



**E-LEGITIMATIONS
NÄMNDEN**

Implementation Profile for BankID Identity Providers within the Swedish eID Framework

Version 1.1 - 2018-06-19

ELN-0612-v1.1

Table of Contents

1. **Introduction**
 - 1.1. Requirements Notation
 - 1.2. References to SAML 2.0 Standards and Profiles
 - 1.3. BankID Methods and Applications
 - 1.3.1. Representation as Identity Providers
 - 1.3.2. Recommended Limitations
2. **Attributes**
 - 2.1. Attribute Transformation
 - 2.1.1. The authContextParams Attribute
3. **Identity Provider User Interface**
 - 3.1. General Requirements
 - 3.2. Automatic Start of the BankID Client
 - 3.3. Prompting for Personal Identity Number (personnummer)
 - 3.4. Cancelling an Operation
4. **Authentication Requests**
 - 4.1. Binding and Security Requirements
 - 4.2. Authentication for Signature
 - 4.2.1. Input to BankID Signing
 - 4.2.1.1. userVisibleData - Signature Message
 - 4.2.1.2. userNonVisibleData
 - 4.2.2. Mobile BankID and the personNumber attribute
5. **Authentication Responses**
 - 5.1. Attribute Release Rules
 - 5.2. Error Responses
6. **Metadata**
 - 6.1. Service Providers
 - 6.2. Identity Providers
 - 6.3. Signature Services
7. **References**
8. **Changes between versions**

1. Introduction

This profile defines how a SAML Identity Provider that offers authentication using the Swedish BankID technology should implement its services to be compliant with the Swedish eID Framework. It extends the "Deployment Profile for the Swedish eID Framework", [[EidProfile](#)], with requirements and recommendations for Identity Providers offering BankID authentication and signature services.

The BankID interface for authentication and signature, the Relying Party Interface, is described in the "BankID Relying Party Guidelines", [[BankID_Spec](#)], specification. This specification MUST be fully implemented and supported by BankID Identity Providers compliant with the Swedish eID Framework specifications.

1.1. Requirements Notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)].

The use of SHOULD, SHOULD NOT, and RECOMMENDED reflects broad consensus on deployment practices intended to foster both interoperability and guarantees of security and confidentiality needed to satisfy the requirements of many organizations that engage in the use of federated identity. Deviating may limit a deployment's ability to technically interoperate without additional negotiation, and should be undertaken with caution.

1.2. References to SAML 2.0 Standards and Profiles

When referring to elements from the SAML 2.0 core specification [[SAML2Core](#)], the following syntax is used:

- `<saml2p:Element>` – for elements from the SAML 2.0 Protocol namespace.
- `<saml2:Element>` – for elements from the SAML 2.0 Assertion namespace.

When referring to elements from the SAML 2.0 metadata specifications, the following syntax is used:

- `<md:Element>` – for elements defined in [[SAML2Meta](#)].
- `<mdattr:Element>` – for elements defined in [[SAML2MetaAttr](#)].

1.3. BankID Methods and Applications

There are three types of BankID:

- Mobile BankID - End users use the "BankID app" on their mobile devices to authenticate or perform a signature. In these cases the user certificate is stored in the app and protected by a personal code.
- BankID on file - End users use the desktop program "BankID Security Application" to authenticate or perform a signature. The user certificate is stored in a file on the computer and is protected by a user password.
- BankID on card - End users make use of the same desktop program as described above, but the certificate is placed on a smart card. The user private key is unlocked using the PIN-pad on the smart card reader.

The three above methods are all "BankID", but historically, relying parties have made a difference between "Mobile BankID" and "BankID" (the original desktop version).

1.3.1. Representation as Identity Providers

An actor offering BankID services can choose to use **one** BankID Identity Provider supporting all different BankID methods, or use **several** Identity Provider instances, one for each BankID method.

Services that support all methods within one Identity Provider instance usually displays a question to the user before authentication starts, where the user chooses between "Using BankID on this device or another device". In an environment where a discovery service (or similar) is being used, this means that the user has to make two choices before the actual authentication process starts; first at the discovery service where the user selects "BankID" and then at the BankID Identity Provider where the user selects the type of BankID authentication to use.

It is RECOMMENDED that BankID services are split into separate Identity Providers for each supported BankID method. The reasons for this are the above argument about discovery, but also the fact that a Service Provider should be able to select which type of authentication that is required (for example, Mobile BankID may be accepted but not BankID on file).

1.3.2. Recommended Limitations

The table below states the RECOMMENDED support and behaviour when support for BankID is implemented using separate Identity Providers (as recommended in section 1.3.1 above).

Identity Provider	Desktop	Mobile Phone	Tablet
Mobile BankID	Start BankID on other device ¹ (mobile phone or tablet).	Start BankID on the same device ² .	Prompt the user to ask whether to start BankID on the tablet or on another device ³ (mobile phone).
BankID on file (or on card)	Start BankID on the same device ⁴ .	Not supported ⁵ .	Not supported ⁵ .

