2016-07-05

Bg Link 2.0

Programmer’s Guide

2.0.7

Postadress: 105 19 Stockholm | Besöksadress: Palmfeltsvägen 5 |Webb: bankgirot.se | Bankgironr: 160-9908
Styrelsens säte: Stockholm | Växel: 08-725 60 00 | Org.nr: 01-556047-3521 | VAT No. SE556047352101

Contents

Revision history

Version	Date	Author	Comment
0.1	2013-12-18		First draft
2.01	2014-05-27		Sequence number removed from RequestContext.
2.0.3	2014-09-05		Certificate handling
2.0.5	2014-10-14		Service address updated in the example configuration.
2.0.6	2016-05-31		Added certificate type for mobile BankID.
2.0.7	2016-07-05	Kenneth Jansson	Revised version.

References

No	Document	Description
1	BankID Relying Party Guidelines	Description and implementation guidelines for the BankID's central server solution. The relying party guideline can be found at: http://bankid.com/rp/info
2	Bg Link 2.0 - Service Interface	Description of the web service interface.

1 General idea

Bg Link 2.0 is a completely rebuilt version of Bg Link 1.2 built in .NET 4.5 and runs on Windows Server 2012. The interface has been updated, but the principles are the same.

In Bg Link 2.0 the new BankID central server solution is implemented as a part of Bg Link. The client application starts the BankID client itself but authentication, signing and polling is done through Bg Link 2.0. To fully understand the BankID authentication and signing solution see “BankID Relying Party Guidelines” [ref 1].

2 Requirements

To consume the Bg Link service the client must setup the service binding to enable secure conversation between itself and the Bg Link service. The user needs also a BankID compatible certificate to be able to logon to the service.

2.1 Certificate handling

The Bg Link service uses the authentication mode “AnonymousForSslNegotiated” for initializing the secure conversation. In this mode, the client is anonymous and the service is authenticated by an X.509 certificate that is negotiated at runtime, the certificate is sent over SSL to the client. Example configuration can be found at the end of this document in section 6 – Example Client Configuration.

2.1.1 Test environment specific configuration

When communicating with the test environment which is using a self-signed certificate, then some extra configuration is needed at the client side in order to establish the secure channel. CertificateValidationMode must be set to “None” and revocationMode must be set to “NoCheck” in the clientCredentials/serviceCertificate tag. This configuration **MUST** however be removed when communicating with the production server, since it reduces the security.

```
<behaviors>
  <endpointBehaviors>

    <behavior name="MessageTransportBehavior">
      <clientCredentials>
        <serviceCertificate>
          <authentication certificateValidationMode="None" revocationMode="NoCheck"/>
        </serviceCertificate>
      </clientCredentials>
    </behavior>
  </endpointBehaviors>
</behaviors>
```

2.2 BankID certificates

For a BankID certificate to be valid for use with Bg Link the certificate OID or SERIALNUMBER must be listed below. Except for the OID to be correct the issuer must also be approved by the Bank for which the user has user rights on. BankID has a test environment which can be used for test purposes. See “BankID Relying Party Guideline” [ref 1] for instructions regarding how to setup the BankID client application to run towards the test environment. BankID test certificates can be downloaded from: https://demo.bankid.com/nyademobanken/.

The following certificate types are allowed:

OID (Test)	OID (Prod)	Description
1.2.752.71.*	1.2.752.71.*	All Nordea BxID and eID
1.2.752.60.*	1.2.752.60.*	BgID + test BankID on file. Customer test environment.
1.2.3.4.*	1.2.752.81.*	BxID SHB
1.2.3.4.*	1.2.752.103.*	BxID SEB
1.2.3.4.25	1.2.752.78.1.5	Mobile BankID

3 Responsibilities

The responsibilities for the client and the service is listed in this section but more information about the different flows and operations can be found under section 4 - Flow charts and section 5 - Interface.

