection protocol implemented by Samlink.Web Services (WS) is Samlink's new connection protocol for transfer of batch transmission. data between the customer and the bank, aimed at banks' corporate clients (hereinafter Client). The Web Services connection protocol is based on internationally-recognised standards and complies with W3C standards (World Wide Web Consortium, see www.W3.org). Data communication will always take place through encrypted SSL connection online (TCP/IP), so VPN encryption is not required. Identification of the Client is based on Public Key Infrastructure (PKI) certificate, which the Client will get from the bank. The bank shall register the certificate and Samlink shall function as the Certificate Authority (CA).

The WS connection protocol enables companies' data communication protocol, PKI certification and security specifications in compliance with the Web Services Interoperability Organization (see www.ws-i.org) specifications. This document describes the standard as it is applied at Samlink.

The technical specifications of the WS protocol have been described in other documents, which are available at the Federation of Finnish Financial Services website (www.fkl.fi). The specifications are in English.

# 2 WEB SERVICES

WS data communication supports file transfer from the Client or to the Client. The Client shall always be the active party in establishment of connections and opens the connection both when sending data to the bank and when retrieving data from the bank (push-pull).

The user must have banking software that supports the WS connection protocol. The currently used ftp/PATU security protocol will work alongside the Web Service protocol until further notice.

### 2.1 ABBREVIATIONS AND TERMS USED IN THE SERVICE DESCRIPTION

| | |
|---|---|
| WS | Web Services. De facto data communication standard which complies with international standards such as SOAP and XML. |
| PKI | Public Key Infrastructure. International standard for identifying a party to the connection (the owner of the certificate). |
| XML | Extensible Markup Language. Format that is used, for example, in the Corporate payments service and SOAP messages. |
| PATU | PAnkki TUrvallisuus (‘banking security’). A specification published by the Federation of Finnish Financial Services for the current identification technology used by Finnish banks. |
| CA | Certificate Authority. The body granting/publishing the PKI certificate. |
| SSL | Secure Sockets Layer. Decryption technology used in Internet connections. |
| HTTPS | Hypertext Transfer Protocol Secure. The encrypted version of HTTP. |
| SOAP | Standardised message format of the WS connection. |

## 3 AGREEMENT ON THE USE OF THE WEB SERVICES CONNECTION

The Client and the bank shall sign an agreement on the use of the Web Services connection. The agreement shall determine the Client and the contact person representing the Client.

During the signing of the agreement the bank shall hand over the first part of the one-time password meant for the retrieval request for the certificate while the second part will be mailed in a sealed envelope. The address window of the envelope shall show the pointer information of the envelope.

In case the Client’s application does not support the certificate retrieval request as such, the one-time password shall be used for retrieving the certificate from Samlink's certificate service with a secure e-mail.

### 3.1 CERTIFICATES

The agreement form handed over during the signing of the agreement includes the information the user needs to download their own PKI certificate from Samlink to company’s system. The required information is as follows:

- WS-user ID
- pointer information in the letter
- one-time password.

In the bank's register, the certificate is always designated to a certain organisation. If the certificate is used in automatic communication between machines, the certificate of a company may be available for use by some other than the designated individual. The Client is liable to ensure that certificates are stored appropriately and that they can only be used legally.

### 3.2 PRECONDITIONS OF USING WS CONNECTION

- The Client must have a valid agreement with the bank on the use of Web Services connection.
- The Client must possess the one-time password given by the bank during the signing of the agreement, which is used for retrieving the client-specific PKI certificate from Samlink's service to the Client's system. This phase can be bypassed if the Client's application does not support electronic retrieval of the certificate. The digital signature based on the PKI certificate, authentication of the Client and user rights for the service in question are checked at the bank on the basis of the certificate.
- Software to implement the digital signature and bank connection.

Payment transfer data to be sent or retrieval request for the data is digitally signed with the private key belonging to the Client's PKI certificate before connecting to the bank. The signature can be made with separate software or as an integrated part of the bank connection program.

The digital signature is implemented and bank connection is formed with software that supports connection complying with Samlink's Web Services specifications. The general Web Services specifications have been jointly determined by Finnish banks and it is available at the Federation of Finnish Financial Services website (www.fkl.fi).

Samlink's bank-specific instructions for the application of the specifications are presented in the separate service description.

Software companies also have a separate Samlink description of the Web Services interface.

Before sending messages to the bank, the structural integrity of the messages must be verified and messages tested.

## 4 USE OF CERTIFICATES AND PKI KEYS IN BANK CONNECTIONS

PKI technology and certificates are used to authenticate the Client in Web Services connections. PKI or the Public Key Infrastructure is an operating model for the use of keys and certificates. The operating model utilises unsymmetrical encryption methods based on key pairs so that the basic functions of secure electronic communications can be implemented, such as digital signature using the private key of the signee.

