Danske Bank

Web Services implementation overview

Two sets of Web Services

PKI Web Services
- Create, revoke and manage certificates

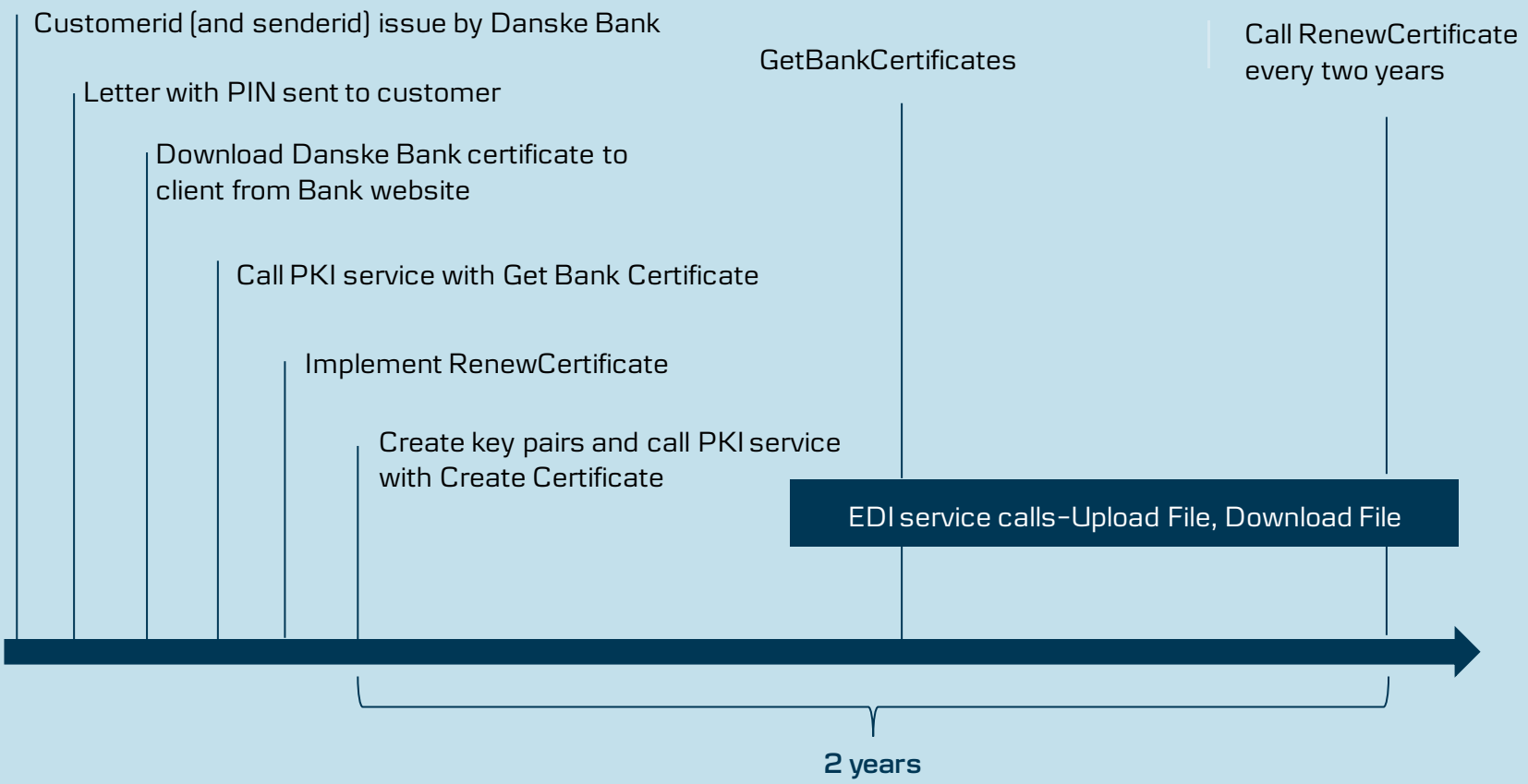
EDI Web Services
- File transmissions to and from the bank