3.1 Web service communication

3.1.1 Client Application

The client application is responsible for sending a correct request context with each call. The context shall include MessageId, ProgramId, SessionId and Timestamp. The only exception is when calling the operation Logon where the SessionId is not mandatory and will be ignored if set. The SessionId that shall be included with all following requests to the Bg Link Web Service is returned as a part of the Logon response.

The client application is responsible for checking the status of each response from Bg Link Web Service. A response can have status ACK (ok) or NACK (not ok). If status is NACK the fault object in the response context is set with an error code and a message.

3.1.2 Bg Link Web Service

The Bg Link Web service is responsible for validating all requests and for sending the correct status in the response together with either a fault object or a response object. Bg Link is responsible for handling data that should live between calls such as file data during signing.

3.2 BankID processes

3.2.1 Client Application

The client starts the authentication and signing process by calling the described operations in Bg Link. Bg Link returns the autoStartToken and order reference from the BankID's central server. The client starts the BankID client application with the autoStartToken and then polls for the status of the authentication/signing. The polling is done once every 2 seconds until Status COMPLETE is returned. When COMPLETE is returned the client also knows that the authentication/signing process is fully complete.

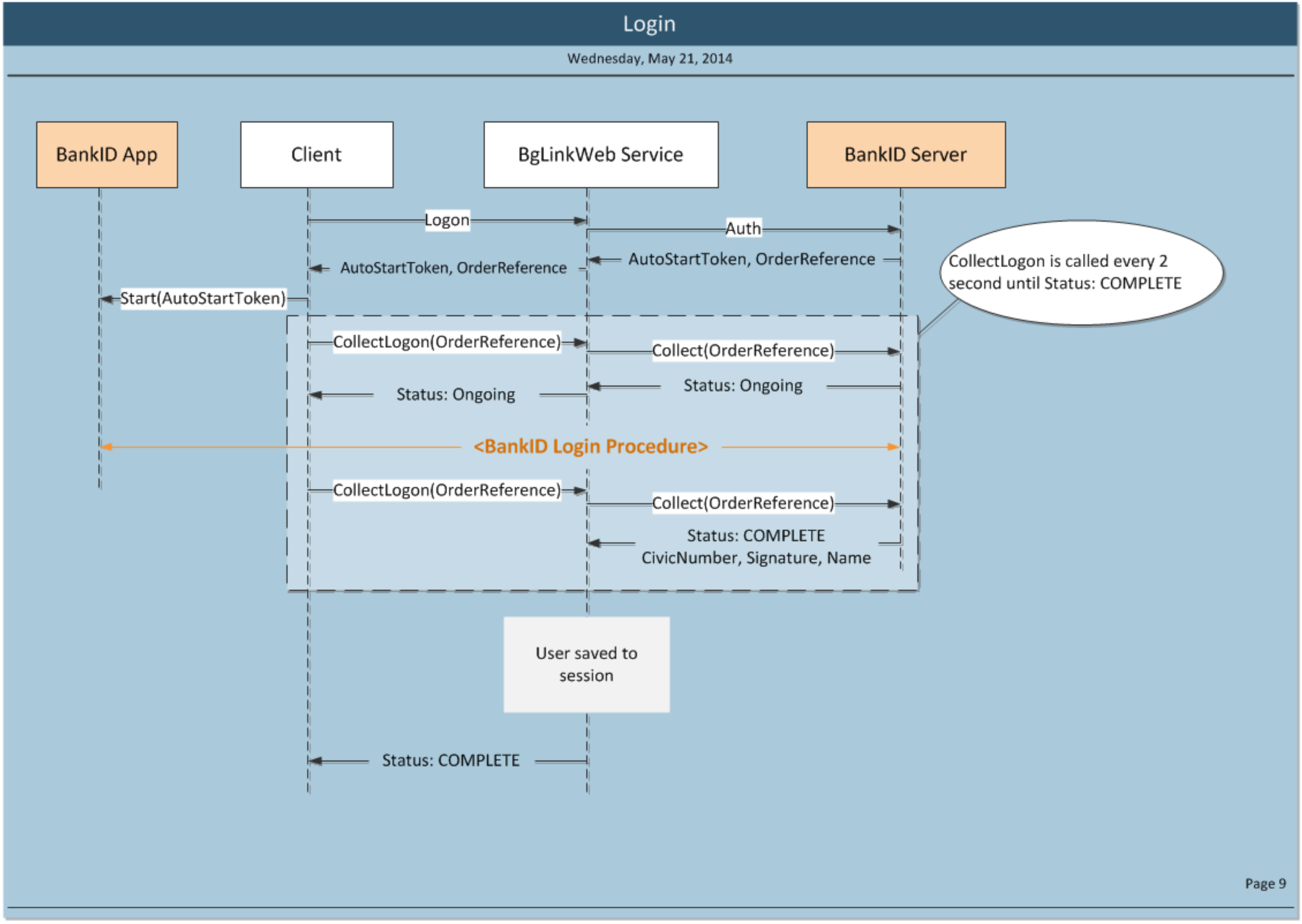
3.2.2 Bg Link Web Service

The Bg Link Web Service handles all communication with BankID's central server.

