Martin Heikkilä

ZignSec

BANKID NORWAY V5.1

Integration guidelines

ZignSec AB (publ)
Version 1.1 |October. 2024
PUBLISHED

BankID Norway v5.1 Integration guidelines

Code:	
Version:	1.1
Date of version:	2024-Oct-04
Created by:	Martin Heikkilä Customer Service Manager
Approved by:	Jason Coombes, Head of Risk and Compliance
Confidentiality level:	PUBLIC

Table of Contents

BankID Overview

Norwegian BankID is a widely utilized electronic identification (eID) and digital signature solution developed by a consortium of Norwegian banks. It offers a secure and convenient way for citizens, businesses, and public institutions to authenticate online. BankID enables access to a broad range of services, including banking, e-commerce, and government portals.

The service combines a unique user ID, a personal password, and one-time codes generated through a physical code device or the BankID mobile app. With its robust security features and widespread adoption, BankID plays a crucial role in safeguarding users' online transactions in Norway.

BankID services encompass two main scopes:

- Identification
- Digital Onboarding

The BankID OIDC (eID) solution is an OpenID Connect-based service that provides users with authentication and verification using BankID and mobile BankID as identity providers.

Identification

Authentication with BankID

BankID provides means to authenticate users at High or Substantial levels of assurance, making it the preferred method for accessing public services, banking, and various business applications. With over 4 million users, BankID ensures a secure and reliable authentication process that complies with Norwegian and EU regulations.

Using BankID APIs for Authentication

By integrating BankID's API, you can authenticate users and receive their identity details. These details can be used to match and verify the user against an existing customer profile, ensuring secure access.

Levels of Assurance Supported by the eID Scheme:

- High (Standard)
- Substantial (Biometric)

When to Use High Assurance:

- Accessing Sensitive Information: Ideal for viewing or managing personal data, whether it’s your own or someone else’s.
- Signing Documents: Required when official signatures are necessary.
- Updating Critical Personal Information: Such as changing a registered address or other vital details.
- Performing High-Impact Actions: For activities that require strong user confirmation, like canceling a subscription or changing transaction limits.
- Conducting High-Risk Transactions: Especially for transactions involving large sums or high risk to the user or service provider.

When to Use BankID with Biometrics:

- Authentication: Secure login for various applications.
- Low-Sum Payments: Ideal for transactions involving smaller amounts.
- Age Verification: For services that require proof of age.
- Customer Service Authentication: To confirm user identity during customer service interactions.
- Seamless App Login: Enables users to log in effortlessly using face recognition, fingerprint, or PIN, enhancing trust in the service.

Note: This is a general guideline. Businesses should conduct their own risk assessments to determine the most appropriate BankID method for their specific use cases.

End User Data returned

The following data fields are returned directly from the eID scheme:

- NNIN (if legally permitted)
- Full Name
- Date of Birth (DoB)
- Gender
- Age
- GUID

Merchants may also request additional user data, such as NNIN, address, email, and phone number. This will prompt the user to consent to share this information after authentication. Users may decline to share any information requiring consent.

Scopes

A **scope** is a way for the OIDC Client to indicate to the OIDC Provider what service it requests access to, or in technical terms which resources at pertinent Resource Servers. The response from a Resource Server consists of datasets with attributes on the user and/or the authentication event.

You find a complete description here at the supplier: Link to Scopes documentation

User Experience Guidelines for BankID Integration

This section covers user experience design, offering guidance on presenting BankID to end users and tips for implementing it effectively.

Identity Providers

BankID currently offers two identity verification methods for end users:

1. **BankID Netcentric**: This method requires a code device issued by the user's bank or the BankID app, along with a personal password that the user sets up through their online banking platform. Some banks have developed their own mobile apps that can be used instead of the code device.
2. **BankID Substantial**: This method allows for biometric authentication directly on the user's mobile device.

Basic Flow: End-User Interactions

The end user interacts with BankID through three stages, depending on the service requested:

1. **NNIN Input and BankID Method Selection**: The user enters their National Identity Number (NNIN) or Social Security Number (SSN) and selects the desired BankID method, depending on the information provided in the login_hint parameter.
2. **Authentication/Signing**: The user signs in and/or provides credentials for the selected BankID method.
3. **(Optional) Consent Dialogues**: If requested by the merchant, the user provides consent to share their data.