The certificate refers specifically to X.509 standard certificates, where the Certificate Authority (CA) is Samlink. This confidential relationship has only two parties; the bank and the Client. The certificate is granted on the basis of the Client's Web Services agreement.

The Client uses the certificate, or rather the secret and public key described by it, to sign for and send data while the bank uses it to identify the Client. The bank can use the signature to verify that the data has been approved by a body that has the right to use the certificate and the corresponding service. At the same time, it is verified that the data has not been amended since the signature.

The certificate is valid for two years, after which it has to be renewed.

The digital signature is always implemented in a manner complying with the banks' Web Services description, in which the XML structure named ApplicationRequest is the object of signature. ApplicationRequest is a simple XML structure, which contains the identifier data of the Client and the data.

The digital signature is of the envelope type. This means that the entire content of the message to be signed with its possible data to be sent belongs to the sphere of the signature. The digital signature covers both the authentication and the immutability of the data. Any change in the contents will spoil the signature. The changes are recognized in the bank’s Web Services service and the connection is denied. Correspondingly, the bank signs a message titled ApplicationRequest when creating messages to the Client with the Web Services connection. Consequently, the parties to the Web Services connection can ensure that the message has come from the agreed party and that the data has not changed during transfer.

It is possible to duplicate the envelope type signature, in which case the signee signs for the whole content and also the previous signature. Duplicated ApplicationRequest signature is not available for use in Samlink’s Web Services connection protocol..

### 4.1 AUTHENTICATION OF THE CLIENT AND RIGHT TO USE THE SERVICE

The authorisation to use the service is based on the digital signature of the ApplicationRequest message, and consequently the authentication of the Client and the checking of the authorisation from the bank’s service agreement system. Before bank connection, the signed ApplicationRequest message is relayed within the SOAP message, in its body element. ApplicationRequest can be signed in advance before sending.

The SOAP message is signed with the data provider’s own PKI key not more than one hour before the bank connection. This signature is merely the authorisation to use the Web Services connection, not signing for any data in the service. The signature of the SOAP message only ensures that the data provider has the right to communicate with the bank's batch transfer service with a Web Services connection and send ApplicationRequest messages signed by the Client and to receive ApplicationRequest messages signed by the bank and intended for the Client.

The following figure 1 presents the relationships between the data to be sent (Payload), the ApplicationRequest message and SOAP message sent to the bank. However, in order to avoid dependencies between nested XML structures, the messages must be base64-coded before they are placed as contents of a field.