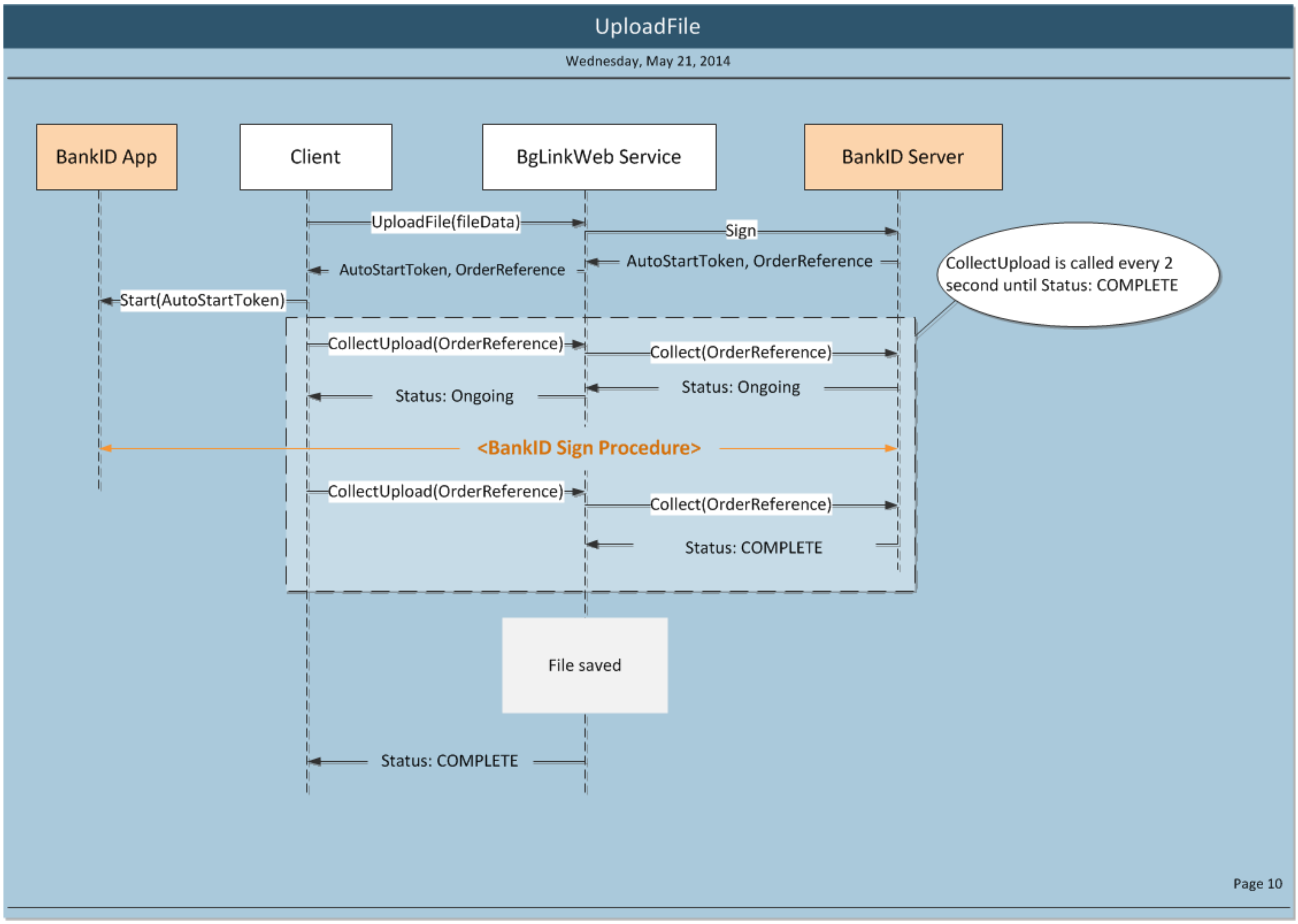
4 Flow charts

The main flows are described in this section. Other flows such as getting a list of uploaded files are not described here and are straight forward single calls.

