1 Introduction .......................................................................................................................... 4
  1.1 Versions .............................................................................................................................. 4
  1.2 Terms and Definitions ......................................................................................................... 5
  1.3 How it Works ....................................................................................................................... 5
  1.4 Client Platforms ................................................................................................................. 5
2 Use Cases .................................................................................................................................. 5
  2.1 Basic Use Cases .................................................................................................................. 5
  2.2 Flow of Events .................................................................................................................... 6
  2.3 Exceptions .......................................................................................................................... 6
3 Launching .................................................................................................................................. 7
  3.1 Launching the BankID app from a Browser ........................................................................ 7
    3.1.1 Behaviour in Different Browsers .................................................................................... 7
    3.1.2 Parameters in the Start URL ....................................................................................... 7
  3.2 Launching the BankID app from Native App on Mobile Device ........................................ 8
    3.2.1 Android ....................................................................................................................... 8
    3.2.2 iOS ............................................................................................................................... 8
    3.2.3 Windows 10 Mobile ...................................................................................................... 9
4 QR codes .................................................................................................................................. 9
5 Technical Requirements .......................................................................................................... 10
6 Recommended User Messages ................................................................................................ 10
7 Production Environment ......................................................................................................... 14
8 Test Environment ..................................................................................................................... 15
9 Information Regarding the Web Service API .......................................................................... 16
  9.1 SSL Certificates ................................................................................................................ 16
  9.2 appapi and appapi2 .......................................................................................................... 16
  9.3 Versions ............................................................................................................................ 16
    9.3.1 Breaking Change ........................................................................................................ 16
  9.4 Test Environment .............................................................................................................. 17
  9.5 HTTP/1.1 ........................................................................................................................ 17
  9.6 TLS Versions ...................................................................................................................... 17
10 Support .................................................................................................................................. 17
  10.1 Developer Support ............................................................................................................ 17
  10.2 End User Support ............................................................................................................. 17
11 Recommended Terminology .................................................................................................... 17
12 File Signing ............................................................................................................................. 18
13 Verifying Signatures ............................................................................................................... 18
14 RP Interface Description ....................................................................................................... 19
  14.1 /rp/v5/auth and /rp/v5/sign ............................................................................................... 19
    14.1.1 Parameters for auth and sign ..................................................................................... 19
    14.1.2 Additional Parameters for sign .................................................................................. 19
    14.1.3 Response from auth and sign .................................................................................... 19
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>14.2</td>
<td>/rp/v5/collect</td>
<td>20</td>
</tr>
<tr>
<td>14.2.1</td>
<td>Parameters for collect</td>
<td></td>
</tr>
<tr>
<td>14.2.2</td>
<td>Response from collect</td>
<td></td>
</tr>
<tr>
<td>14.2.3</td>
<td>hintCode for Pending Orders</td>
<td></td>
</tr>
<tr>
<td>14.2.4</td>
<td>hintCode for Failed Orders</td>
<td></td>
</tr>
<tr>
<td>14.2.5</td>
<td>completionData for Completed Orders</td>
<td></td>
</tr>
<tr>
<td>14.3</td>
<td>/rp/v5/cancel</td>
<td>23</td>
</tr>
<tr>
<td>14.3.1</td>
<td>Parameters for cancel</td>
<td></td>
</tr>
<tr>
<td>14.3.2</td>
<td>Response from cancel</td>
<td></td>
</tr>
<tr>
<td>14.4</td>
<td>Errors</td>
<td>23</td>
</tr>
<tr>
<td>14.5</td>
<td>Requirement</td>
<td>24</td>
</tr>
<tr>
<td>14.5.1</td>
<td>Example – allowFingerprint for sign</td>
<td>25</td>
</tr>
<tr>
<td>14.5.1</td>
<td>Example – certificatePolicies for auth with Mobile BankID</td>
<td>25</td>
</tr>
<tr>
<td>14.5.1</td>
<td>Example – Combined Requirements</td>
<td>25</td>
</tr>
</tbody>
</table>
1 Introduction

This document contains guidelines for Relying Parties (RP, Förlitande Part in Swedish) when using BankID in their own services. Please check https://www.bankid.com/bankid-i-dina-tjanster/rp-info and verify that you have the latest version of this document.

Note: To manage a generation shift of the root certificate protecting the service we have introduced a new end point for the service; appapi2.bankid.com. This new end point is protected using a new root CA. RP must use the new end point. RP must trust the new root CA. The old end point will not work after June 2019.

Note: This document describes the new JSON interface. The old SOAP interface is described in previous version of this document. Please check https://www.bankid.com/bankid-i-dina-tjanster/rp-info if you need the old version.

1.1 Versions

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.x</td>
<td></td>
<td>Historical versions. Please contact <a href="mailto:teknikinfo@bankid.com">teknikinfo@bankid.com</a> if you need this information.</td>
</tr>
<tr>
<td>&lt;2.10</td>
<td></td>
<td>Recommended User Messages: The term “BankID app” may be used for the PC client. RequirementAlternativesType: Support for fingerprint sensors added. Versions: Reduced the version history. Editorial.</td>
</tr>
<tr>
<td>2.10</td>
<td>2016-02-23</td>
<td>Description of fileSign removed (deprecated). Versions: Reduced the version history. Editorial and minor improvements.</td>
</tr>
<tr>
<td>2.11</td>
<td>2016-09-29</td>
<td>Windows 10 Mobile support added. Windows Phone 8 support removed. iOS example code updated. Now using Swift.</td>
</tr>
<tr>
<td>2.12</td>
<td>2016-10-14</td>
<td>More occurrences of Windows Phone changed to Windows 10 Mobile and contents corrected accordingly where needed.</td>
</tr>
<tr>
<td>2.13</td>
<td>2016-10-26</td>
<td>A new url must be used to access the service (appapi2.bankid.com). A new issuer certificate must be used as trusted issuer to be able to access appapi2.bankid.com appapi2.bankid.com accepts only TLS1.1 and TLS1.2. Fingerprint supported for Android. Fingerprint supported for signing by using requirementAlternatives. Editorial and minor improvements.</td>
</tr>
<tr>
<td>2.14</td>
<td>2017-02-07</td>
<td>Version 5 of the service introduced. JSON replaces XML/SOAP A cancel method introduced Recommendation to start the iOS app using universal links. New IP addresses for the test environment. Description of how breaking changes are managed in the API. Editorial and minor improvements.</td>
</tr>
<tr>
<td>2.15</td>
<td>2017-03-21</td>
<td>The parameter autostarttoken for iOS was wrong.</td>
</tr>
<tr>
<td>2.16</td>
<td>2017-11-14</td>
<td>An upcoming change of IP addresses to access the service added.</td>
</tr>
<tr>
<td>3.1</td>
<td>2018-06-13</td>
<td>Support for QR codes. A clarification related to the default behaviour for the autoStartTokenRequired requirement.</td>
</tr>
<tr>
<td>3.2</td>
<td>2018-09-03</td>
<td>Minor editorial.</td>
</tr>
</tbody>
</table>
1.2 Terms and Definition

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BankID Security Application</td>
<td>The client software that needs to be installed in the end users mobile device or personal computer (PC). The same term is used for PCs and mobile platforms.</td>
</tr>
<tr>
<td>BankID app</td>
<td>BankID app is the short form used in this document. In Swedish the client software installed on PCs is called “BankID säkerhetsprogram”, ”BankID-programmet” or “BankID-appen”.</td>
</tr>
<tr>
<td>BankID</td>
<td>In Swedish the client software installed on mobile platforms is called “BankID säkerhetsapp” or “BankID-appen”</td>
</tr>
<tr>
<td>RP</td>
<td>Relying Party that uses the BankID web service to provide authentication and signing functionality to the end user.</td>
</tr>
</tbody>
</table>

1.3 How it Works
To be able to use BankID’s identification and signature features users must install the BankID app in a mobile device or PC. They also need to order a BankID from their bank. An RP uses the BankID identification or signature services via a web service API described in this document. The web service API can only be accessed by a RP that has a valid SSL client certificate. The RP certificate is obtained from the bank that the RP has purchased the BankID service from.