For detailed information on designing the user experience for BankID authentication, including the flow of interactions, method selection, and consent management, please refer to the official BankID User Experience Documentation. This resource provides comprehensive guidelines on ensuring a seamless and secure experience for end users across different authentication methods.

Customization

BankID offers various customization options for the user interface presented to end users. These include the ability to add a custom logo and merchant name, control display modes for different devices (like mobile apps or popups), and adjust the user interface to ensure a consistent experience across platforms. The logo should meet specific size and format requirements (300 x 60 px, max 10kB, PNG/SVG). Customization is managed via parameters during the provisioning process. You can find more details here.

Digital onboarding

Using BankID in the Onboarding Process

We offer products that simplify the onboarding process while adhering to regulatory requirements. Businesses may use BankID products in various ways, depending on their needs.

Storing NNIN from End-Users

- **Consent Required:** To store a user's National Identity Number (NNIN), consent must be obtained.
- **Merchant Responsibilities:** Merchants must handle consent storage, with BankID offering a UX flow for this process.
- **Technical Details:** Merchants must be provisioned to access nnin_altsub and nnin scopes

Please note, merchants must be provisioned to get access to the nnin_altsub and nnin scopes. You'll need a legal reason to store and use national identity numbers. This access is given as a part of the commercial agreement process.

Error Handling

Handling User Cancellation

The end-user can cancel an ongoing authentication or signing session at any time. If this happens, the user will be redirected back to the specified redirect URL provided by the merchant application.

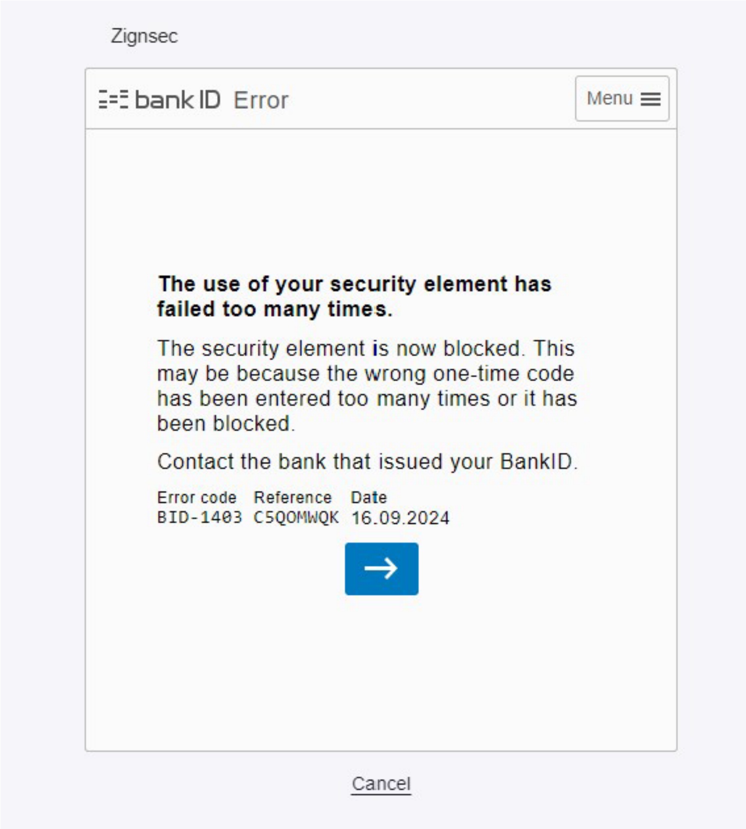
The merchant application must be prepared to handle this callback and respond appropriately.

Handling Errors

If an error occurs during an ongoing authentication or signing session, the following scenarios may take place:

- The end-user might be shown an error message, often accompanied by an error code, with options to retry or return to the merchant application.
- If the error occurs under the "right conditions," the user can be redirected back to the merchant application, using the same parameters as when a user cancels the session.
- In rare cases, an error other than access_denied might be returned, along with an error_description parameter, depending on the situation.
- In severe cases, the user might be stuck on the BankID platform with no option to return to the merchant application.

