ZignSec

BANKID SWEDEN V5 IMPLEMENTATION GUIDELINES

ZignSec AB (publ)

Version 1.3 | Updated September 2024

BankID Sweden v5 Implementation Guidelines

Code:	
Version:	1.3
Date of version:	2024-September-25
Created by:	Martin Heikkilä, Head of Support
Approved by:	Jason Coombes, Head of Risk and Compliance
Confidentiality level:	PUBLIC

PUBLIC

©ZignSec AB (publ)

Table of Contents

PUBLIC

©ZignSec AB (publ)

BankID

BankID is a trusted electronic identification system in Sweden, built on a Public Key Infrastructure (PKI). It provides secure authentication and non-repudiation for online transactions. The system employs two-factor authentication (2FA), combining a personal certificate tied to an individual's social security number with a PIN or password. End-to-end encryption ensures data security. As of September 2021, it was a fundamental part of Sweden's digital infrastructure with over 8 million active users, regulated by the Swedish Financial Supervisory Authority.

PUBLIC

©ZignSec AB (publ)

Secure start to be mandatory

In order to protect both users and e-services,

the secure start of BankID becomes mandatory for all authorities,

companies and organizations that use BankID in their e-services.

Please update as soon as possible.

To meet the requirements for secure start you need to implement the changes listed below. By updating to the latest version of ZignSec implementation you will meet all requirements.

1. Use autostart for BankID on the same device
2. Use animated QR code for BankID on another device
3. Remove start with personal identity numbers

Ways of integration BankID

ZignSec provides two ways for implementing Swedish BankID:

- **Browser Flow**- The workflow is executed within a ZignSec-controlled browser session.
- **API Flow** - A backend without a user interface, suitable for server, mobile, desktop app, or custom scenarios. This flow also includes the Phone Flow - An authentication process when the user is engaged in a telephone conversation.

Use cases

Swedish BankID can be implemented in different ways, depending on the device initiating the flow.
The use cases are:

- The user aims to authenticate using an app on the **same device** where the BankID app is installed.
- The user aims to authenticate using a web browser running on **other device** than the one the BankID app is installed on. For this use case, QR code is the recommended way to trigger authentication.
- Please find more details in the references

Here are examples of the links showing the visual flow.

- Mobile device - **same device** flow where the app is installed and triggered from the mobile.
- Desktop to mobile device - **other device** flow where the app is triggered on the desktop to the mobile by QR-code.
- Desktop same device - **same device** flow when the app is installed on the desktop and triggered there. This flow is the least common since most users have the BankID installed on their mobile.

Note! More than 80% of BankID users are only using the BankID mobile app.

Authentication or Sign

Authentication is aimed for identification and sign to be used for digital signatures. But both methods except the same parameters this is a change from previous versions when there was limitations to adding text in the BankID app.

PUBLIC

©ZignSec AB (publ)

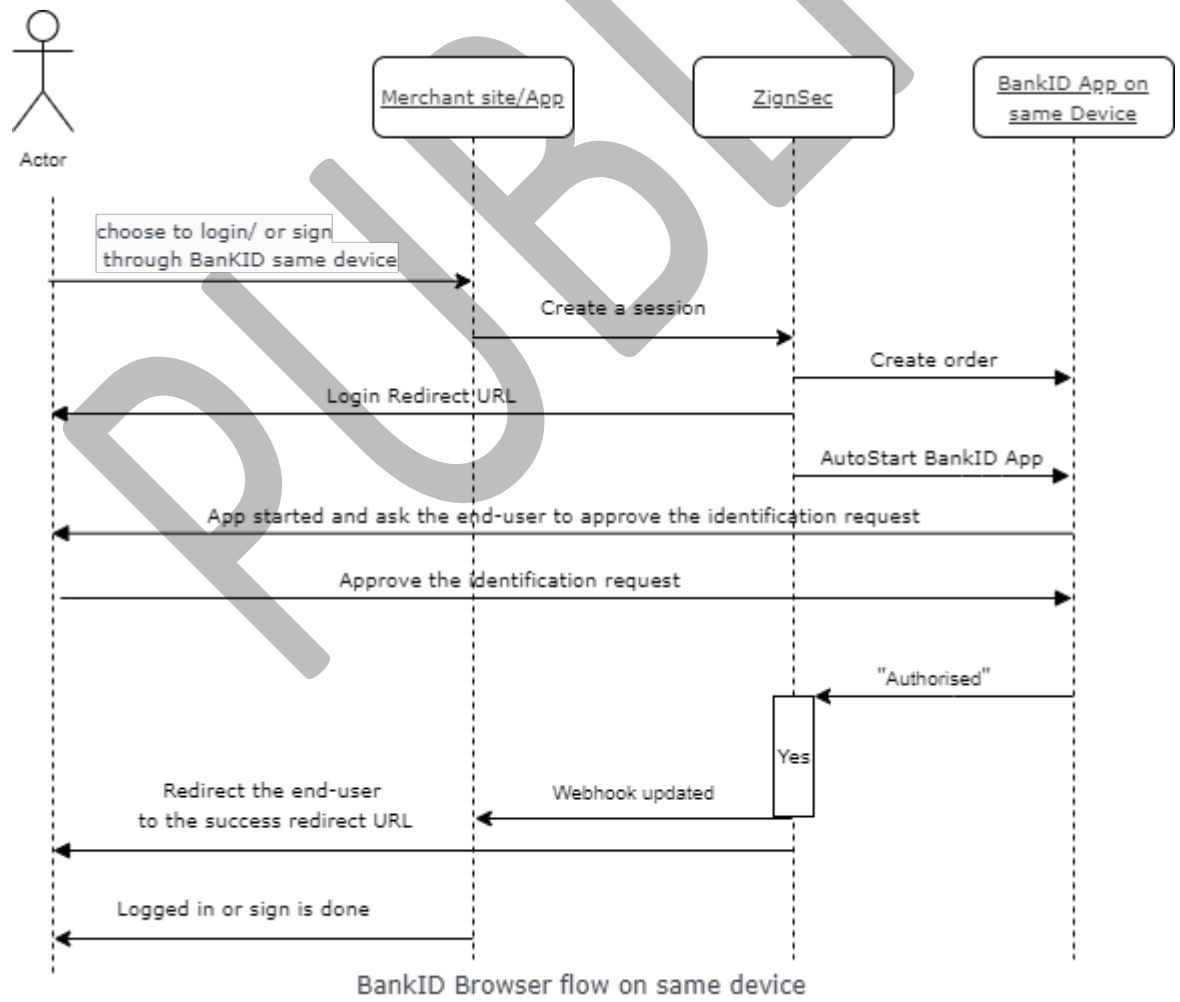
Browser Flow

Execution Sequence

The initial call triggers the end user's operation - either authenticate or sign. This call instantly activates the authenticate or sign process, and the BankID app is immediately notified to display either authenticate or sign. To avoid continuous polling, consider configuring a webhook for “completed/error”. *Execution Sequence*