If the BankID app is installed on the same device as the RP service executes in, the BankID app can be launched automatically by the RP service. In this case, the users do not need to enter their personal number in the RP service. If, on the other hand, the RP service is used in a web browser on a PC and the users want to use a Mobile BankID the users will have to manually launch the BankID app on their mobile device. In this case, the users need to provide their personal number in the RP service.

1.4 Client Platforms
BankID is available for Windows, macOS, Android, iOS and Windows 10 Mobile platforms. Smartcards are supported for Windows and macOS only. Detailed information on platform support can be found at https://support.bankid.com.

2 Use Cases
There are a number of use cases that can be implemented using the BankID solution. In this document, we describe the most common use cases to keep it simple and to give the reader a basic understanding of the solution.

- If the BankID app is installed on another device than the user uses to access the service, and the RP supports QR code, the users must manually start their BankID app and scan the QR code. In this case, the users do not need to provide their personal number.
- If the BankID app is installed on another device, and the RP does not support QR code, the users must provide their personal number and manually start the BankID app.
- If the BankID app is installed on the same device the user uses to access the service, the RP should help the user to start the BankID app automatically. In this case, the users do not need to provide their personal number.
- If the BankID app is installed on the same device, but the BankID app cannot be automatically started, the user must provide their personal number and manually start the BankID app on the same device. RPs should consider this use case as a fallback in case the automatic start fails.

To make the user experience consistent the RP should use the recommended messages and error messages in Recommended User Messages.

The possibilities to restrict the type of BankID that can be used and how to define other requirements are described in Requirement.

2.1 Basic Use Cases
The following basic use cases exist:

A. The user access the service using a browser on a personal computer. Users should be asked if they want to login or sign using “BankID on this computer” or “Mobile BankID”. Message RFA19 should be used.
a. Users that select to use BankID on this computer does not need to enter their personal number and the RP must start the BankID app on the computer. See chapter Launching.
b. Users that select Mobile BankID, and the RP does not support QR code, must enter their personal number start the BankID app manually on their mobile device.
c. Users that select Mobile BankID, and the RP supports QR code, must start their BankID app manually on their mobile device and scan the QR code.

B. The user access the service using a browser on a mobile device. Users should be asked if they want to login or sign using “Mobile BankID on this device” or “Mobile BankID on another device”. Message RFA20 should be used.
   a. Users that select to use this device do not need to enter their personal number and the RP must start the BankID app on the mobile device. See chapter Launching.
b. Users that select to use another device, and the RP does not support QR code, must enter their personal number and start the BankID app manually on the other device.
c. Users that select to use another device, and the RP supports QR code, must start their BankID app manually on the other device and scan the QR code.

C. The user access the service using a native app on a mobile device. In this case, the user most likely wants to use a BankID on the same device. The RP may however provide possibilities to use another device in this case as well.
   a. The users do not need to enter their personal number and the RP app launches BankID App programmatically (see Launching the BankID app from Native App on Mobile Device).
b. Users that select to use another device, and the RP does not support QR code, must enter their personal number and start the BankID app manually on the other device.
c. Users that select to use another device, and the RP supports QR code, must start their BankID app manually on the other device and scan the QR code.

In some cases, it may be impossible to start the BankID app automatically. The reason could be browsers blocking it or that the RP app does not have the capabilities to launch external URL:s. In this case, the users can always start the BankID app manually. In this case, the users need to enter their personal number.

2.2 Flow of Events
   1. Users that select “another device” are asked to enter their personal number, if it’s not already saved or known by the RP. As an alternative to entering personal number, the RP may support QR codes that the user scans.
   2. The RP uses the auth or sign method of the web service API to initiate the order. The web service returns an autoStartToken and an orderRef. If the user selected “another device”, RP should set condition certificatePolicies to “1.2.752.78.1.5” to restrict the order to Mobile BankID only.
   3. If the user selected “same device” the RP tries to start the BankID app. The autoStartToken must be used in the start command if the personal number is not provided in the web service call, see Launching. Once the BankID app has finished execution, focus will be returned to the browser/app.
   4. If the user selected “another device”, the RP informs the user to start the BankID app manually.
   5. If the RP supports QR code, the RP creates a QR code based on the autoStartToken, which the user scans.
   6. The RP service displays a progress indicator.
   7. The auth or sign order is displayed in the BankID app. The RP name (as stated in the RP certificate) is displayed. The user enters personal security code or cancels the order.
   8. The RP periodically uses the collect method of the web service API, until a final response is received and continuously updates the message displayed to the user. See Recommended User Messages.
   9. RP removes the progress indicator.

2.3 Exceptions
   1. The web service call in step 2 fails. The use case is cancelled and the RP shall instruct the user according to Recommended User Messages. The RP must not try to start the BankID app.
   2. The collect call in step 8 fails. The use case is cancelled and RP shall instruct the user according to Recommended User Messages.
   3. The automatic start in step 3 fails due to different reasons:
      - The user has not installed the BankID app
      - Erroneous start command
      - User did not allow the browser to launch the URL
The web browser will inform the user that the URL cannot be opened. hintCode “startFailed” will be returned to the RP as response to the collect call in step 8 if the automatic start of the BankID app has not been completed within a certain time limit (30 seconds). The RP shall instruct the user according to Recommended User Messages.

4. The automatic start in step 3 is successful but the user has no BankID of correct type. The BankID app will display an error message. hintCode “started” will be returned to the RP as response to the collect call in step 8. RP shall instruct the user according to Recommended User Messages.

5. In step 4, the user fails to start the BankID app manually or no BankID of correct type exists in the started client. Different hint codes will be delivered to RP as response to the collect call in step 8. The RP shall instruct the user according to Recommended User Messages.

6. In step 8, the user fails to complete the operation within the time limit (3 minutes). hintCode “expiredTransaction” is returned from collect.

7. In step 8, the RP decides to cancel the order using the cancel method. The user is informed that the order was cancelled in the BankID app.

8. In step 5, the user fails to scan the QR code. hintCode “startFailed” will be returned to the RP as response to the collect call in step 8 if the QR code has not been scanned within a certain time limit (30 seconds). The RP shall instruct the user according to Recommended User Messages.

3 Launching

3.1 Launching the BankID app From a Browser

The URL syntax is:

```
bankid:///?autostarttoken=[TOKEN]&redirect=[RETURNURL]
```

The URL works on Android, iOS and Windows 10 Mobile when the built-in web browser is used. The URL works on PCs with all commonly used browsers. Some differences exist on different platforms.

On iOS the preferred URL syntax is:

```
https://app.bankid.com/?autostarttoken=[TOKEN]&redirect=[RETURNURL]
```

**Note** that the redirect parameter must be last in the parameter list. The autostarttoken and rpref parameters are optional.