Here's an example of how an error message might be displayed in the browser



The use of your security element has failed too many times.

The security element is now blocked. This may be because the wrong one-time code has been entered too many times or it has been blocked.

Contact the bank that issued your BankID.

Error code	Reference	Date
BID-1403	C5QOMWQK	16.09.2024

API Overview

Core Functionalities

Environments

We maintain environments you can use:

- **Test (TEST)** environment: https://test-gateway.zignsec.com/api/v5/sessions
- **Production (PROD)** environment**:** https://gateway.zignsec.com/api/v5/sessions

Authentication

Each request to our API should be authenticated by sending your subscription key in the "Authorization" header. Our support creates subscription keys for you (a pair for each environment), and it's highly recommended to regularly rotate the keys (currently it's done by sending a support request, but please let us know if you'd like to automate it).

If you need different configurations, it's possible to register multiple tenants and configure them differently.

REST API

Headers

Header	Description	Required
Authorization	This header parameter is the subscription key you received from ZignSec during the registration process. Example: Authorization: 123456add0cff22873c428e987654321	Yes
Content-Type	Specifies the media type of the request body data. Set to application/json if JSON object.	Yes

OpenAPI specification and documentation

LIVE DOCUMENTATION

- https://test-gateway.zignsec.com/api/v5/openapi/bankidno/#/

BankId Norway Examples

API Endpoints

AUTHENTICATION

The choice of BankID Authentication endpoints is driven by the key needs of your business and use case. Please refer to the scopes documentation to understand the differences better. The endpoints utilise OIDC protocol.

DEFAULT ENDPOINT

Endpoint: POST /bankidno/auth - Swagger UI (zignsec.com)

Description: Standard endpoint. This API endpoint is to authenticate users with minimal requirements to the user data (see the Scopes documentation). Default scopes `openid + profile` (these scopes are requested in all endpoints listed here).

NEW USERS ONBOARDING (ASKING FOR NNIN)

Endpoint: POST /bankidno/auth/register - Swagger UI (zignsec.com)

Description: This API endpoint is used to onboard a new user by requesting an access to the end user's National Identification Number (NNIN). It prompts the end users to provide consent for sharing their data. Technically it uses `nnin` additional scope.

AUTHENTICATE ALREADY REGISTERED USERS (NNIN ALREADY POSSESSED)

Endpoint: POST /bankidno/auth/member - Swagger UI (zignsec.com)

Description: This endpoint will work for users you already possess their national identity number and does not ask customer for the consent to retrieve the end user's National Identification Number (NNIN). Technically it uses `nnin_altsub` additional scope.

GET SESSION DETAILS

Endpoint: GET /bankidno/auth/{sessionId} - Swagger UI (zignsec.com)

Description: This API endpoint retrieves the status and details of a BankID identity verification session in Norway. It allows you to check the outcome of a previously initiated verification request.

Settings and scopes can be changed upon request just contact ZignSec support.

Testing

Use either of the following test user:

Name	Personal Number	Entry Passcode	Personal Password
Aksel Herseth	06046517928	otp	qwer1234
Ole Bramserud	11920287974	otp	qwer1234
Sanna Hansen	12829025475	otp	qwer1234
Test Testsen	20872329758	otp	qwer1234

Or you can request your own BankID test users or test Apps by emailing support@zignsec.com. Please include the name and fødselsnummer (personal identification number) for each test user. The information should be formatted as follows:

- For characters 'æøå' to be accepted, save file as Unicode-text in Excel .
- Accepted line format is shown below. Use either comma ',' or semicolon ';' as field delimiter.

[Personal ID Number] [BankID Friendly Name] [Last Name] [First Name and possibly Middle Name]

Alternatively, you can create your own test user on the following page: BankID RA 1.6.6-SNAPSHOT - BankID Norge

For guidance on using the page, refer to the RA Light User Guide - BankID Norway Developer Portal

Production testing

Currently, there are no test users available for the production environment. Merchants who wish to conduct tests in staging areas using the production environment will need to use real BankID users.

Change History

Date of Change	Changed By	Summary of Change
February 2024	Jason Coombes	First version
September 2024	Martin Heikkilä	1.1