Danske Bank

Service Description

Web Services protocol and PKI security solution

31.12.2017

TABLE OF CONTENTS

Date	Version	Change
1.2.2011	Version 1.0	
31.3.2011	Version 1.1	Added services AMVN Direct Debits and VKEN Currency exchange
1.6.2011	Version 1.2	Added e-invoices
15.6.2011	Version 1.3	Added 4.3 The customer can have feedback only from XML – payments (pain.001).
17.10.2011	Version 1.4	Added new services Payment terminal, Factoring
9.12.2011	Version 1.5	4.3 Added the file size maximum
3.1.2012	Version 1.6	4.4 Corrected FILN, FIVN and FIRN
19.03.2012	Version 1.7	4.3 Added the file size 10 megabytes
15.11.2012	Version 1.8	Name change to Danske Bank
01.12.2012	Version 1.9	Added in the service list conversion message FIPL
10.1.2013	Version 1.10	Update chapters 4.3 and 4.4, ISO message version 3
11.2.2013	Version 1.11	4.2 Certificat address is changed. 4.3 changed from 10 megabytes to 40 megabytes.
5.7.2013	Version 1.12	Added chapter 4.3 FISL Sender-info. Chapter 4.4 added XML Account Reports
15.10.2013	Version 1.13	Chapter 4.3 changed from 40 megabytes to 70 megabytes.
31.1.2014	Version 1.14	Direct Debit service ended
8.7.2014	Version 1.15	Added camt-message parameters.
20.03.2015	Version 1.16	Link corrected. Payment terminal applications away.
04.02.2016	Version 1.17	4.4 Added MCT Master Card for Corporate card transaction

1 Web Services protocol

1.1 General

The Web Services protocol (hereinafter "Web Services") is a safe and modern data communications solution that enables communications between a company's financial management systems and the Bank's system. Web Services can be generated either with eBanking software or directly from a company's financial management systems. Web Services is intended for material transfer between a company and the Bank.

Danske Bank's Web Services rely on an information security and message specification system applied jointly by Finnish banks. A technical description is available under 'Security and Message Specification for Messages' on the website of the Federation of Finnish Financial Services at fkl.fi.

Web Services uses an encrypted Internet connection. Parties are identified and materials are protected using the PKI security solution.

The Web Services protocol can be used to send and retrieve materials supported by the Bank. The materials supported by the protocol are listed in chapter 4..

The customer opens a Web Services connection in order to send or retrieve materials. The customer needs a Web Services user interface for establishing the connection and processing materials, such as the Danske Link electronic banking software.

1.2 Abbreviations and terms used

Application request	A service request included in a message sent via Web Services.
Application response	Response issued by the Bank to the customer's service request via Web Services.
PKI	*Public Key/Infrastructure,* public key infrastructure.
Private Key	Private key – A confidential part of an asymmetric pair of keys, which is used in the encryption of the public key. The private key is typically used for digital signatures or for opening a message encrypted using a public key.
Root Certificate	Root Certificate – The top-most entrusted level in a public key system - The root certificate signs and distributes certificates to lower level certifiers and cancels them, where necessary.
SOAP	A standardised Web Service connection message form, which includes the service requests sent via Web Services and their responses.
XML	eXtensible Markup Language, by means of which the meaning of the data can be described. XML language is used as a format for exchanging information between systems and for saving documents. It helps to organise vast amounts of data more clearly.

2 Agreement

The use of Web Services requires a valid service agreement with the Bank. The agreement defines the accounts, users and user rights that a company uses in the service.

The bank offers two different models for the agreement on Web Services link protocol.

1. A separate agreement on Web Services link protocol shall be concluded.

2. Web services –link protocol shall be joined to the agreement on Business Online web bank.

Agreement model 2 makes it possible for the users of the corporate web bank to process the banking material which has been sent and can be retrieved through the Web Services link protocol.

3 PKI security solution

3.1 PKI Security Solution

The processing of certificates in Danske Bank's Web Services relies on the PKI (Public Key Infrastructure) solution. In the model used by Danske Bank, there are two pairs of keys and two certificates for each customer. One of them is for signing the material and the other for encrypting it.

3.2 Connection and establishment

When concluding the agreement, the customer receives the instructions needed for starting the Web Services protocol. Certificates can only be retrieved when the agreement has been signed and the customer receives a one-time PIN code via mail for retrieving the certificates. The customer sends a certificate request to the Bank, on the basis of which the Bank will create certificates for the customer.

In order to be able to retrieve the certificates the customer needs in addition to a PIN –code also a user ID (6 alpha –numeric) for the Web Services link protocol and PKI security solution. The PIN –code and the user ID shall be input into the banking software used by the customer, where after the software sill send the bank a request for retrieval of the certificates through the Web Services link protocol. The customer shall save the certificates in his banking software. After this, the user of the Web Services link protocol may commence.