**Note** that the parameter names must be lower case.

**Note** that if the BankID app is started but no matching web service call to auth or sign has been done, an error message will be displayed in the app.

3.1.1 Behaviour in Different Browsers

3.1.1.1 Internet Explorer

Internet Explorer manipulates the URL in the redirect parameter. In this specification, we state that the RETURNURL must be URL encoded. However, Internet Explorer decodes the content prior passing it to the BankID app. This is why it must be last in the list of parameters. In the same way, Internet Explorer may decode the content of the RETURNURL when the BankID app passes the return URL back to the browser. If the RP includes session information that is affected by URL encoders/decoders, problems may occur. It is recommended to use only URL encoding safe characters in the parameters.

3.1.2 Parameters in the Start URL

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>autostarttoken</td>
<td>Optional. Holds the autoStartToken that was returned from the web service call. If the user personal number was not included in the web service call the autostarttoken must be provided. We strongly recommend to always use the autostarttoken when the URL is used to start the client. If it is not included and the user reloads the page or if the page erroneously repeats the start command, the user may get an error claiming that the BankID is missing. The likelihood of this to happen is reduced if autostarttoken is used. <strong>Note</strong> that the parameter names must be lower case.</td>
</tr>
<tr>
<td>Redirect</td>
<td>Required.</td>
</tr>
</tbody>
</table>
The BankID app uses the parameter redirect to launch the RP web app after completed (including cancelled) auth or sign. The redirect URL must be UTF-8 and URL encoded and should match the web address the user is visiting when RP web app launches the BankID app. It may include parameters to be passed to the browser. For iOS the redirect must have a value. For all other platforms it may be empty (“redirect=”), or set to “null” (“redirect=null”). If it is empty or null the BankID app will terminate without launching any URL and the calling application will be in focus. The general recommendation is to use redirect=null when it is possible.

Note for Windows and macOS
If redirect has a value the redirect parameter must be used together with autostarttoken.
If autostarttoken is excluded, the content of redirect will be ignored and the behavior will be as if redirect=null.

Note for Android
If the user has several browsers installed on an Android device the user is sometimes presented with a question asking what browser to use. BankID recommends that redirect=null is used on Android. This ensures the user will return to the browser previously used.

rpref
Optional.
Relying Party Reference. Not supported in mobile devices.
Any reference the RP wants to use. The value will be included in the resulting signature. A typical use case is to protect a file when it is transported from a client to a server (compute hashsum of the file content in the client, include the hashsum as rpref, compare it (server side) with a hashsum of the file content computed in the server). The value must be base64 encoded, URL encoded, and 8–255 bytes (after encoding). rpref must be used together with autostarttoken. If autostarttoken is excluded, the content of rpref will be ignored.

3.1.2.1 Examples
The RP wants the BankID app to open a browser with the following URL after finishing execution:
https://demo.bankid.com/nyademobanken/CavaClientRedirectReceiver.aspx?orderRef=bedea56d-7b46-47b1-890b-f787c650be93&returnUrl=./CavaClientAuth.aspx&Environment=Kundtest. The autostarttoken is included. The start URL is:
bankid:///?autostarttoken=a4904c4c-3bb4-4e3f-8ac3-0e950e529e5f&redirect=https%3a%2f%2fdemo.bankid.com%2fnyademobanken%2fCavaClientRedirectReceiver.aspx%3forderRef%3dbedea56d-7b46-47b1-890b-f787c650be93%26returnUrl%3d%2fCavaClientAuth.aspx%26Environment%3dKundtest

3.2 Launching the BankID app from Native App on Mobile Device
3.2.1 Android
Intent intent = new Intent();
intent.setPackage("com.bankid.bus");
intent.setAction(Intent.ACTION_VIEW);
intent.setData(Uri.parse("bankid:///?autostarttoken=<INSERT AUTOSTARTTOKEN HERE>&redirect=null "));
startActivity(intent);

A valid result is not guaranteed to be returned back from the BankID app to the RP app's Activity. The RP app should rely on the collect call to obtain the result of the auth or sign order. If the BankID app is not present on the device, an android.content.ActivityNotFoundException is thrown. RP must inform the user. Message RFA2 should be used.

3.2.2 iOS
let url = URL(string: "https://app.bankid.com/?autostarttoken=<INSERT AUTOSTARTTOKEN HERE>&redirect=<INSERT YOUR LINK HERE>")
UIApplication.shared.open(url!, options: [:]) { (success) in
  // handle success/failure
}

If the BankID app is not present on the device false is returned. RP must inform the user. Message RFA2 should be used.
The RP app must register a Universal Link or a custom URL scheme to make it possible for the BankID app to re-launch RP app.
3.2.3 Windows 10 Mobile

In Visual Studio:
1. Open Package.appxmanifest
2. Open the tab Declarations.
3. Add a "Protocol". Under name enter "rp-app-x".
4. Enter a logo and a "Display name".

Note: rp-app-x is an example; RP should use its own unique URL scheme.

Handle the activation by overriding OnActivated in App.xaml.cs.

```csharp
protected override void OnActivated(IActivatedEventArgs args) {
if (args.Kind == ActivationKind.Protocol) {
    ProtocolActivatedEventArgs ProtocolArgs = args as ProtocolActivatedEventArgs;
    rootFrame = new Frame();
    rootFrame.Navigate(typeof(MainPage), args);
}
Window.Current.Activate();
}
```

4 QR codes

In September 2018, support for QR codes was introduced. The RP service generates a QR code based on the autoStartToken, presents the QR code to the user and asks the user to scan it using the BankID app. If this is successful, the BankID app will automatically proceed with the identification or signature operation.

The typical use case is when the user uses “Mobile BankID on another device” (see use cases above), and there is a security concern that the user does not control both devices. When QR codes are used, the user does not need to provide their personal number.

Note: If personal number is included in the call to the service, RP must consider setting the requirement autoStartTokenRequired to true. By this, the system enforces that no other device than the one started using the QR code is used.

The QR code is generated using the following as input:

```
bankid:///?autostarttoken=[TOKEN]
```

- The redirect parameter must not be included.
- The rpref parameter must not be included.
- The url must not be URL-encoded
- The error correction level can be kept to a minimum. The code is supposed to be read from the screen.
- Colors in the QR code should be kept to a minimum, we recommend to use black.
- Use sufficient margins.
- Avoid to include other information or graphics in the QR code (example layered logotypes)

If the user fails to scan the QR code within the time limit, hintCode “startFailed” will be returned to the RP as response to the collect call. The RP shall instruct the user according to Recommended User Messages.