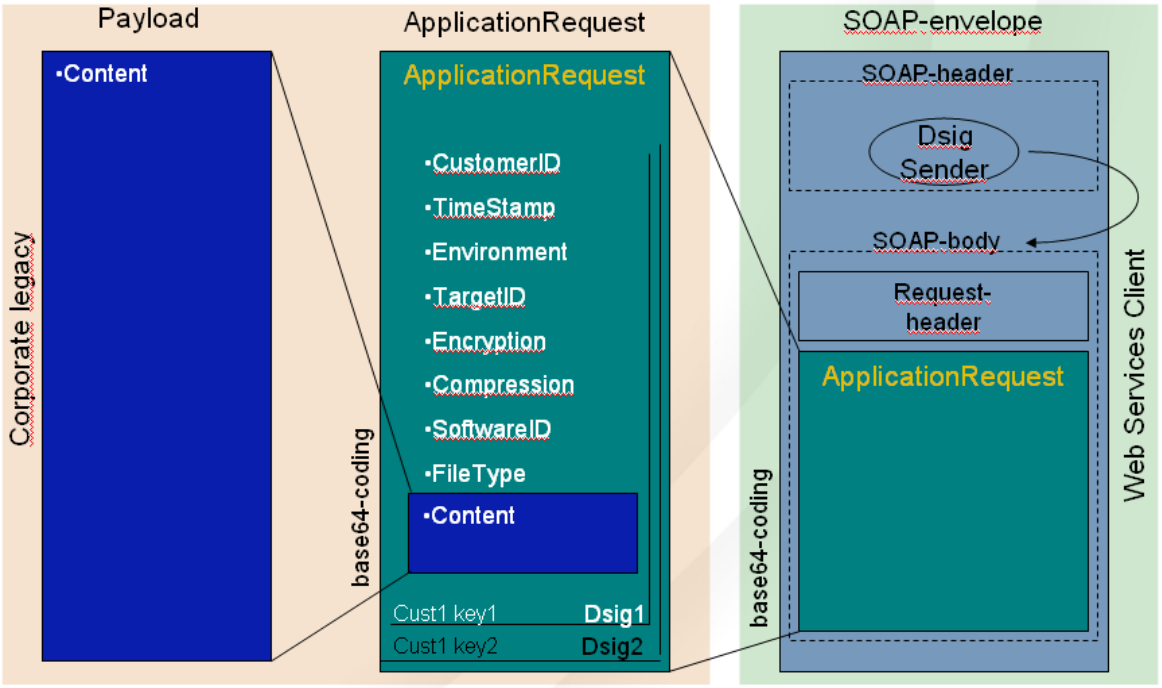


Figure 1. Creating of SOAP message

Usually, the Client also functions in the role of provider of its bank connection software,in which case the SOAP message can be signed with the same PKI key with which the ApplicationRequest was signed.

When the user requests data from the bank, the Content field of the ApplicationRequest is left blank. Even in this case, the ApplicationRequest must be signed in the same way as when sending data to the bank.

### 4.2 INVALIDATION OF CERTIFICATES

If the Client suspects that its key has ended up in the wrong hands or for any other reason wishes to invalidate the certificate, a new certificate has to be ordered from the bank after the invalidation.

This measure is the Client's responsibility and requires renewal of the agreement at the bank.

Termination of the agreement closes the certificate and it cannot be reopened for use.

## 5 WEB SERVICES –CONNECTION DATA

### 5.1 DATA

The following financial messages can be sent or retrieved with a Web Services

connection:

| Aineiston nimi | Aineistotyyppi | Selitys |
|---|---|---|
| SEPA-XML account transfer (sending) | XL | pain.001.001.02 and .03 |
| SEPA-XML fault feedback (retrieval) | XP | pain.002.001.02 and .03 |
| SEPA-XML urgent payment (sending) | XF | pain.001.001.02 and .03 |
| Arriving reference payment (retrieval) | OP | |
| XML- Arriving reference payment (retrieval) | XE | camt.054.001.02 |
| XML- Pyment list (retrieval) | XM | camt.054.001.02 |
| Bank statement (retrieval) | TO | |
| XML- Bank statement (retrieval) | XT | camt.053.001.02 |
| Consolidated bank statement (retrieval) | TK | |
| Consolidated bank statement with transactions (retrieval) | TT | |
| Account event enquiry (retrieval) | RA | |
| Sending of e-invoices (sending) | VL | |
| Retrieval of e-invoices (retrieval) | VN | |
| Retrieval of e-invoicing fault notification (retrieval) | VP | |
| Sending of invoicer sender information (sending) | VS | |
| Retrieval of address receiver information (retrieval) | VR | |
| Receiver proposal (sending) | VE | |
| Finvoice- attachment (sending) | VA | |
| Finvoice- attachment (retrieval) | VB | |
| Currency rates (retrieval) | WK | |

Table 1. File types accepted in Samlink web services

# 6 GENERAL DESCRIPTION OF TRANSFER PROTOCOL

The Web Services connection is a relay of ‘sessionless request-reply’ messages. In the Web Services connection, the Client identifier data is included in each individual connection, unlike the ftp-PATU connection, in which the connection is opened with a presentation message.

Data transfer connection takes place in a manner based on the Web Services standard; by sending and receiving the XML structure compliant with the SOAP standard (SOAP = standardised WS connection message format). SOAP messages have header and body fields which are to be signed by the Client's certificate before sending.

Each connection includes individual digitally signed ApplicationRequest messages with the required measure request (Command). ApplicationRequest is always signed with the Client's personal key. ApplicationRequest is placed in the body section of the SOAP message and is base64-encoded.

The Command is either for sending data to bank (UploadFile) or request to retrieve data (DownloadFile) from the bank. There are two additional commands:

- DownloadFileList, which provides the Client with a list of data available for retrieval
- DeleteFile, with which the Client can delete the data it has sent.

ApplicationRequest is always directed towards some data type. The type of the data requested must be entered in the Filetype field.

The bank responds to each Request message with a Response message. In the case of Uploads, the ApplicationResponse message includes acknowledgement of the data being received or rejected. Various services engender status and feedback messages in accordance with their individual timetables. It must be taken into account that sent data can be rejected later, for example due to insufficient balance on the account.

The fault notification is produced with a SOAP fault message when confirmation of the ApplicationRequest message or signature has failed.

Correspondingly, the Download Request is answered by returning the requested data with an ApplicationResponse message in its Content field in base64 encoding. If the required data is not available, the Response message will contain a clarifying fault notification. The bank’s response will always include the ApplicationResponse message with corresponding fields as in the Request message including Content with the file to be received.

The ApplicationResponse message has been always digitally signed in the bank, so the Client/Client's program can check that the message has come from the agreed party and that it has not changed since the signing.