Implementation steps

Steps

1. Customer id (and sender id) issued by Danske Bank
2. Letter with PIN sent to customer
3. Download Danske Bank root certificate to client from bank website
4. Call PKI service with GetBankCertificate
5. Create key pairs and call PKI service with CreateCertificate
6. Implement RenewCertificate and other PKI functions needed in the future
7. Call EDI service with Upload/Download File
8. Call RenewCertificate (Every two years)
9. Call GetBankCertificates (before old certificate expires, every two years)

Timeline of implementation and calls



Steps 1-3 – Preliminary steps

Customer id (and sender id) issued by Danske Bank

- Onboarding to our Web Services channel requires a technical Web Service user on customer's District agreement. Advisor or Cash Manager orders the Web Service user
- The userid of the Web Service user is the same, which applies in CustomerId and SenderId in the Web services requests

Letter with PIN sent to you

- As soon as the Web service user is created, a letter with PIN code is sent to you. The PIN must be used the first time you call PKI Web Service with CreateCertificate request

Get Bank Root Certificate

- Download Bank Root Certificate from the danskeci website. Verify it using jarsigner

Steps 4-6 – PKI Web Services overview (1/2)

GetBankCertificate (unsigned and unencrypted)

- Returns the current bank certificates. You will use it to encrypt your messages to the bank and to verify the signature of messages from the bank

CreateCertificate (unsigned)

- Create customer certificates based on customer PKCS#10 request and the PIN code you received in step 2 above. You have to encrypt this message, using the public bank certificate you obtained in the previous call

RenewCertificate

- Issues new customer certificates based on PKCS#10 request and previous certificate. You need to call this function before the expiry of your current certificate, in other words, every two years. You have to both sign this message with your current certificate, and encrypt it using the bank certificate

PKI Web Services overview (2/2)

RevokeCertificate

- Revoke an active customer certificate (in case your key, associated to this certificate gets compromised or lost)

GetCertificateStatus

- Create customer certificates based on customer PKCS#10 request and the PIN code you received in step 2 above. You have to encrypt this message, using the public bank certificate you obtained in the previous call

GetCertificateList

- Returns list of active certificates belonging to the user

The three calls from the previous page are sufficient to secure your communication with the bank. After them you can move immediately to implementing EDI Web Services. However, these three calls are also good to have, and especially the top one is necessary if your key gets compromised

Step 7 – EDI Web Services overview

UploadFile
- Upload file to Danske Bank

DownloadFileList
- Returns list of file descriptors at Danske Bank matching call parameters

DownloadFile
- Returns file(s) matching wanted file descriptor

Development and testing

Secure web services
- Note several layers of signing and encryption
- Use standard libraries for signing and encryption