Example

Input bankid:///?autostarttoken=46f6a68-a520-49d8-9be7-f0726d038c26

Result:
5 Technical Requirements

<table>
<thead>
<tr>
<th>Short Name</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFT1</td>
<td>When the BankID app is launched with a URL the content of the parameter redirect must be UTF-8 and URL encoded.</td>
</tr>
<tr>
<td>RFT2</td>
<td>When the BankID app is launched with a URL the URL must not exceed 2000 characters.</td>
</tr>
<tr>
<td>RFT3</td>
<td>When the BankID app is launched with a URL the redirect URL should use HTTPS.</td>
</tr>
<tr>
<td>RFT4</td>
<td>The personal number in the RP web service API must be 12 characters (YYYYMMDDNNNN).</td>
</tr>
<tr>
<td>RFT5</td>
<td>When collect returns completed RP shall read and store the values of signature, userInfo and ocspResponse. RP does not need to verify the signature. BankID verifies the signature.</td>
</tr>
<tr>
<td>RFT6</td>
<td>collect should be called every two seconds and must not be called more frequent than once per second.</td>
</tr>
<tr>
<td>RFT7</td>
<td>RP should display a progress indicator in its web app when waiting for the complete response from collect.</td>
</tr>
<tr>
<td>RFT8</td>
<td>RP must contact BankID’s web service API from RP’s backend server. RP must NOT contact BankID’s web service API from RP’s client app.</td>
</tr>
<tr>
<td>RFT9</td>
<td>RP should always use the latest version of the web service API, see Information Regarding the Web Service API.</td>
</tr>
<tr>
<td>RFT10</td>
<td>If the user selects to use Mobile BankID only, the certificatePolicies condition must be set to 1.2.752.78.1.5</td>
</tr>
<tr>
<td>RFT11</td>
<td>RP must use the issuer of the server cert as trusted root. If the server cert is used as trusted, the RP service will not be able to access the BankID server when the server cert is changed.</td>
</tr>
</tbody>
</table>

6 Recommended User Messages

<table>
<thead>
<tr>
<th>Short Name</th>
<th>Swedish Text</th>
<th>English Text</th>
<th>Event, status, hintCode or errorCode</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFA1</td>
<td>Starta BankID-appen</td>
<td>Start your BankID app.</td>
<td>status=pending hintCode= outstandingTransaction hintCode=noClient</td>
</tr>
<tr>
<td>RFA2</td>
<td>Du har inte BankID-appen installerad. Kontakta din internetbank.</td>
<td>The BankID app is not installed. Please contact your internet bank.</td>
<td>The BankID app is not installed in the mobile device.</td>
</tr>
<tr>
<td>RFA3</td>
<td>Åtgärden avbruten. Försök igen.</td>
<td>Action cancelled. Please try again.</td>
<td>errorCode=cancelled</td>
</tr>
<tr>
<td>RFA4</td>
<td>En identifering eller underskrift för det här personnumret är redan påbörjad. Försök igen.</td>
<td>An identification or signing for this personal number is already started. Please try again.</td>
<td>errorCode=alreadyInProgress</td>
</tr>
<tr>
<td>RFA5</td>
<td>Intern tekniskt fel. Försök igen.</td>
<td>Internal error. Please try again.</td>
<td>errorCode=requestTimeout errorCode=maintenance (repeatedly) errorCode=internalError</td>
</tr>
<tr>
<td>RFA6</td>
<td>Åtgärden avbruten.</td>
<td>Action cancelled.</td>
<td>status=failed hintCode=userId Cancel</td>
</tr>
<tr>
<td>RFA8</td>
<td>BankID-appen svarar inte. Kontrollera att den är startad och att du har internetanslutning. Om du inte har något giltigt BankID kan du hämta ett hos din Bank. Försök sedan igen.</td>
<td>The BankID app is not responding. Please check that the program is started and that you have internet access. If you don’t have a valid BankID you can get one from your bank. Try again.</td>
<td>status=failed hintCode=expiredTransaction</td>
</tr>
<tr>
<td>RFA9</td>
<td>Skriv in din säkerhetskod i BankID-appen och välj Legitimera eller Skriv under.</td>
<td>Enter your security code in the BankID app and select Identify or Sign.</td>
<td>status=pending hintCode=userSign</td>
</tr>
<tr>
<td>RFA13</td>
<td>Försöker starta BankID-appen.</td>
<td>Trying to start your BankID app.</td>
<td>status=pending hintCode=outstandingTransaction</td>
</tr>
<tr>
<td>RFA14 (A)</td>
<td>Söker efter BankID, det kan ta en liten stund… Om det har gått några sekunder och inget BankID har hittats har du sannolikt inget BankID som går att använda för den aktuella identifieringen/underskriften i den här datorn. Om du har ett BankID-kort, sätt in det i kortläsaren. Om du inte har något BankID kan du hämta ett hos din internetbank. Om du har ett BankID på en annan enhet kan du starta din BankID-app där.</td>
<td>Searching for BankID:s, it may take a little while… If a few seconds have passed and still no BankID has been found, you probably don’t have a BankID which can be used for this identification/signing on this computer. If you have a BankID card, please insert it into your card reader. If you don’t have a BankID you can order one from your internet bank. If you have a BankID on another device you can start the BankID app on that device.</td>
<td>status=Pending hintCode=started The RP provided the personal number in the web service call (without using autoStartTokenRequired). The user accesses the service using a personal computer.</td>
</tr>
<tr>
<td>RFA14 (B)</td>
<td>Söker efter BankID, det kan ta en liten stund… Om det har gått några sekunder och inget BankID har hittats har du sannolikt inget BankID som går att använda för den aktuella identifieringen/underskriften i den här enheten. Om du inte har något BankID kan du hämta ett hos din internetbank. Om du har ett BankID på en annan enhet kan du starta din BankID-app där.</td>
<td>Searching for BankID:s, it may take a little while… If a few seconds have passed and still no BankID has been found, you probably don’t have a BankID which can be used for this identification/signing on this device. If you don’t have a BankID you can order one from your internet bank. If you have a BankID on another device you can start the BankID app on that device.</td>
<td>status=Pending hintCode=started The RP provided the personal number in the web service call (without using autoStartTokenRequired). The user accesses the service using a mobile device.</td>
</tr>
<tr>
<td>RFA15 (A)</td>
<td>Söker efter BankID, det kan ta en liten stund… Om det har gått några sekunder och inget BankID har hittats har du sannolikt inget BankID som går att använda för den aktuella identifieringen/underskriften i den här datorn. Om du har ett BankID-kort, sätt in det i kortläsaren. Om du inte har något BankID kan du hämta ett hos din internetbank.</td>
<td>Searching for BankID:s, it may take a little while… If a few seconds have passed and still no BankID has been found, you probably don’t have a BankID which can be used for this identification/signing on this computer. If you have a BankID card, please insert it into your card reader. If you don’t have a BankID you can order one from your internet bank.</td>
<td>status=Pending hintCode=started The RP did not provide the personal number in the web service call. The user accesses the service using a personal computer.</td>
</tr>
</tbody>
</table>
| RFA15 (B) | Söker efter BankID, det kan ta en liten stund… Om det har gått några sekunder och inget BankID har hittats har du sannolikt inget BankID som går att använda för den aktuella identifieringen/underskriften i den här enheten. Om du inte har något BankID kan du hämta ett hos din internetbank. | Searching for BankID:s, it may take a little while… If a few seconds have passed and still no BankID has been found, you probably don’t have a BankID which can be used for this identification/signing on this device. If you don’t have a BankID you can order one from your internet bank. | **status**=**pendin**g  
**hintCode**=**start**ed  
The RP did not provide the personal number in the web service call.  
The user accesses the service using a mobile device. |
|---|---|---|---|
| RFA16 | Det BankID du försöker använda är för gammalt eller spärrat. Använd ett annat BankID eller hämta ett nytt hos din internetbank. | The BankID you are trying to use is revoked or too old. Please use another BankID or order a new one from your internet bank. | **status**=**failed**  
**hintCode**=**certifi**cateErr  
The RP did not use QR code |
| RFA17 (A) | BankID-appen verkar inte finnas i din dator eller telefon. Installera den och hämta ett BankID hos din internetbank. Installera appen från din appbutik eller https://install.bankid.com. | The BankID app couldn’t be found on your computer or mobile device. Please install it and order a BankID from your internet bank. Install the app from your app store or https://install.bankid.com. | **status**=**failed**  
**hintCode**=**start**ed  
Failed  
RP does not use QR code |
| RFA17 (B) | Misslyckades att läsa av QR koden. Starta BankID-appen och läs av QR koden. Om du inte har BankID-appen måste du installera den och hämta ett BankID hos din internetbank. Installera appen från din appbutik eller https://install.bankid.com. | Failed to scan the QR code. Start the BankID app and scan the QR code. If you don't have the BankID app, you need to install it and order a BankID from your internet bank. Install the app from your app store or https://install.bankid.com. | **status**=**failed**  
**hintCode**=**start**ed  
Failed  
RP uses QR code |
| RFA18 | Starta BankID-appen | Start the BankID app | The name of link or button used to start the BankID App |
| RFA19 | Vill du identifiera dig eller skriva under med BankID på den här datorn eller med ett Mobilt BankID? | Would you like to identify yourself or sign with a BankID on this computer or with a Mobile BankID? | The user access the service using a browser on a personal computer. |
| RFA20 | Vill du identifiera dig eller skriva under med ett BankID på den här enheten eller med ett BankID på en annan enhet? | Would you like to identify yourself or sign with a BankID on this device or with a BankID on another device? | The user access the service using a browser on a mobile device. |
| RFA21 | Identifiering eller underskrift pågår. | Identification or signing in progress. | **status**=**pendin**g  
The **hintCode** is unknown to RP. |
| RFA22 | Okänt fel. Försök igen. | Unknown error. Please try again. | **status**=**failed**  
The **hintCode** is unknown to RP.  
An error occurred. The **errorCode** is unknown to RP. |