1. Request Creation: Set up the POST-request for the product. Use the redirect URL returned in the response to start the browser workflow, identified by sessionID. (Link Sample request)
2. Running the Login Process: Simply navigate to the redirect URL in a web browser. The workflow may involve specific user interactions and an external device, such as the Swedish mobile BankID, may be necessary.(Link to Sample response containing redirect URL)
3. Retrieving Status/Results: Get status and individual data using the unique workflow sessionID code. Make this call during or after the workflow is completed. The workflow can indicate pending, completed, or error status (exception, user cancel, timeout) via a browser redirect to the redirect success (or failure) URL and/or through a webhook. (Link to Sample Result response)

Find below the sequence diagram for Browser flow on the same device.

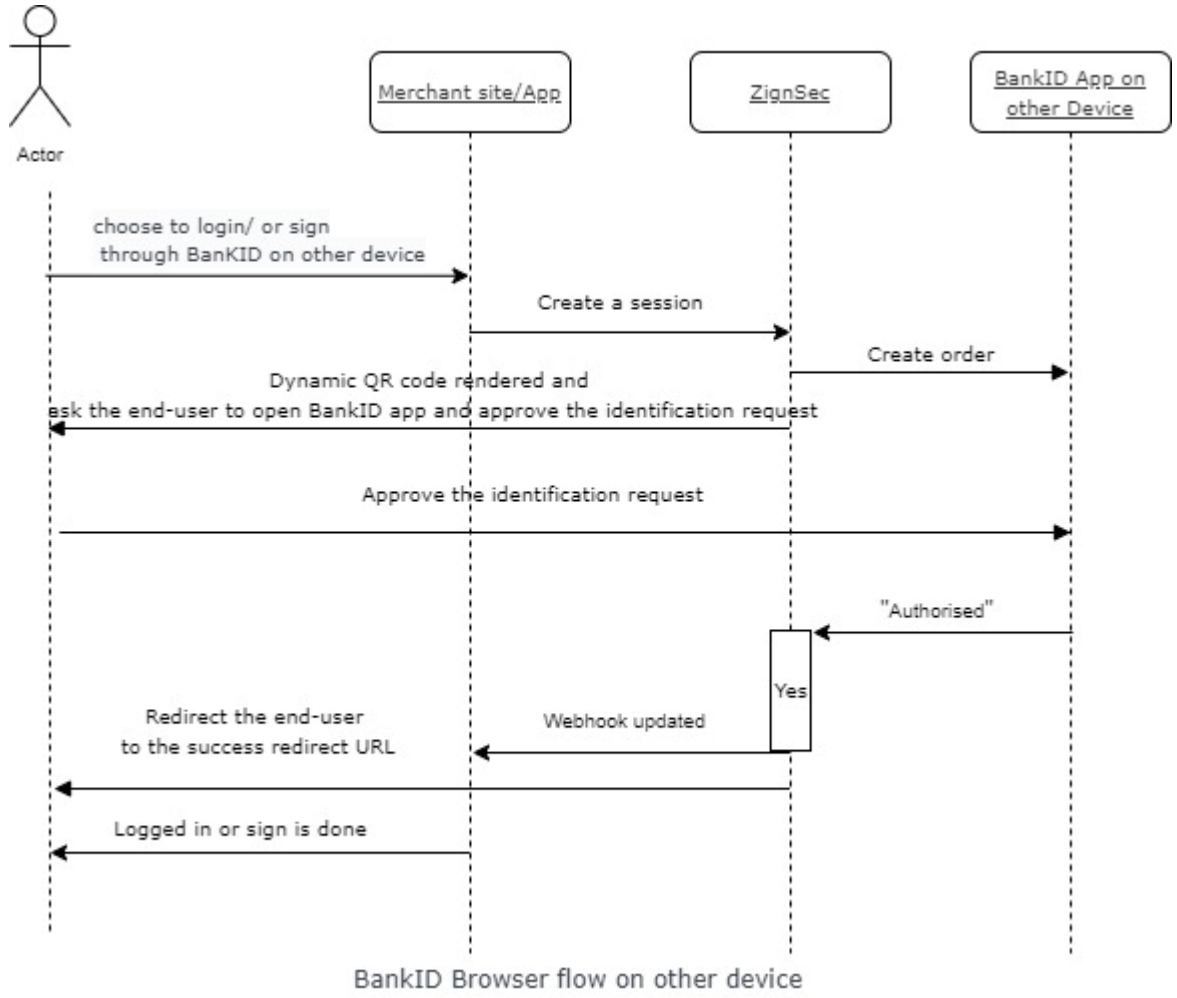


BankID Browser flow on same device

PUBLIC

©ZignSec AB (publ)

And here is the sequence diagram for Browser flow on other device.



BankID Browser flow on other device

Swagger for Browser flow

- Test BankId SE - Browser Flow: Swagger UI (zignsec.com)
- Production BankId SE - Browser Flow: Swagger UI (zignsec.com)

API Endpoint

- Base URL for Test: https://test-gateway.zignsec.com/core/api/sessions/
- Base URL for Production: https://gateway.zignsec.com/core/api/sessions/

Important Note: For customers using Two-Way SSL certificates, they need to call different endpoints base URL like mentioned below

- Test: https://api-test.zignsec.com
- Prod: https://api-prod.zignsec.com

Authenticate

Used for electronic identifying a person

POST - BankID SE Auth - Browser Flow Same Device

©ZignSec AB (publ)

Endpoint: /bankidse/browser/same-device/auth

GET - Get Session Data (BankID SE Auth - Browser Flow Same Device)

Endpoint: /bankidse/browser/same-device/auth/{id}

POST - BankID SE Auth - Browser Flow Other Device

Endpoint: /bankidse/browser/auth

GET - Get Session Data (BankID SE Auth - Browser Flow Other Device)

Endpoint: /bankidse/browser/auth/{id}

Sign

Used for electronic signatures

POST – BankID SE Sign – Browser Flow Same Device

Endpoint: /bankidse/browser/same-device/sign

GET – Get Session Data (BankID SE Sign – Browser Flow Same Device)