The root certificate can be retrieved from the www –pages of Danske Bank at the address: Danske Bank Group PKI -services

3.3 Revoke the Certificates

Customer can revoke certificates, if they are not needed anymore or due some security reasons (for. Ex. Certificates are missed, destroyed or some other security problems

Certificates can be revoked via banking software by revoke-function, which closes the existing valid certificates. Customer can contact to Danske Bank's Software and material transfer support. The agreement number or the user number is needed from the customer before the certificates can be closed.

3.4 The Certificate Lifecycle

All certificates have a certain lifetime. Customers are expected to check the status of their certificates on a regular basis. If a certificate is about to expire the customer must renew the certificate using the PKI Web Service RenewCertificate function. If the customer does renewal in advance, then there is no need to order new pin-code. Advice for certificate renewal can be found in the instructions of banking software.

If the customer doesn't renew a certificate before it expires – the customer must contact Customer Support in order to get a new PIN-code. Using this PIN-code the customer can now create a new set of certificates.

4 Using Web Services

4.1 Schedules (Cut off)

Web Services is available 24 /7.

4.2 Contact addresses

EDI Web Services - Sending material to and retrieving it from the Bank

https://businessws.danskebank.com/financialservice/edifileservice.asmx

PKI Web Services – Management of keys and certificates

https://businessws.danskebank.com/ra/pkiservice.asmx

4.3 Sending material

The customer generates materials in its own financial management system and sends them to Danske Bank.

When sending material to the Bank, the customer signs the message using its private key and encrypts the material using the Bank's public key.

The following materials can be sent via Danske Bank's Web Services:

C2BL pain.001.001.02 pain.001.001.03	Payment Transmission ISO 20022, pain.001.001.02 or 03 Payment Transmission ISO 20022, pain.001.001.02 Payment Transmission ISO 20022, pain.001.001.03
AYEL	Trade Union Membership
FALL	Factoring
FILL	E-invoice
FISL	Sender-info
IBAL	IBAN conversion transmission
OL2L (LM02), OL3L (LM03)	Invoice payment service
PELL	Recurring payments, salaries, pensions
UM2L	International payments
UMTL	Global Transfer MT101

In addition to the above materials Danske Bank's Web Service also supports the Danske Bank Group's local data formats. You can find the list of data formats in section 4.5 Web services Channel Technical Description.

When receiving a transmission, Danske Bank will send a confirmation message (*ApplicationResponse*) to the customer, with a status code indicating that the transmission was successful. Danske Bank then transfers the material for processing and the payments are made on their due dates.

The other file types than XML –payment file (pain.001) the bank sends feedback file of receiving (pain.002), but no feedback for further handling. Please, look in XML file service description.

At present, the material specific size limitation for Danske Bank's Web services link protocol connection is 70 megabytes as compressed for each transferred material batch. The payment material, SOAP frame and base64 coding are all included in the 70 megabytes sending the file. If the material will be more than 70 megabytes, please contact Danske Bank's Software and material transfer support before sending the material(see chapter 5).

4.4 Retrieving material

When the customer retrieves materials, the Bank signs the message using its own secret key and encrypts the material using the customer's public key.

The materials listed below can be retrieved via Danske Bank's Web Services.

C2BN pain.002.001.02 pain.002.001.03	Status report ISO 20022, pain.002.001.02 ja 03 Status report ISO 20022, pain.002.001.02 Status report ISO 20022, pain.002.001.03 Status report is formed automatically of the transmission of XML-payments, version, version 02 or 03.
camt.052.001.02	XML balance and transaction query
camt.053.001.02	XML account statement
camt.054.001.02	XML reference number and payment list
camt.054.001.02	XML feedback for cross-border transfers
APSN	Balance inquiry
FILN	E-invoice retrieval
FIVN	E-invoice error list
FIRN	E-invoice receiver
IBAN	IBAN account number conversion
KTON	Electronic account statement
MCT	MasterCard Corporate Card transaction
SWFN	SWIFT MT940 account statement
TAPN	Transaction inquiry
UM2N	Feedback of Foreign Payments
USEN	Advance information of Foreign payments
VIPN	Reference Transaction list
VKEN	Foreign Exchange Rate

In addition to the above materials Danske Bank's Web Service also supports the Danske Bank Group's local data formats. You can find the list of data formats in section 4.5 Web services Channel Technical Description.

4.5 Technical descriptions

For technical descriptions, see the following links:

Description of the Web Services protocol and escription of the encryption and compression of Web Services messages

Integration Services/Web Services

Description of PKI Web Services

PKI Service Description

4.6 Testing

The customer and the generator of the software may test the service in a production enviroment. The testing requires the conclusion of an agreement on Web Services link protocol and PKI Security Solution.

The customer and the generator of the sowftware may use the 'TEST' value in the service request for the XML material to be sent to the bank in the element (ApplicationRequest)<EnviromentID> whereby the bank will control the correctness of the payment material, but shall not book the payments. Please observe that the use of the TEST value concerns only ISO20022 -material (pain.001). If it is used in other payment files the payments shall be processed and booked in the usual way.

5. Help and support

The contact information of Danske Bank's Corporate Service is available here