NB: RFA7, RFA10, RFA11 and RFA12 are deprecated, and intentionally removed.
7 Production Environment

<table>
<thead>
<tr>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL certificate (RP certificate)</td>
<td>Provided by the bank that RP purchases the BankID service from. See section SSL Certificates below.</td>
</tr>
<tr>
<td>JSON Web Service URL</td>
<td><a href="https://appapi2.bankid.com/vp/v5">https://appapi2.bankid.com/vp/v5</a></td>
</tr>
<tr>
<td>Issuer of server certificate</td>
<td>See section SSL Certificates below.</td>
</tr>
</tbody>
</table>

The server certificate is issued by the following CA:

CN = BankID SSL Root CA v1
OU = Infrastructure CA
O = Finansiell ID-Teknik BID AB

Certificate:

BEGIN CERTIFICATE-----
MIIFCCCAoCAAgAwIBAgITbUIIBEwDQYJKoZIhvcNAQEFbDEWNJUzC3BGS0BAWJQAgEB
eMAwggE0MA0GCSqGSIb3DQEBCwYIXzAwSDAwDQYJKoZIhvcNAQEFbDEWNJUzC3BGS0B
AQFAAwEAMAwEB/zABBg0GA1UdDgQWBBQsL1OqA3KUc3v3JnBerj9aFRMQHAAoGBzJ
-----END CERTIFICATE-----

Network information:
The BankID app for Android, iOS, Windows 10 Mobile, iOS X and Windows in production connects to the BankID server on the IP address 185.198.4.18 using port 443 and address 185.198.4.19 using port 80. The BankID app for OS X and Windows also connects to the IP 5.150.251.26 using port 80.
### 8 Test Environment

BankID provides a test environment for an RP to use when developing and testing its service. To be able to use the test environment the RP will need:

1. An SSL certificate (RP certificate) for identification with the BankID web service API.
2. The URL for BankID’s web service API.
3. Trust the issuer of the SSL certificate.
4. A test version of the BankID app.
5. A BankID for test.

<table>
<thead>
<tr>
<th>Description</th>
<th>Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passphrase for above certificate</td>
<td>qwerty123</td>
</tr>
<tr>
<td>JSON Web Service URL</td>
<td><a href="https://appapi2.test.bankid.com/rp/v5">https://appapi2.test.bankid.com/rp/v5</a></td>
</tr>
<tr>
<td>Issuer of server certificate</td>
<td>See section SSL Certificates below. CN = Test BankID SSL Root CA v1 Test O = Finansiell ID-Teknik BID AB</td>
</tr>
</tbody>
</table>
9 Information Regarding the Web Service API

9.1 SSL Certificates

The RP certificate must be installed/configured in your “key store”. It does not need to be verified by your application and the issuer of the RP certificate is not needed. The RP certificate is verified by the BankID server when the channel is established. The BankID server will then present its server certificate to your application. The server certificate needs to be verified by your application. To make that verification possible the issuer of the server certificate needs to be installed/configured in your “trust store”. Key stores and trust stores are managed differently depending on your environment and is not explained in this document.

Note that different certificates are used for production and test.

Note that the certificates may need to be converted to a different file format to be accepted by your environment.

Note that your application needs access to your key store and trust store and your application needs to use correct key store and trust store.

Note that line breaks may need to be removed from the issuer of the server certificate pasted from this document.

9.2 appapi and appapi2

To manage a generation shift of the root certificate protecting the service we have introduced a new endpoint for the service; appapi2.bankid.com. This new endpoint is protected using a new root CA. RP must use the new endpoint. RP must trust the new root CA. The old endpoint will not work after June 2019.

- The previous appapi.bankid.com and the current appapi2.bankid.com provides the same functionality.
- appapi2.bankid.com is protected using a new root CA.
- appapi2.bankid.com must be used when integrating support for BankID. Old integrations must be changed to use the new endpoint and the new root CA must be in the trust store.
- appapi.bankid.com is protected using a root CA that expires June 2019 and must not be used. appapi.bankid.com will not work after the certificate has expired.

9.3 Versions

A new version of the web service API will be published on a new URL every time there is a breaking change in the API. RP should always use the latest version of the API. The general rule is that old versions will shut down 2 years after the release of the successor. As new functionality is introduced to the system the behavior of an existing version of the interface may change, e.g. existing faults may also be used in new situations.

This document is written for version 5 (current version) of the interface.

<table>
<thead>
<tr>
<th>V</th>
<th>URL</th>
<th>Changes</th>
<th>Release date</th>
<th>End of life</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td><a href="https://appapi2.bankid.com/rp/v4">https://appapi2.bankid.com/rp/v4</a></td>
<td>A new CA issues the server certificate. A new end point to access the service. Requires TLS1.1 or TLS1.2</td>
<td>March 2017</td>
<td>February 2020</td>
</tr>
<tr>
<td>5</td>
<td><a href="https://appapi2.bankid.com/rp/v5">https://appapi2.bankid.com/rp/v5</a></td>
<td>Http/JSON replaces SOAP/XML cancel introduced.</td>
<td>February 2018</td>
<td></td>
</tr>
</tbody>
</table>

9.3.1 Breaking Change

The following table describes the general principles for breaking changes. Security reasons may shorten the notice period.