Endpoint: /bankidse/browser/same-device/sign/{id}

POST - BankID SE Sign - Browser Flow Other Device

Endpoint: /bankidse/browser/sign

GET - Get Session Data (BankID SE Sign - Browser Flow Other Device)

Endpoint: /browser/sign/id

Sample of BankID SE Auth - Browser Flow Other Device

```
curl -X 'POST' \
  'https://test-gateway.zignsec.com/core/api/sessions/bankidse/browser/auth' \
  -H 'accept: application/json' \
  -H 'authorization: Your-Subscription-Key' \
  -H 'Content-Type: application/json' \
  -d '{
  "locale": "En",
  "metadata": {
    "language": "en",
    "requirement": {
      "certificate_policies": [
        "1.2.752.78.1.5",
        "1.2.752.60.1.6"
      ],
      "mrtd": false,
      "personal_number": "194911201111",
      "pin_code": false
    }
```


©ZignSec AB (publ)

```
  },
  "redirect_failure": "https://my_failure_url.com",
  "redirect_success": "https://my_success_url.com",
  "relay_state": "my-unique-customer-id",
  "webhook": "https://my_webhook_url.com"
}'
```

Request Parameters

Parameter	Type	Description	Required
Locale	string	Preferred Language to Use. Example: En	no
metadata	list	Sign request	yes
language	string	Decides web form user interface language. The default language is taken from the merchants setting 'DefaultLanguage' or EN = English if none is set there. Language can be changed both on a request level here, or on setting level.	no
requirement	list	RP may use the requirement parameter to describe how a signature must be created and verified. A typical use case is to require Mobile BankID or a certain card reader.	no
card_reader	Enum: [Class1, Class2]	Class1 - Default. The transaction must be performed using a card reader where the PIN code is entered on the computers keyboard, or a card reader of higher class., Class2 - The transaction must be performed using a card reader where the PIN code is entered on the reader, or a reader of higher class	no
certificate_policies	string	The oid in certificate policies in the user certificate. List of String. One wildcard "" is allowed from position 5 and forward i.e.. 1.2.752.78. 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	no

PUBLIC

©ZignSec AB (publ)

Parameter	Type	Description	Required
		"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 If no certificate policies is set the following are default in the production 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 The following are default in the test system: 1.2.3.4.5, 1.2.3.4.10, 1.2.3.4.25, 1.2.752.60.1.6, 1.2.752.71.1.3 If one certificate policy is set all the default policies are dismissed.	
Mrtd	boolean	If present, and set to true, the client needs to provide MRTD (Machine readable travel document) information.	no
personal_number	string	A personal number to be used to complete the transaction. If a BankID with another personal number attempts to sign the transaction, it fails.	no
pin_code	boolean	Users are required to sign the transaction with their PIN code, even if they have biometrics activated.	no
Theme	Enum Default, Light, Dark	Default - Default theme, Light - Light theme, Dark - Dark theme	no

PUBLIC

©ZignSec AB (publ)

Parameter	Type	Description	Required
user_non_visible_data	string	Data not displayed to the user. base-64 string. 1-200,000 characters after base 64-encoding	no
user_non_visible_text	string	The text to be displayed and signed. string. 1--40,000 characters after base 64 encoding	no
user_visible_data	string	The text to be displayed and signed. base-64 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	no
user_visible_data_format	string	If present, and set to simpleMarkdownV1, this parameter indicates that userVisibleData holds formatting characters which, will potentially make the text displayed to the user nicer to look at. For further information of formatting options, please see the guidelines for formatting text.	no
user_visible_text	string	The text to be displayed and signed. string. Converted to UserVisibleData. If both UserVisibleData and UserVisibleText sent, the UserVisibleData will be used. 1--40 000 characters after base 64 encoding	no
redirect_failure	string	URL to redirect the end-user to on failure. Example: https://my_failure_url.com	no
redirect_success	string	URL to redirect the end-user to on success. Example: https://my_success_url.com	no
relay_state	string	Optional Custom Parameter. Example: my-unique-customer-id	no
webhook	string	Webhook URL where your backend will receive session events. Example: https://my_webhook_url.com	no

PUBLIC

©ZignSec AB (publ)

PUBLIC

©ZignSec AB (publ)

Sample Response


```
{
  "data": {
    "errors": [],
    "id": "8bd5f1bf-3239-4f17-8ed6-fc620b05884c",
    "redirect_url": "https://test-gateway.zignsec.com/ui/bankidse/8bd5f1bf-3239-4f17-8ed6-fc620b05884c/?otp=Z_6-zcEsoUane_-Wjcf-DQ&language=en&theme=Light",
    "status": "GeneratedLink"
  }
}
```


Response parameters

Parameter	Description
Id	A unique session identifier generated for each workflow instance
Errors	A JSON array of error conditions
redirect_url	The URL that the user needs to be redirected to complete the data via the web interface.

Sample Response after completing workflow.


```
{
  "errors": [],
  "id": "ca1d0bcd-94e3-483d-a4dc-f207eb248a29",
  "result": {
    "bankIDSE": {
      "ocspResponse": "MIIHdgo....JQ4N/A+RoS4...",
      "orderRef": "458727f9-82f6-45ba-be86-5ca692ff851f",
      "signature": "PD94bWwgdm....mVkRGF0Y5hdHVyZT4=",
      "userInfo": {
        "givenName": "Erik Lennart",
        "ipAddress": "109.228.185.130",
        "name": "Erik Lennart Eriksson",
        "personalNumber": "194911201111",
        "surname": "Eriksson"
      }
    },
    "identity": {
      "addressInfoRaw": "",
```


PUBLIC

©ZignSec AB (publ)

```
        "age": 74,
        "countryCode": "SE",
        "customerPersonId": "my-unique-customer-id",
        "dateOfBirth": "1949-11-20",
        "email": "",
        "firstName": "Erik Lennart",
        "fullName": "Erik Lennart Eriksson",
        "gender": "M",
        "idProviderName": "BankIDSE",
        "idProviderPersonId": "",
        "idProviderRequestId": "1b2e07e5-2f26-4d9e-904c-2ed73f9cbdc8",
        "identificationDate": "2023-12-14T11:40:53.2316596Z",
        "lastName": "Eriksson",
        "personalNumber": "194911201111",
        "phone": "",
        "resultReportPdf": ""
      }
      "method": "Auth",
      "userMessage": "NoMessage"
    },
    "status": "Finished"
}
```