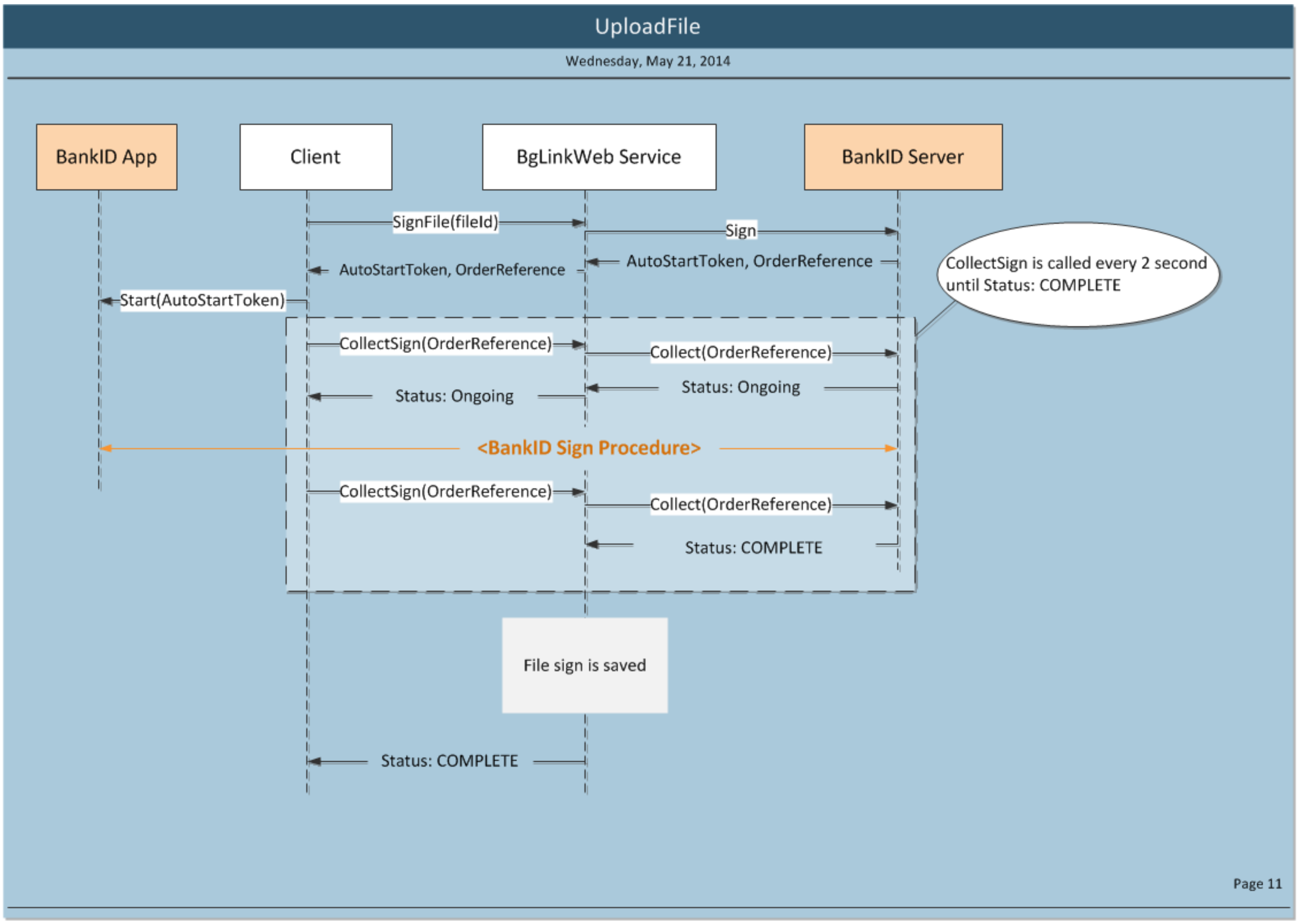
4.1.1 Login


Login
Wednesday, May 21, 2014
BankID App
Client
BgLinkWeb Service
BankID Server
Logon
Auth
AutoStartToken, OrderReference
AutoStartToken, OrderReference
Start(AutoStartToken)
CollectLogon is called every 2 second until Status: COMPLETE
CollectLogon(OrderReference)
Collect(OrderReference)
Status: Ongoing
Status: Ongoing
<BankID Login Procedure>
CollectLogon(OrderReference)
Collect(OrderReference)
Status: COMPLETE
CivicNumber, Signature, Name
User saved to session
Status: COMPLETE
Page 9

4.1.2 Upload file



4.1.3 Sign file



5 Interface

The interface will not be described here. For a complete interface reference see “Bg Link 2.0 - Service Interface” [ref 2].

6 Example Client Configuration

Below is an example client configuration for communicating with Bg Link Web Service.

```
<system.serviceModel>

    <serviceHostingEnvironment aspNetCompatibilityEnabled="true" />

    <bindings>
      <customBinding>

        <!-- Bg Link Service Binding -->
        <binding name="BgLinkBinding" sendTimeout="00:10:00">
          <reliableSession />
          <security defaultAlgorithmSuite="Basic256Sha256" authenticationMode="SecureConversation"
                    requireDerivedKeys="true" includeTimestamp="true"

messageSecurityVersion="WSSecurity11WSTrustFebruary2005WSSecureConversationFebruary2005WSSecurityPolic
y11BasicSecurityProfile10"
                    requireSignatureConfirmation="false" canRenewSecurityContextToken="true">
            <secureConversationBootstrap defaultAlgorithmSuite="Basic256Sha256"