<table>
<thead>
<tr>
<th>Change</th>
<th>Breaking</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add optional in-parameter</td>
<td>NO</td>
<td>We may add additional optional in-parameters without prior notice.</td>
</tr>
<tr>
<td>Add required in-parameters</td>
<td>YES</td>
<td>We may add additional required in-parameters. This will be done using a new endpoint and with a two year notice.</td>
</tr>
</tbody>
</table>
Remove any in-parameter | YES | We may remove support for in-parameters. This will be done using a new end point and with a two year notice.
---|---|---
Add return-parameter | NO | We may add additional return-parameters without prior notice. RP must consider this in their implementation. Implementations must **not** discard the complete response if it includes unknown parameters.
Remove any return-parameter | YES | We may remove return-parameters. This will be done using a new end point and with a two year notice.
Remove method | YES | We may remove methods. This will be done using a new end point and with a two year notice.
Add method | NO | We may add new methods without prior notice.
Change issuer of server certificate | YES | We may change issuer of the server certificate. This will be done using a new end point and with a two year notice.
Add new hintCodes | NO | We may add new hintCode without prior notice. RP must consider this in their implementation. If RP receives an "unknown" hint code a general message should be presented to the user.
Add new errorCodes | NO | We may add new errorCode without prior notice. RP must consider this in their implementation. If RP receives an "unknown" error code a general message should be presented to the user.

9.4 Test Environment

New versions and release candidates are used in the test environment prior to being taken into use in the production environment. Due to this, the content and functionality in the test environment and production environment may temporarily differ.

9.5 HTTP/1.1

The service only supports HTTP/1.1. HTTP/1.0 will not work.

9.6 TLS Versions

appapi2.bankid.com requires TLS1.1 or TLS1.2. We strongly recommend to use TLS1.2.

10 Support

10.1 Developer Support

Please study this guideline carefully before contacting us. Our experience is that all answers are provided in this document. Please also study the FAQ at https://www.bankid.com/bankid-i-dina-tjanster/rp-info. As a last resort, you may contact us using teknikinfo@bankid.com. In non-technical matters, please contact the bank through which you have purchased the BankID service.

10.2 End User Support

<table>
<thead>
<tr>
<th>Short name</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFS1</td>
<td>RP should inform the user what to do in case of lost or forgotten security code (contact the issuer).</td>
</tr>
<tr>
<td>RFS2</td>
<td>RP must provide support for its own service.</td>
</tr>
<tr>
<td>RFS3</td>
<td>When the user is having problems, the RP should redirect the user to <a href="https://test.bankid.com">https://test.bankid.com</a>. Users that cannot successfully use their BankID at <a href="https://test.bankid.com">https://test.bankid.com</a> should be redirected to the issuing bank in case of a BankID related problem and in case of network error to mobile phone carrier or the internet service provider. If the user can successfully identify and sign at <a href="https://test.bankid.com">https://test.bankid.com</a>, the user should be redirected to the RP user support.</td>
</tr>
</tbody>
</table>

11 Recommended Terminology

<table>
<thead>
<tr>
<th>Description</th>
<th>Recommended terminology in Swedish</th>
<th>Recommended terminology in English</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile BankID</td>
<td>Mobilt BankID</td>
<td>Mobile BankID</td>
</tr>
</tbody>
</table>
12 File Signing

Our recommendation is to use the sign method with the following notes:
1. Present the document to be signed to the user using your own application/website.
2. Compute a message digest of the binary representation of the document.
3. Compile an abstract of the content of the document.
4. Use method sign with userVisibleData set to the abstract and userNonVisibleData set to the message digest.

The benefits of using this method are that it is available for PCs and mobile devices, that there is no size limitation and that all types of documents can be signed.

13 Verifying Signatures

The signatures (including the certificates) returned from the service are already verified by the service. **Note:** The Relying Party does not need to verify the signatures.

It is however possible for the Relying Party to verify them. To do that, the following data is needed:

- The signature returned from the service. A specification of the content is delivered to you on request.
- The certificate of the user and intermediate CA:s. These are included in the signature.
- The ocspResponse returned from the service.
- The self signed root certificate. This is delivered to you on request.

The following principle is applicable:
1. Verify the signature.
2. Verify the certificates in the certificate chain up to the self signed root. Note that certificates may have expired at the time of verification if it is later than the time of use.
3. Verify the status of the ocspResponse to be ok.
4. Verify the signature of the ocspResponse.
5. Verify the certificate of the ocspResponse signer and that it is issued by the same CA as the user certificate in question.
6. Verify the nonce included in the ocspResponse to be correct by matching it with a hash computed of the signature. See completionData for Completed Orders.
14 RP Interface Description

In Rpv5, a JSON based format is used.
- HTTP1.1 is required
- All methods are accessed using HTTP POST to /rp/v5/<method>.
- Http header 'Content-Type' must be set to 'application/json'.
- The parameters including the leading and ending curly bracket is in the body.

14.1 /rp/v5/auth and /rp/v5/sign

Initiates an authentication or signing order. Use the collect method to query the status of the order. If the request is successful, HTTP 200, the orderRef and autoStartToken is returned.

Example request auth without personal number.

```
POST /rp/v5/auth HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "endUserIp": "194.168.2.25"
}
```

Example request sign with personal number.

```
POST /rp/v5/sign HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "personalNumber": "190000000000",
    "endUserIp": "194.168.2.25",
    "userVisibleData": "IFRoaXMgaXMgYSBzYW1wbGUgdGV4dCB0byBiZSBzaWduZWQ="
}
```

14.1.1 Parameters for auth and sign

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>personalNumber</td>
<td>Optional</td>
<td>The personal number of the user. String. 12 digits. Century must be included. If the personal number is excluded, the client must be started with the autoStartToken returned in the response</td>
</tr>
<tr>
<td>endUserIp</td>
<td>Required</td>
<td>The user IP address as seen by RP. String. IPv4 and IPv6 is allowed. Note the importance of using the correct IP address. It must be the IP address representing the user agent (the end user device) as seen by the RP. If there is a proxy for inbound traffic, special considerations may need to be taken to get the correct address. In some use cases the IP address is not available, for instance for voice based services. In this case, the internal representation of those systems IP address is ok to use.</td>
</tr>
<tr>
<td>Requirement</td>
<td>Optional</td>
<td>Requirements on how the auth or sign order must be performed. See below.</td>
</tr>
</tbody>
</table>

14.1.2 Additional Parameters for sign

<table>
<thead>
<tr>
<th>Name</th>
<th>Required</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>userVisibleData</td>
<td>Required</td>
<td>The text to be displayed and signed. String. The text can be formatted using CR, LF and CRLF for new lines. The text must be encoded as UTF-8 and then base 64 encoded. 1-40 000 characters after base 64 encoding.</td>
</tr>
<tr>
<td>userNonVisibleData</td>
<td>Optional</td>
<td>Data not displayed to the user. String. The value must be base 64-encoded. 1-200 000 characters after base 64-encoding.</td>
</tr>
</tbody>
</table>

14.1.3 Response from auth and sign

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>autoStartToken</td>
<td>Used as reference to this order when the client is started automatically. String.</td>
</tr>
<tr>
<td>orderRef</td>
<td>Used to collect the status of the order. String.</td>
</tr>
</tbody>
</table>

Example response from auth and sign.
HTTP/1.1 200 OK
Content-Type: application/json
{
    "orderRef": "131daac9-16c6-4618-beb0-365768f37288",
    "autoStartToken": "7c40b5c9-fa74-49cf-b98c-bfe651f9a7c6"
}

14.2 /rp/v5/collect

Collects the result of a sign or auth order using the orderRef as reference. RP should keep on calling collect every two seconds as long as status indicates pending. RP must abort if status indicates failed. The user identity is returned when complete.