Sample of Error response


```
{
  "errors": [
    {
      "code": "CANCELLED_BY_USER",
      "description": "Action cancelled by user"
    }
  ],
  "id": "2cab790d-d0d6-4aa5-9d94-c08caab5dfba",
  "result": {
    "method": "Auth",
    "userMessage": "NoMessage"
  },
  "status": "Cancelled"
}
```


©ZignSec AB (publ)

Response Parameters

Parameter	Type	Description
Errors	list	list of errors see separate table
Id	string	UUID for the session used to fetch the status and result of a session
Result	list	Contains the result of the session more details below
ocspResponse	String	The OCSP response. 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: • SHA-1 hash over the base 64 XML signature encoded as UTF-8. • 12 random bytes is added after the hash. • The nonce is 32 bytes (20 + 12).
orderRef	string	Idprovider UUID for the session, used when communicating issues with specific session with provider
signature	String	The signature as described in the BankID Signature Profile specification. Base64-encoded. XML signature.
userInfo	Object	Information related to the user: • personalNumber: The personal identity number. • name: The given name and surname of the user. • givenName: The given name of the user. • surname: The surname of the user. • ipAddress: The IP address of the user agent as the BankID server discovers it.
method	String	The method used: "Auth" for Authentication and "Sign" for signature.
identity	Object	Identity structure: Our main id data holder found in the responses from all our eIDs products.

PUBLIC

©ZignSec AB (publ)

Parameter	Type	Description
		• countryCode: Indicates the country the identification is performed in. • customerPersonId: Optional Custom Parameter. Example: my-unique-customer-id • dateOfBirth: In the format YYYY-MM-DD • gender: Male(M) or Female(F) • personalNumber: Availability depends on the underlying identity provider in the respective country. In Denmark (MitID) and Norway (BankID) it is normally not delivered. • idProviderName: IDP data. ZignSec´s name of the underlying identity provider, for example MitID, BankIDSE, BankIDNO • idProviderPersonId: IDP data. A provider specific unique identifier for the person identified • idProviderRequestId: IDP data. A provider specific unique identifier for the transaction, if available. (for traceability) • identificationDate: IDP data. A datetime for when the identification took place.
userMessage	String	NoMessage, RFA1, RFA2, RFA3, RFA4, RFA5, RFA6, RFA8, RFA9, RFA13, RFA14, RFA14A, RFA14B, RFA15, RFA15A, RFA15B, RFA16, RFA17, RFA17A, RFA17B, RFA18, RFA19, RFA20, RFA21, RFA22, RFA23
Status	String	GeneratedLink, Pending, Finished, Failed, Cancelled, Timeout.

Errors

Parameter	Type	Description
Code	string	Error code. Can be used for automatic error processing.
description	string	Error description. Human readable text.
Details	string	Error details. Might contain technical information.

PUBLIC

©ZignSec AB (publ)

API Flow

Execution Sequence

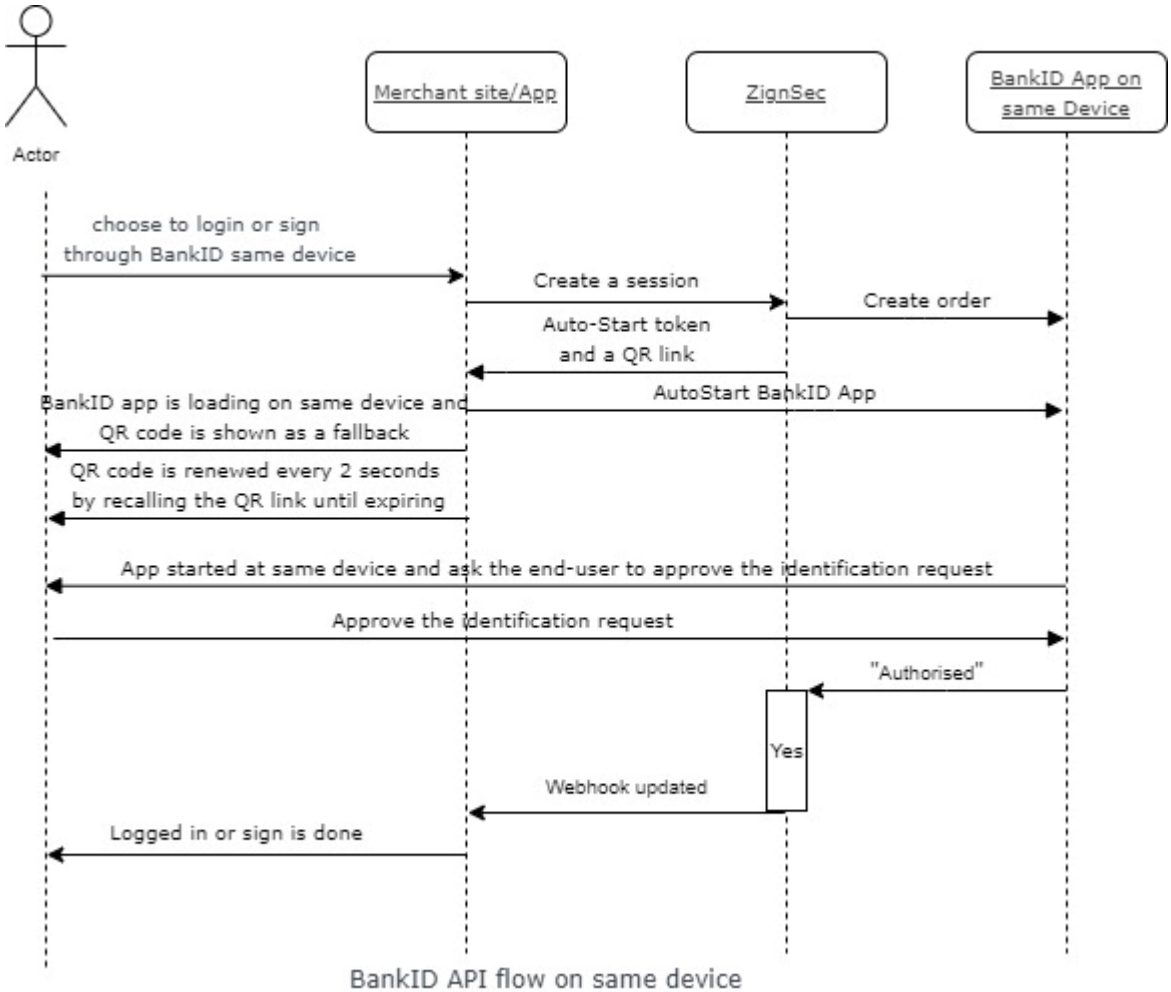
The opening call initiates the desired end user operation - Authenticate or Sign.