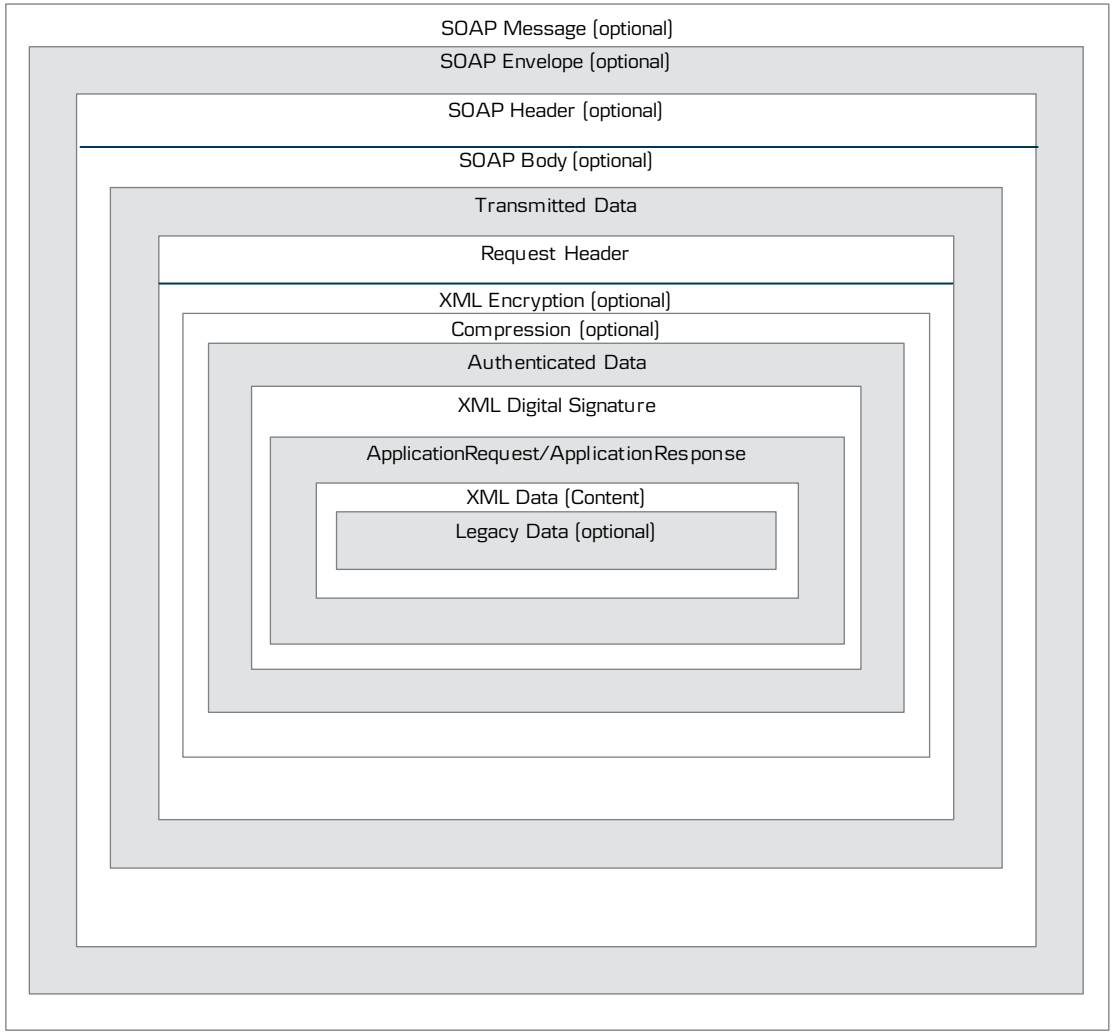
Testing PKI Web Services
- The real PIN can only be used once
- Use the 'customertest' option – A test environment to use when you are creating the integration to the PKI Web Services, which returns predefined values to calls
- Production certificates must be used for testing

Testing EDI Web Services – Only applies to payment files
- Use 'TEST' option in Environment field to test mark payment files
- Payment files are validated but not executed
- If ordered – Feedback files will be created and available for download

Request structure

Layers

- Application Request
- Customer signature
- Compression (optional)
- Encryption
- Add Request Header
- Add SOAP body and header
- Transport signature
- Transmit file using HTTPS



Technology

Implementing Web Services towards danske bank requires knowledge of the following subjects

- **XMLDSIG – XML Signature Syntax and Processing (Second Edition)**
  http://www.w3.org/TR/xmldsig-core1/
- **XML Encryption – XML Encryption Syntax and Processing**
  http://www.w3.org/TR/xmlenc-core/
- **X.509v3 – Internet X.509 Public Key Infrastructure Certificate and CRL Profile**
  http://tools.ietf.org/html/rfc5280
- **PKCS #10 – Certification Request Syntax Specification Version 1.7**
  http://tools.ietf.org/html/rfc2986
- **SOAP – Simple Object Access Protocol**
  http://www.w3.org/TR/soap/
- **WSDL – Web Services Description Language (WSDL) 1.1**
  http://www.w3.org/TR/wsdl

Support and help

We can help with questions about the calls to the service, with xml formatting, with testing and errors

Contact
Integration Services
Integration-Services@danskebank.com