Example request collect:

POST /rp/v5/collect HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "orderRef": "131daac9-16c6-4618-beb0-365768f37288"
}

14.2.1 Parameters for collect

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>orderRef</td>
<td>The orderRef returned from auth or sign.</td>
</tr>
</tbody>
</table>

14.2.2 Response from collect

The response will have different content depending on status of the order. The status may be pending, failed or complete.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>orderRef</td>
<td>The orderRef in question.</td>
</tr>
<tr>
<td>status</td>
<td>pending: The order is being processed. hintCode describes the status of the order. failed: Something went wrong with the order. hintCode describes the error. complete: The order is complete. completionData holds user information.</td>
</tr>
<tr>
<td>hintCode</td>
<td>Only present for pending and failed orders. See below.</td>
</tr>
<tr>
<td>completionData</td>
<td>Only present for complete orders. See below.</td>
</tr>
</tbody>
</table>

14.2.3 hintCode for Pending Orders

The order is pending. RP should use the hintCode to provide the user with details and instructions and keep on calling collect until failed or complete.

<table>
<thead>
<tr>
<th>hintCode</th>
<th>Reason</th>
<th>Action by RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>outstandingTransaction</td>
<td>The order is pending. The client has not yet received the order. The hintCode will later change to noClient, started or userSign.</td>
<td>If RP tried to start the client automatically, the RP should inform the user that the app is starting. Message RFA13 should be used. If RP did not try to start the client automatically, the RP should inform the user that she needs to start the app. Message RFA1 should be used.</td>
</tr>
<tr>
<td>noClient</td>
<td>The order is pending. The client has not yet received the order.</td>
<td>If RP tried to start the client automatically: This status indicates that the start failed or the users BankID was not available in the started client. RP should inform the user. Message RFA1 should be used. If RP did not try to start the client automatically: This status indicates that the user not yet has started her client. RP should inform the user. Message RFA1 should be used.</td>
</tr>
</tbody>
</table>
started

The order is pending. A client has been started with the autoStartToken but a usable ID has not yet been found in the started client. When the client starts there may be a short delay until all ID:s are registered. The user may not have any usable ID:s at all, or has not yet inserted their smart card.

If RP does not require the autoStartToken to be used and the user provided her personal number the RP should inform the user of possible solutions. Message RFA14 should be used.

If RP require the autoStartToken to be used or the user did not provide her personal number the RP should inform the user of possible solutions. Message RFA15 should be used.

Note: started is not an error, RP should keep on polling using collect.

userSign

The order is pending. The client has received the order.

The RP should inform the user. Message RFA9 should be used.

We may introduce new hint codes without prior notice. RP must handle unknown hint codes in their implementations.

If an unknown hintCode is returned for a pending order, RP should inform the user. Message RFA21 should be used.

RP should update their implementation to support the new hintCode as soon as possible.

Example response from collect for a pending order:

HTTP/1.1 200 OK
Content-Type: application/json
{
  "orderRef": "131daac9-16c6-4618-beb0-365768f37288",
  "status": "pending",
  "hintCode": "userSign"
}

14.2.4 hintCode for Failed Orders

This is a final state. The order failed. RP should use the hintCode to provide the user with details and instructions. The same orderRef must not be used for additional collect requests.

<table>
<thead>
<tr>
<th>hintCode</th>
<th>Reason</th>
<th>Action by RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>expiredTransaction</td>
<td>The order has expired. The BankID security app/program did not start, the user did not finalize the signing or the RP called collect too late.</td>
<td>RP must inform the user. Message RFA8.</td>
</tr>
<tr>
<td>certificateErr</td>
<td>This error is returned if: 1) The user has entered wrong security code too many times. The BankID cannot be used. 2) The users BankID is revoked. 3) The users BankID is invalid.</td>
<td>RP must inform the user. Message RFA16.</td>
</tr>
<tr>
<td>userCancel</td>
<td>The user decided to cancel the order.</td>
<td>RP must inform the user. Message RFA6.</td>
</tr>
<tr>
<td>cancelled</td>
<td>The order was cancelled. The system received a new order for the user.</td>
<td>RP must inform the user. Message RFA3.</td>
</tr>
<tr>
<td>startFailed</td>
<td>The user did not provide her ID, or the RP requires autoStartToken to be used, but the client did not start within a certain time limit. The reason may be: 1) RP did not use autoStartToken when starting BankID security program/app. RP must correct this in their implementation. 2) The client software was not installed or other problem with the user’s computer.</td>
<td>The RP must inform the user. Message RFA17.</td>
</tr>
</tbody>
</table>

We may introduce new hint Codes without prior notice. RP must handle unknown hint Codes in their implementations.

If an unknown hintCode is returned for a failed order, RP should inform the user. Message RFA22 should be used.
Example response from collect for a failed request:

HTTP/1.1 200 OK
Content-Type: application/json
{
  "orderRef":"131daac9-16c6-4618-beb0-365768f37288",
  "status":"failed",
  "hintCode":"userCancel"
}

14.2.5 completionData for Completed Orders

This is a final state. The order was successful. The user has provided the security code and completed the order. The completionData includes the signature, user information and the OCSP response. RP should control the user information and continue their process. RP should keep the completion data for future references/compliance/audit.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Information related to the user, holds the following children:</td>
</tr>
<tr>
<td></td>
<td>• personalNumber: The personal number. String.</td>
</tr>
<tr>
<td></td>
<td>• name: The given name and surname of the user. String.</td>
</tr>
<tr>
<td></td>
<td>• givenName: The given name of the user. String.</td>
</tr>
<tr>
<td></td>
<td>• surname: The surname of the user. String.</td>
</tr>
<tr>
<td>device</td>
<td>Information related to the device, holds the following child:</td>
</tr>
<tr>
<td></td>
<td>• ipAddress: The IP address of the user agent as the BankID server discovers it. String.</td>
</tr>
<tr>
<td>cert</td>
<td>Information related to the users certificate (BankID), holds the following children:</td>
</tr>
<tr>
<td></td>
<td>• notBefore: Start of validity of the users BankID. String, Unix ms.</td>
</tr>
<tr>
<td></td>
<td>• notAfter: End of validity of the Users BankID. String, Unix ms.</td>
</tr>
<tr>
<td></td>
<td>Note: notBefore and notAfter are the number of milliseconds since the UNIX Epoch, a.k.a. &quot;UNIX time&quot; in milliseconds. It was chosen over ISO8601 for its simplicity and lack of error prone conversions to/from string representations on the server and client side.</td>
</tr>
<tr>
<td>signature</td>
<td>The signature. The content of the signature is described in BankID Signature Profile specification. String. Base64-encoded. XML signature.</td>
</tr>
<tr>
<td>ocspResponse</td>
<td>The OCSP response. String. Base64-encoded. The OCSP response is signed by a certificate that has the same issuer as the certificate being verified. The OSCP response has an extension for Nonce. The nonce is calculated as:</td>
</tr>
<tr>
<td></td>
<td>• SHA-1 hash over the base 64 XML signature encoded as UTF-8.</td>
</tr>
<tr>
<td></td>
<td>• 12 random bytes is added after the hash</td>
</tr>
<tr>
<td></td>
<td>• The nonce is 32 bytes (20 + 12)</td>
</tr>
</tbody>
</table>

Example response from collect for a complete order:

HTTP/1.1 200 OK
Content-Type: application/json
{
  "orderRef":"131daac9-16c6-4618-beb0-365768f37288",
  "status":"complete",
  "completionData":{
    "user":{
      "personalNumber":"190000000000",
      "name":"Karl Karlsson",
      "givenName":"Karl",
      "surname":"Karlsson"
    },
    "device":{
14.3 /rp/v5/cancel

Cancels an ongoing sign or auth order. This is typically used if the user cancels the order in your service or app.