1. This initial call triggers the authenticate or sign process on the BankID backend instantly, alerting the BankID app to display the authenticate or sign page. It's advisable to have a web hook set up for “completion/error” to bypass frequent checks.
   Establish a login session and launch BankID backend and app for the designated operation - Authenticate or Sign. This will result in a new BankID session token. (Link to Sample request)
2. Commence the login procedure in a BankID app, you find details in the Launching paragraph below.
3. To retrieve the Final Results, ProgressStatus, or Errors, call the API in any of the following ways:
   -Automate the posting of results to the client's webhooks for success and error, previously registered with ZignSec.
   -Continually monitor the progress status, errors, and ultimately get the results. (Link to Sample Result response)
4. Cancel request terminates an ongoing sign, auth or phone order. This is generally utilized when the user discontinues the order within your service or application

Here is the sequence diagrams related to the API flow

PUBLIC

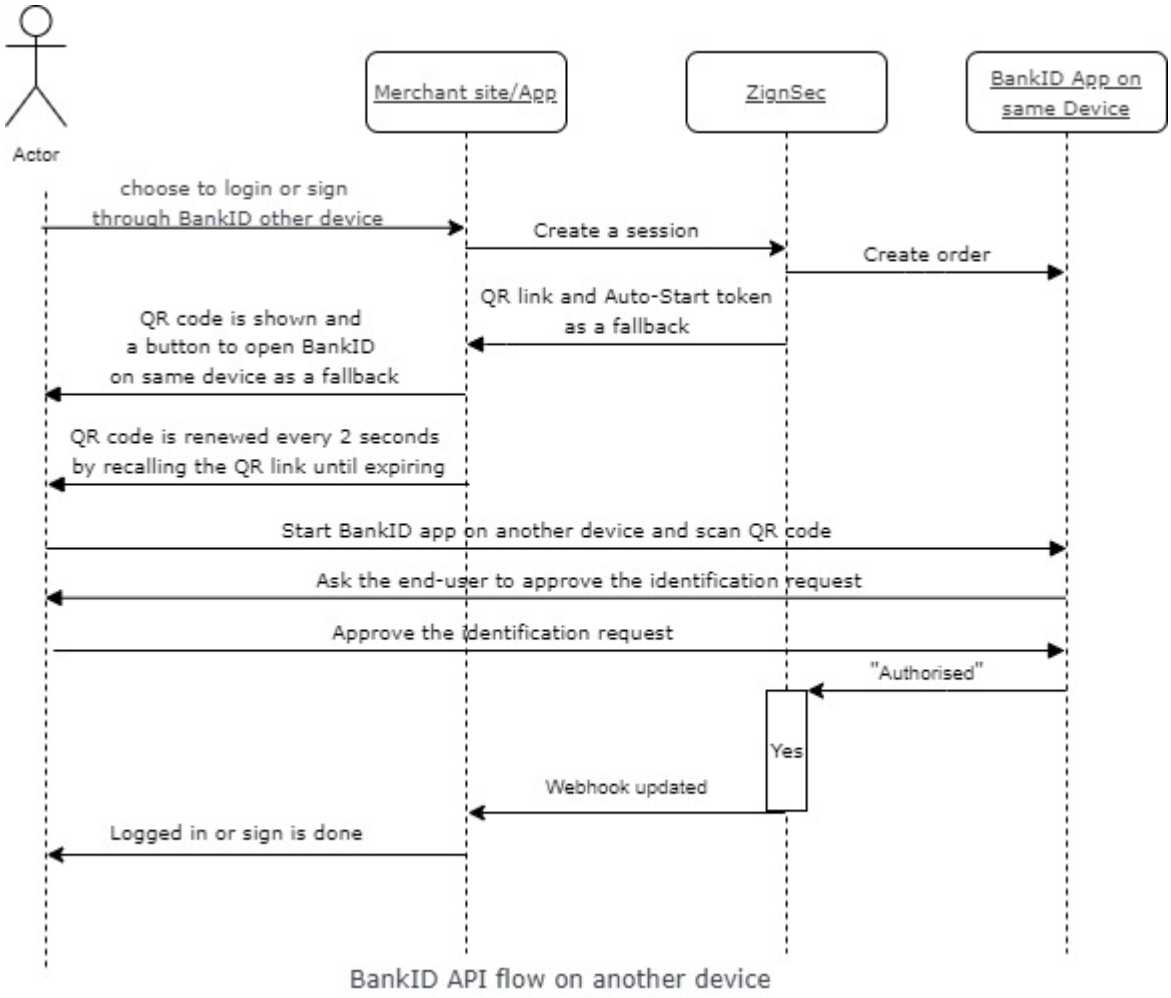
©ZignSec AB (publ)



BankID API flow on same device

PUB

©ZignSec AB (publ)



BankID API flow on another device

Swagger for API flow

- Test BankId SE - API Flow: Swagger UI (zignsec.com)
- Production BankId SE - API Flow: Swagger UI (zignsec.com)

API Endpoints

- Base URL for Test: https://test-gateway.zignsec.com/core/api/sessions/
- Base URL for Production: https://gateway.zignsec.com/core/api/sessions/

Authenticate

POST - BankID SE (Create Authentication Session)

Endpoint: /bankidse/auth

GET - Get Session Data (BankID SE (Create Authentication Session))

Endpoint: /bankidse/auth/{id}

Sign

POST - BankID SE (Create Signing Session)

©ZignSec AB (publ)

Endpoint: /bankidse/sign

GET - Get Session Data (BankID SE (Create Signing Session))

Endpoint: bankidse/sign/{id}

Sample of a BankID SE Auth Request

```
curl -X 'POST' \
  'https://test-gateway.zignsec.com/core/api/sessions/bankidse/auth' \
  -H 'accept: application/json' \
  -H 'authorization: Your-Subscription-Key' \
  -H 'Content-Type: application/json' \
  -d '{
  "locale": "En",
  "metadata": {
    "end_user_ip": "127.0.0.1",
    "requirement": {
      "certificate_policies": [
        "1.2.3.4.5",
        "1.2.3.4.10",
        "1.2.3.4.25",
        "1.2.752.60.1.6",
        "1.2.752.78.1.1",
        "1.2.752.78.1.2",
        "1.2.752.78.1.5",
        "1.2.752.71.1.3"
      ],
      "mrtd": false,
      "pin_code": false
    },
    "user_non_visible_text": "The text you\''ll never see",
    "user_visible_text": "Please authorize the TEST"
  },
  "redirect_failure": "https://my_failure_url.com",
  "redirect_success": "https://my_success_url.com",
  "relay_state": "my-unique-customer-id",
  "webhook": "https://my_webhook_url.com"
}'
```