                authenticationMode="AnonymousForSslNegotiated" requireDerivedKeys="true"
                includeTimestamp="true"

messageSecurityVersion="WSSecurity11WSTrustFebruary2005WSSecureConversationFebruary2005WSSecurityPolic
y11BasicSecurityProfile10"
                requireSignatureConfirmation="true">
              <localClientSettings detectReplays="true" />
              <localServiceSettings detectReplays="true" />
            </secureConversationBootstrap>
            <localClientSettings detectReplays="true" />
            <localServiceSettings detectReplays="true" />
          </security>
          <textMessageEncoding>
            <readerQuotas maxDepth="500000000" maxStringContentLength="500000000"
maxBytesPerRead="500000000"
                          maxNameTableCharCount="500000000" maxArrayLength="500000000" />
          </textMessageEncoding>
          <httpsTransport requireClientCertificate="false" maxBufferSize="500000000"
maxReceivedMessageSize="500000000" />
        </binding>

      </customBinding>
    </bindings>


    <client>

      <!-- Bg Link Endpoint -->

<endpointaddress="https://www.bt.bglinkws.bgonline.se/WebService/BgLinkService.svc"
                binding="customBinding" bindingConfiguration="BgLinkBinding"
                contract="BgLinkServiceReference.IBgLinkService"
                name="CustomBinding_IBgLinkService" >
        <identity>
          <dns value="…"/>
        </identity>
      </endpoint>

    </client>
  </system.serviceModel>
```