The structure of the ApplicationRequest, ApplicationResponse and SOAP messages has been described in detail in the document Web Services Security and Communication Description as well as other documents which are available at the Federation of Finnish Financial Services website, www.fkl.fi.

### 6.1 CREATION OF DATA AND SENDING IT TO THE BANK

The following outlines the steps required to create and send the message.

The bank connection program will usually execute these measures without the user seeing them. If the data is signed and send with different programs, the signing of the message takes place in accordance to steps 1 to 5 and sending of the message correspondingly in accordance with the steps 6 to 8.

See also fig. 1 in section 4.1 which explains the connections between messages.

Signing the data:

1. Create the payment transfer material (e.g. SEPA-XML data) in the company's system. The data must the converted with base64 encoding for the duration of sending. The data is called the Payload.
2. Create an XML structure called ApplicationRequest which includes elements Content and Signature.
3. Place Payload/data in the Content element of the ApplicationRequest.
4. Sign the entire ApplicationRequest digitally using the Client-specific certificate and its private key. Convert the signed message into a base64-encoded format.
5. Transfer the message to data communications program or storage media..

Delivery of the data

6. Place the signed and base64-encoded ApplicationRequest into the body section of the new SOAP message, in its ApplicationRequest field.
7. Sign the SOAP message digitally with the data provider's certificate's private key. The key can be the same as the above-mentioned key which was used to sign the ApplicationRequest message
8. Send the SOAP message using the WS protocol and wait for the bank’s answer. Check the signature of the response and show the content of the ApplicationResponse message to the user..

The bank’s response complies with the ApplicationResponse message determined in the Web Services description. The response has a status code which tells that sending has succeeded (=0) or that there has been a malfunction (larger than 0).

### 6.2 RETRIEVAL OF DATA FROM THE BANK

The retrieval of data happens largely as above but because there is no data to be sent, the Content field is left blank (steps 1, 2 and 4 are left out). The content of the Command field is the DownloadFile or DownloadFileList.

The bank’s response complies with the ApplicationResponse message determined in the banks’ Web Services description. If a file is requested in the response it is in the ApplicationResponse/Content field and is base64-encoded. The ApplicationResponse Message has been always digitally signed in the bank, so the Client/Client's program can check that the message has come from the agreed party.

### 6.3 THE TECHNICAL INSTRUCTIONS OF THE BANK CONNECTION PROGRAM

Samlink’s Web Services connection protocol has been described in more detail in separate instructions. These instructions are mainly intended for use by companies producing bank connection programs, so that all the service features and security specifications can be strictly followed.

# 7 WEB SERVICE CONNECTION TEST FOR THE BANK CONNECTION PROGRAM

It is good to test the connection settings of the bank connection program before sending the first payment data by using a separate test feature of the Web Service connection.

The testing takes place with the bank connection program just like the sending of payment data but in the program's test status. In this case the bank connection program sets the value TEST in the Environment field of the ApplicationRequest message. Payments sent in test status are not entered in the account.

When the connection has been found to work flawlessly, it can be used for the bank's Web Services connections.

# 8 TIMETABLES

Data can be sent and retrieved 24/7. The processing and completion timetables of XML data sent to or retrieved from the bank can be found in the separate service description.

Retransmission of approved data or its deletion must be separately agreed upon with the payment transaction department of the Companies.

# 9 WEB SERVICES CONNECTION ADDRESS

**Aktia Savings Bank Plc**

File transfer: https://aineistopalvelut.aktia.fi/services/CorporateFileService

Certificate service: https://aineistopalvelut.aktia.fi/wsdl/CertificateService.xml

**Local cooperative banks and savings banks**

File transfer: https://ws.samlink.fi/services/CorporateFileService

Certificate service: https://ws.samlink.fi/wsdl/CertificateService.xml

The connection is always SSL-secured.

# 10 PKI CERTIFICATES AND THEIR DISTRIBUTION

When agreeing upon the connection protocol, the Client’s contact person will receive a two-part one-time password with the right to send the certificate request to the bank’s system and retrieve a signed certificate with the WS connection. The Client will receive a certificate with which the data or request (ApplicationRequest) is signed digitally before connection to the bank.

It is also possible to deliver the certificate request to the bank in other ways, in case the Client's application does not support the action. The Certificate Authority’s certification practice has been described in separate documents:

- Samlink Customer CA certification principles for WS data services certificates
- Samlink Customer CA certification practice

## SAMLINK'S ADVISORY PHONE NUMBERS

The payment transactions call-centre will answer your questions about testing, verifying the data and use of electronic services at +358 (0)100 4052 (EUR 1.17 + local calling costs) on banking days 8.30 am–4.30 pm.