Request parameters

Additional request parameter (Here is a link to the other request parameters)

©ZignSec AB (publ)

Parameter	Type	Description	Required
end_user_ip	string	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.	yes
useCase		To be used to get more accurate userMessage depending on the useCase that is being used. (This setting can be set on account level if required, just contact support@zignsec.com for assistance) Possible values: SameDevice and OtherDevice Example: • SameDevice + outstandingTransaction -> RFA13 • OtherDevice + outstandingTransaction -> RFA1	no

Sample Response for BankID API auth

This response has an onboarding setting turned on. This setting gives you ready examples to add to your code depending on the device. Read more about launching the app in the following part.


```
{
  "data": {
    "errors": [],
    "id": "00e3bbf4-a6b5-48e8-b5bb-2b4417be17f7",
    "result": {
      "autoStartToken": "43181c31-a299-4af7-964f-9e84909efb39",
      "devExamples": {
        "autoStartUrls": {
          "android": "https://app.bankid.com/?autostarttoken=43181c31-a299-4af7-964f-9e84909efb39&redirect=null",
          "ios": "https://app.bankid.com/?autostarttoken=43181c31-a299-4af7-964f-9e84909efb39&redirect=https://translate.google.com/?sl=auto&tl=sv&text=All%20right!&op=translate",
          "pc": "bankid:///?autostarttoken=43181c31-a299-4af7-964f-9e84909efb39&redirect=null",
          "pcWithReturn": "bankid:///?autostarttoken=43181c31-a299-4af7-964f-9e84909efb39&redirect=https://translate.google.com/?sl=auto&tl=sv&text=All%20right!&op=translate"
        }
      },
      "orderRef": "e719a549-dc96-448a-a3fd-77769afd7df3",
```


©ZignSec AB (publ)

```
        "qrCodeLink": "https://test-gateway.zignsec.com/ui/bankidseweb/00e3bbf4-a6b5-48e8-b5bb-2b4417be17f7/qr?otp=KpIDtL2pbUCu0pqIkylCSg",
        "qrStartToken": "88a0a376-8809-42e0-9b90-117252ed3b31"
      },
      "status": "Pending"
   }
}
```


Sample response with onboarding setting turned off

Same response as above with onboarding setting set to false. Just reach out to us and we will set the setting per your request.


```
{
   "data": {
      "errors": [],
      "id": "df0bc372-a5c7-482c-8289-be73ad34ffde",
      "result": {
         "autoStartToken": "99890334-5ace-451d-8449-00e0a34ef94a",
         "orderRef": "572941e9-020a-431e-b161-f34589e4770b",
         "qrCodeLink": "https://test-gateway.zignsec.com/ui/bankidseweb/df0bc372-a5c7-482c-8289-be73ad34ffde/qr?otp=f71NR5LX9EatG4IyGV9HTQ",
         "qrStartToken": "01c0a40f-5e38-4757-b314-f772430ca264"
      },
      "status": "Pending"
   }
}
```


Cancel

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

POST - BankID SE Cancel

Endpoint: /bankidse/cancel

Sample of cancel request

```
curl --location 'https://test-gateway.zignsec.com/core/api/sessions/bankidse/cancel' \
--header 'accept: application/json' \
--header 'Authorization: Your-Subscription-Key ' \
--header 'Content-Type: application/json' \
--data '{
  "metadata": {
    "session_id": "18511c63-5849-469b-bfec-6f1229a5997b"
  }
}'
```


©ZignSec AB (publ)

Sample of response

```
{
   "data": {
      "errors": [
         {
            "code": "CANCELLED_BY_USER",
            "description": "Action cancelled by user"
         }
      ],
      "id": "c788df2b-cc2e-45c0-bc87-b94cd503dbff",
      "result": {
         "method": "Auth",
         "userMessage": "NoMessage"
      },
      "status": "Cancelled"
   }
}
```

Launching the BankID app

Launching from native app on mobile device

Android

```
Intent intent = new Intent();
intent.setAction(Intent.ACTION_VIEW);
intent.setData(Uri.parse("https://app.bankid.com/?autostarttoken=&lt;INSERT AUTOSTARTTOKEN HERE&gt;&amp;redirect=null"));
intent.setFlags(Intent.FLAG_ACTIVITY_NEW_TASK);
startActivity(intent);
```

There is no guarantee that a valid result will be returned from the BankID app to the application's activity. The application should rely on the collect call to obtain the authentication or signature result. If the BankID app is not installed on the device, an android.content.ActivityNotFoundException is thrown. The application must inform the user and use Message RFA2. On Android 5, the URI should use the "bankid" scheme instead of the "https" scheme.

iOS

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

If the BankID app is not installed on the device, "false" is returned. The application must inform the user and use Message RFA2. The application must register a universal link or a custom URL scheme to allow the

©ZignSec AB (publ)

BankID app to relaunch the application. During the Apple App Store review process, the app requires login information to a demo account. This demo account should either not require BankID for login or provide a way to configure the app to use the BankID test environment.

Launching the BankID app from a browser

The "redirect" parameter should be placed last in the parameter list. The "autostarttoken" and "rpref" parameters are optional. Parameter names should be in lowercase. If the BankID app is launched without any matching web service calls for authentication or signature, an error message will be displayed in the app.

App links and universal links on Android and iOS

The syntax for the URL is as follows:

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

The URL works on Chrome (Android) and Safari (iOS).

Desktop and other mobile browsers

The syntax for the URL is as follows:

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

The URL works on PCs with all commonly used browsers. There may be variations on different platforms.

QR code

The typical use case for QR codes is when the user uses “Mobile BankID on other device” (see Use cases), and there is a security concern that the user does not control both devices.