Example request cancel:

POST /rp/v5/cancel HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
"orderRef": "131daac9-16c6-4618-beb0-365768f37288"
}

14.3.1 Parameters for cancel

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>orderRef</td>
<td>The orderRef from the response from auth or sign. String.</td>
</tr>
</tbody>
</table>

14.3.2 Response from cancel

A successful response contains an empty JSON object.

Example response cancel

HTTP/1.1 200 OK
Content-Type: application/json
{}

14.4 Errors

The following table describes possible errors, their cause and the action to take by RP.

<table>
<thead>
<tr>
<th>HTTP</th>
<th>errorCode</th>
<th>Reason</th>
<th>Action by RP</th>
</tr>
</thead>
<tbody>
<tr>
<td>400</td>
<td>alreadyInProgress</td>
<td>An auth or sign request with personal number was sent, but an order for the user is already in progress. The order is aborted. No order is created. Details are found in details.</td>
<td>RP must inform the user that an auth or sign order is already in progress for the user. Message RFA4 should be used.</td>
</tr>
<tr>
<td>400</td>
<td>invalidParameters</td>
<td>Invalid parameter. Invalid use of method. Using an orderRef that previously resulted in completed. The order cannot be collected twice. Using an orderRef that previously resulted in failed. The order cannot be collected twice. Using an orderRef that is too old. completed orders can only be collected up to 3 minutes and failed orders up to 5 minutes. Details are found in details.</td>
<td>RP must not try the same request again. This is an internal error within RP's system and must not be communicated to the user as a BankID error.</td>
</tr>
</tbody>
</table>
400  We may introduce new error codes without prior notice. RP must handle unknown error codes in their implementations. If an unknown errorCode is returned, RP should inform the user. Message RFA22 should be used. RP should update their implementation to support the new errorCode as soon as possible.

401  unauthorized  RP does not have access to the service.  RP must not try the same request again. This is an internal error within RP's system and must not be communicated to the user as a BankID error.

404  notFound  An erroneously URL path was used.  RP must not try the same request again. This is an internal error within RP's system and must not be communicated to the user as a BankID error.

408  requestTimeout  It took too long time to transmit the request.  RP must not automatically try again. This error may occur if the processing at RP or the communication is too slow. RP must inform the user. Message RFA5.

415  unsupportedMediaType  Adding a "charset" parameter after 'application/json' is not allowed since the MIME type "application/json" has neither optional nor required parameters. The type is missing or erroneously.  RP must not try the same request again. This is an internal error within RP's system and must not be communicated to the user as a BankID error.

500  internalError  Internal technical error in the BankID system.  RP must not automatically try again. RP must inform the user. Message RFA5.

503  Maintenance  The service is temporarily out of service.  RP may try again without informing the user. If this error is returned repeatedly, RP must inform the user. Message RFA5.

Example response from collect with an invalid orderRef:

```plaintext
HTTP/1.1 400 Bad Request
Content-Type: application/json
{
  "errorCode":"invalidParameters",
  "details":"No such order"
}
```

### 14.5 Requirement

RP may use the requirement parameter to describe how the signature must be created and verified. A typical use case is to require Mobile BankID or a special card reader. Multiple requirement may be used in the same request. A requirement can be set for both auth and sign orders. The following table describes requirements, their possible values and defaults.

<table>
<thead>
<tr>
<th>Name</th>
<th>Value</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>cardReader</td>
<td>&quot;class1&quot; - (default). The transaction must be performed using a card reader where the PIN code is entered on the computer keyboard, or a card reader of higher class. &quot;class2&quot; - The transaction must be performed using a card reader where the PIN code is entered on the reader, or a reader of higher class. &lt;no value&gt; - defaults to &quot;class1&quot;. This condition should be combined with a certificatePolicies for a smart card to avoid undefined behavior.</td>
<td>No special type of card reader required.</td>
</tr>
<tr>
<td>certificatePolicies</td>
<td>The oid in certificate policies in the user certificate. List of String. One wildcard &quot;<em>&quot; is allowed from position 5 and forward ie. 1.2.752.78.</em></td>
<td>If no certificate policies is set the following are default in the production system:</td>
</tr>
</tbody>
</table>
The values for production BankIDs are:
"1.2.752.78.1.1" - BankID on file
"1.2.752.78.1.2" - BankID on smart card
"1.2.752.78.1.5" - Mobile BankID
"1.2.752.71.1.3" - Nordea e-id on file and on smart card.
The values for test BankIDs are:
"1.2.3.4.5" - BankID on file
"1.2.3.4.10" - BankID on smart card
"1.2.3.4.25" - Mobile BankID
"1.2.752.71.1.3" - Nordea e-id on file and on smart card.
"1.2.752.60.1.6" - Test BankID for some BankID Banks

The following are default in the test system:
1.2.752.78.1.1, 1.2.752.78.1.2,
1.2.752.78.1.5, 1.2.752.71.1.3
If one certificate policy is set all the default policies are dismissed.

issuerCn
The cn (common name) of the issuer. List of String.
Wildcards are not allowed. Nordea values for production:
"Nordea CA for Smartcard users 12" - E-id on smart card
issued by Nordea CA.
"Nordea CA for Softcert users 13" - E-id on file issued by
Nordea CA
Example Nordea values for test:
"Nordea Test CA for Smartcard users 12" - E-id on smart card
issued by Nordea CA.
"Nordea Test CA for Softcert users 13" - E-id on file issued by
Nordea CA
If issuer is not defined all relevant BankID and Nordea
issuers are allowed.

autoStartTokenRequired
If present, and set to true, the client must have been started
using the autoStartToken. Boolean. To be used if it is
important that the BankID App is on the same device as the
RP service.
If this requirement is omitted, the client does not need to be
started using autoStartToken. It does not work to set it to false
(we may reconsider this, and make it possible to set it to false
in future release).
The client does not need to be
started using autoStartToken.

allowFingerprint
Users of iOS and Android devices may use fingerprint for
authentication and signing if the device supports it and the
user configured the device to use it. Boolean. No other devices
are supported at this point.
If set to true, the users are allowed to use fingerprint.
If set to false, the users are not allowed to use fingerprint.
true for authentication.
false for signing.

14.5.1 Example – allowFingerprint for sign

POST /rp/v5/sign HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
  "personalNumber":"190000000000",
  "endUserIp": "192.168.0.1"
  "requirement": {"allowFingerprint":true}
}

14.5.1 Example – certificatePolicies for auth with Mobile BankID

POST /rp/v5/auth HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
  "personalNumber":"190000000000",
  "endUserIp": "192.168.0.1"
  "requirement": {"certificatePolicies":["1.2.752.78.1.5"]}
}

14.5.1 Example – Combined Requirements
Multiple conditions can be set for a requirement (AND). Multiple values can be set for a condition
certificatePolicies and issuerCn (OR).
POST /rp/v5/auth HTTP/1.1
Content-Type: application/json
Host: appapi2.bankid.com
{
    "personalNumber": "190000000000",
    "endUserIp": "192.168.0.1",
    "requirement": {
        "certificatePolicies": ["1.2.752.78.1.5", "1.2.752.71.1.3", "1.2.752.78.1.2"],
        "autoStartTokenRequired": true
    }
}