QR code generation

The QR image needs to be updated once every 1-2 sec. (we use 2 sec. on our UI)

1. When our Browser flow is used, it is handled by ZignSec.
2. When the Api flow is used, your will get a "qrCodeLink" in a response. Customers should display the image "qrCodeLink" and re-render it every 1-2 sec

Note: if you navigate to "qrCodeLink" and hit refresh the page you will see new QR each time

Sample QR html and JavaScript code

Here an example on the html and JavaScript needed to make the QR code animated:

html

```
...
<img id="qr-image" src="..." />
...
```

JavaScript

```
const qrCodeLink = '...'; // from bankidse/auth request
const imageElement = document.getElementById('qr-image');
const intervalInMilliseconds = 2000; // re-render QR every 2 seconds
let t = 0;
setInterval(function () {
  imageElement.setAttribute('src', qrCodeLink + "?t=" + t)
```


©ZignSec AB (publ)
PUBLIC

```
    t++;
}, intervalInMilliseconds)
```

PUBLIC

©ZignSec AB (publ)

Phone Flow

The process for initiating an authentication order over the phone and querying its status involves:

1. **Start**: A user converses over the phone, typically with customer service.
2. **Initiation**: Authentication is initiated during the call as needed.
3. **User Action**: The user is instructed to perform a task for authentication, such as entering a one-time password.
4. **Monitoring**: The 'collect' function periodically checks the status of the authentication process. Please find more details about Collect status at the end of this document.
5. **Confirmation**: Upon successful authentication, the system updates the status, and the user is notified.
6. **Completion**: The call proceeds with the user now authenticated, enabling secure interactions.

Swagger for Phone flow

- Test: Swagger UI (zignsec.com)
- Production: Swagger UI (zignsec.com)

POST

BankID SE (Create Authentication Session over the Phone)

Endpoint: /bankidse/phone/auth/

GET

Get Session Data (BankID SE (Create Authentication Session over the Phone))

Endpoint: /bankidse/phone/auth/id

Sample of Phone auth request

```
curl -X 'POST' \
  'https://test-gateway.zignsec.com/core/api/sessions/bankidse/phone/auth' \
  -H 'accept: application/json' \
  -H 'authorization: Your-Subscription-key' \
  -H 'Content-Type: application/json' \
  -d '{
  "locale": "En",
  "metadata": {
    "call_initiator": "user",
    "personal_number": "194610241111",
    "user_non_visible_text": "The text you\''ll never see",
    "user_visible_text": "Please authorize yourself for the TEST call"
  },
  "redirect_failure": "https://my_failure_url.com",
  "redirect_success": "https://my_success_url.com",
  "relay_state": "my-unique-customer-id",
```


©ZignSec AB (publ)
PUBLIC

```
  "webhook": "https://my_webhook_url.com"
}'
```

Additional request parameters

(Here is a link to the other request parameters)

Parameter	Type	Description	Required
call_initiator	string	Indicate if the user or the RP initiated the phone call.	yes
personal_number	string	The personal number of the user. 12 digits	yes

PUBLIC

©ZignSec AB (publ)

User Messages

When processing an order, the BankID service sends status updates through the Collect API. It's advisable to present this order status , ensuring users stay informed and are notified of any possible errors.

BankId SE errors

Errors will be returned when a session status is having one of the following values: Failed, Timeout or Cancelled

- In general case, it's caused by
  - COMMUNICATION_ERROR - rest call error - retry recommended
  - SERVER_ERROR -
  - CONFIGURATION_ERROR - something is not configured on our side for your account, no retry, please contact ZignSec support
  - PROVIDER_BAD_REQUEST - provider returned "bad request" - no retries. Most probably the underlying bankidse session (order) is already finished
  - TIMEOUT - timeout elapsed, no retry, you need another session to authorize user
  - CANCELLED_BY_USER - session is cancelled by user, no retry, you need another session to authorize user
- Specific case:
  - ERROR - error received while collecting data from BankId SE - rely on "Recommended user message"
    - description: BankIDSE_ERROR
    - details: string details

Collect Info Status

Collect status can be :

• pending: The order is being processed. hintCode describes the status of the order.

• complete: The order is complete. completionData holds user information.

• failed: Something went wrong with the order. hintCode describes the error.

Please note that the hintCode is only present for pending and failed orders.

Status	User Message	Hint Code	Progress Status	Reason	Action by RP
complete	NoMessage		COMPLETE		
failed	RFA16	certificateErr	CERTIFICATE_ERR	This error is returned if: -The user has entered the wrong PIN code too many times. The BnkID cannot be used. -The user's BankID is blocked. -The user's BankID is invalid.	The RP must inform the user using message RFA16.

PUBLIC

©ZignSec AB (publ)

failed	RFA17A	startFailed	START_FAILED	The user did not provide their ID or the client did not launch within a certain time limit. Potential causes are: RP did not use autoStartToken when launching the BankID security app. RP must correct this in their implementation. Client software was not installed or other problem with the user's device.	The RP must inform the user using message RFA17.
failed	RFA17B	startFailed	START_FAILED	The user did not provide their ID or the client did not launch within a certain time limit. Potential causes are: RP did not use autoStartToken when launching the BankID security app. RP must correct this in their implementation. Client software was not installed or other problem with the user's device.	The RP must inform the user using message RFA17.
failed	RFA3	cancelled	CANCELLED	The order was cancelled. The system received a new order for the user.	The RP must inform the user using message RFA3.
failed	RFA6	userCancel	USER_CANCEL	The order was cancelled by the user. userCancel may also be returned in some rare cases related to other user interactions.	The RP must inform the user using message RFA6.
failed	RFA8	expiredTransaction	EXPIRED_TRANSACTION	The order has expired. The BankID security app/program did not launch, the user did not finalize the signing or the RP called collect too late.	The RP must inform the user using message RFA8.

PUBLIC

©ZignSec AB (publ)

pending	RFA1	outstandingTransaction	OUTSTANDING_TRANSACTION	Order is pending. The BankID app has not yet received the order. The hintCode will later change to noClient, started or userSign.	If RP tried to launch the client automatically, the RP should inform the user that the app is launching. Message RFA13 should be used. If RP did not try to start the client automatically, the RP should prompt user to start the app. Message RFA1 should be used.
pending	RFA9	userSign	USER_SIGN	Order is pending. The BankID client has received the order.	The RP should inform the user using message RFA9.
pending	RFA15B	started	STARTED	Order is pending. A BankID client has launched with autostarttoken but a usable ID has not yet been found in the client. When the client launches there may be a short delay until all IDs are registered. The user may not have any usable IDs, or is yet to insert their smart card.	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.
pending	RFA23	userMrtd		Order is pending. A client has launched and received the order but additional steps for providing MRTD information is required to proceed with the order.	The RP should inform the user using message RFA23.

PUBLIC

©ZignSec AB (publ)

pending	RFA1	noClient		Order is pending. The client has not yet received the order.	If RP tried to launch the client automatically: This status indicates that the launch failed, or that the user's BankID was not available in the client. RP should inform the user. Message RFA1 should be used. If RP did not try to launch the client automatically: This status indicates that the user has not yet launched the client. RP should inform the user. Message RFA1 should be used.

PUBLIC

©ZignSec AB (publ)

Recommended user messages

Short name	Swedish	English	Event, status, hintCode or errorCode
RFA1	Starta BankID-appen.	Start your BankID app.	status=pending hintCode=outstandingTransaction hintCode=noClient
RFA2	Du har inte BankID-appen installerad. Kontakta din bank.	The BankID app is not installed. Please contact your bank.	The BankID app is not installed in the mobile device.
RFA3	Åtgärden avbruten. Försök igen	Action cancelled. Please try again.	errorCode=cancelled
RFA4	En identifiering eller underskrift för det här personnumret är redan påbörjad. Försök igen.	An identification or signing for this personal number is already started. Please try again.	errorCode=alreadyInProgress
RFA5	Internt tekniskt fel. Försök igen.	Internal error. Please try again.	errorCode=requestTimeout errorCode=maintenance (repeatedly) errorCode=internalError
RFA6	Åtgärden avbruten.	Action cancelled.	status=failed hintCode=userCancel
RFA8	BankID-appen svarar inte. Kontrollera att den är startad och att du har internetanslutning. Om du inte har något giltigt BankID kan du skaffa ett hos din bank. Försök sedan igen.	The BankID app is not responding. Please check that it's started and that you have internet access. If you don't have a valid BankID you can get one from your bank. Try again.	status=failed hintCode=expiredTransaction

PUBLIC

©ZignSec AB (publ)

Short name	Swedish	English	Event, status, hintCode or errorCode
RFA9	Skriv in din säkerhetskod i BankID-appen och välj Identifiera eller Skriv under.	Enter your security code in the BankID app and select Identify or Sign.	status=pending hintCode=userSign
RFA13	Försöker starta BankID-appen.	Trying to start your BankID app.	status=pending hintCode=outstandingTransaction
RFA14 (A)	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 skaffa ett hos din bank. Om du har ett BankID på en annan enhet kan du starta din BankID-app där.	Searching for BankID, 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 get one from your bank. If you have a BankID on another device you can start the BankID app on that device.	status=pending hintCode=started The user accesses the service using a personal computer.
RFA14 (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 skaffa ett hos din bank. Om du har ett BankID på en	Searching for BankID, 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 get one from your bank.	status=pending hintCode=started The user accesses the service using a mobile device.

PUBLIC

©ZignSec AB (publ)

Short name	Swedish	English	Event, status, hintCode or errorCode
	annan enhet kan du starta din BankID-app där.	If you have a BankID on another device you can start the BankID app on that device.	
RFA15 (A)	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 skaffa ett hos din bank.	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 get one from your bank.	status=pending hintCode=started The user accesses the service using a personal computer.
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 skaffa ett hos din bank.	Searching for BankID, 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 get one from your bank.	status=pending hintCode=started 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 skaffa ett nytt hos din bank.	The BankID you are trying to use is blocked or too old. Please use another BankID or get a new one from your bank.	status=failed hintCode=certificateErr

PUBLIC

©ZignSec AB (publ)

Short name	Swedish	English	Event, status, hintCode or errorCode
RFA17 (A)	BankID-appen verkar inte finnas i din dator eller mobil. Installera den och skaffa ett BankID hos din bank. 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 get a BankID from your bank. Install the app from your app store or https://install.bankid.com	status=failed hintCode=startFailed RP does not use QR code.
RPA17 (B)	Misslyckades att läsa av QR-koden. Starta BankID-appen och läs av QR-koden. Kontrollera att BankID-appen är uppdaterad. Om du inte har BankID-appen måste du installera den och skaffa ett BankID hos din bank. 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. Check that the BankID app is up to date. If you don't have the BankID app, you need to install it and get a BankID from your bank. Install the app from your app store or https://install.bankid.com	status=failed hintCode=startFailed RP uses QR code
RFA18	Starta BankID-appen.	Start the BankID app.	The name of the 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 accesses 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 accesses the service using a browser on a mobile device.

PUBLIC

©ZignSec AB (publ)

Short name	Swedish	English	Event, status, hintCode or errorCode
RFA21	Identifiering eller underskrift pågår.	Identification or signing in progress.	status=pending The hintCode is unknown.
RFA22	Okänt fel. Försök igen.	Unknown error. Please try again.	status=failed The hintCode is unknown. An error occured. The errorCode is unknown.
RFA23	Fotografera och läs av din ID-handling med BankID-appen.	Process your machine-readable travel document using the BankID app.	status=pending hintCode=userMrtd

Recommended terminology

Description	Swedish	English
Mobile BankID	Mobilt BankID	Mobile BankID
BankID Security Application for mobile devices	BankID-appen	The BankID app
BankID Security Application for PCs	BankID-appen eller BankID-programmet	The BankID app
Security code, password, PIN	Säkerhetskod (för Mobilt BankID) Lösenord (för BankID på fil) PIN (för BankID på kort)	Security code (for Mobile BankID) Password (for BankID on file) PIN (for BankID on card)
Sign	Skriva under	Sign
Signature	Underskrift	Signature

PUBLIC

©ZignSec AB (publ)

Description	Swedish	English
Identify	Identifiera	Identify
Identification/authentication	Identifiering	Identification

Test BankID SE

To get started,

1- Download the BankID app to your phone, or the program BankID Security Application to your computer.
2- Note that a reconfiguration of the Bankid app is required.
3- Move ahead in this test guide and follow the instructions to get a BankID for test.

All details are mentioned in the BankID Test website ; Here you find a demo and more information on how to integrate the Swedish BankID. You can use one of these test users list .

***Note that you can not use the test BankID app and real BankID app on the same device.

PUBLIC

©ZignSec AB (publ)

Change History

Date of Change	Changed By	Summary of Change
October 2023	Martin Heikkilä	First version
December 2023	Martin Heikkilä	Version 1.1 • Added Swagger links • Added identity node in result response body • Added useCase parameter to API flow
April 2024	Marwa Guellouz	Version 1.2 • Added Sequence diagrams for Browser Flow on same device and other device • Added Sequence diagrams for API Flow • Added a table for the collect status
September 2024	Liliane Umutoni	Version 1.3 • Updated the links to the developers page.

PUBLIC

©ZignSec AB (publ)