1. The user initiates a BankID operation from his or hers desktop computer and selects to use Mobile BankID. In this case the Mobile BankID app is started on another device (since Mobile BankID does not exist on desktop computers).
2. The user initiates a BankID operation from his or hers mobile phone and selects to use Mobile BankID. In this case the BankID app is started on the same device. It is highly unlikely that a user uses one mobile phone to visit a service and wants to use his or hers BankID on another device.
3. The user initiates a BankID operation from his or hers tablet and selects to use Mobile BankID. In this case the recommendation is to prompt the user to ask whether the Mobile BankID app should be automatically started on the tablet, or if the user wishes to use BankID on another device (probably a mobile phone). The reason for this recommendation is that most users have a BankID on their mobile phones, but not necessarily on their tablets.
4. The user initiates a BankID operation from his or hers desktop computer and selects to use BankID on file. The BankID Security Application is started on the same computer. It is not a likely use case to use one computer to connect to the service and another one for BankID.
5. This case should not be supported. If the user selects "BankID on file" from a mobile phone or tablet, the Identity Provider should display an error message stating that Mobile BankID should be used instead and post an error response back to the Service Provider.

Note: Items 4 and 5 above also apply to BankID on card. A service MAY choose to implement BankID on file and BankID on card as separate Identity Providers or as one Identity Provider instance.

For Identity Providers implementing BankID support in **one** Identity Provider instance it is RECOMMENDED to make the assumption that the BankID app should be started on the same device if the user connects via a mobile phone.

2. Attributes

An BankID Identity Provider use the BankID Relying Party API, as described in [[BankID_Spec](#)], to communicate with the BankID-server when providing its services to end users. When a BankID-operation has completed successfully, the Identity Provider (the BankID Relying Party) invokes the collect-method to obtain the result from the operation.

The table [below](#) contains attribute transformation mappings between attributes from a collect-method response as described in section 13.2 of [[BankID_Spec](#)] and attributes defined within the Swedish eID Framework as defined in [[EidAttributes](#)].

An Identity Provider should not necessarily release all transformed attributes received from the BankID-server to the Service Provider. See further section [5.1](#), "[Attribute Release Rules](#)".

2.1. Attribute Transformation

BankID attribute	SAML Attribute	Description
orderRef	transactionIdentifier urn:oid:1.2.752.201.3.2	The BankID order reference received from a BankID Auth- or Sign-method invocation. This parameter is supplied as an input parameter to the collect-call and is the unique transaction identifier for the BankID-operation.
completionData. user.personalNumber	personalIdentityNumber urn:oid:1.2.752.29.4.13	Swedish "personnummer". 12 digits without hyphen.
completionData. user.givenName	givenName urn:oid:2.5.4.42	User's given name.
completionData. user.surname	sn urn:oid:2.5.4.4	User's surname.
completionData. user.name	displayName urn:oid:2.16.840.1.113730.3.1.241	User's given name and surname.
completionData. cert.notBefore	<i>bankidNotBefore</i> key in authContextParams urn:oid:1.2.752.201.3.3	Start of validity of user's BankID. No direct attribute mapping exists, but may be represented as key-value pair in authContextParams, where the key is <i>bankidNotBefore</i> , see 2.1.1 below.
BankID attribute	SAML Attribute	Description
completionData. cert.notAfter	<i>bankidNotAfter</i> key in authContextParams urn:oid:1.2.752.201.3.3	End of validity of user's BankID. No direct attribute mapping exists, but may be represented as key-value pair in authContextParams, where the key is <i>bankidNotAfter</i> , see 2.1.1 below.
completionData. device.ipAddress	<i>bankidUserAgentAddress</i> key in authContextParams urn:oid:1.2.752.201.3.3	The IP-address of the user agent presented to the BankID server. In cases where a user uses BankID "on another device" this address may not be the same as the web user agent. No direct attribute mapping exists, but may be represented as key-value pair in authContextParams, where the key is <i>bankidUserAgentAddress</i> , see 2.1.1 below.

completionData. signature	userSignature urn:oid:1.2.752.201.3.11	The signature applied by the user as part of the authentication/signature process.
completionData. ocspResponse	authServerSignature urn:oid:1.2.752.201.3.13	The OCSP response signed by the BankID issuer that proves that the user BankID was checked for revocation.

2.1.1. The authContextParams Attribute

The authContextParams attribute, see section 3.2.1 of [\[EidAttributes\]](#), is a general purpose attribute to be used when non-standardized authentication data is to be transferred in a SAML assertion.

The attribute is used by attribute providers to release data from an authentication process that has no attribute definition of its own. Thus, should the BankID attributes completionData.cert.notBefore, completionData.cert.notAfter and completionData.device.ipAddress be transformed and included into an assertion, they would have to be placed as key-value pairs of the authContextParams attribute as the example below.

```
<saml2:Attribute xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    FriendlyName="authContextParams"
    Name="urn:oid:1.2.752.201.3.3"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
  <saml2:AttributeValue xsi:type="xs:string">
    bankidNotBefore=2016-05-30T09%3A30%3A10Z;bankidNotAfter=2018-05-30T09%3A30%3A10Z;bankidUserAgentAddress=85.229.202.232
  </saml2:AttributeValue>
</saml2:Attribute>
```

The example above represents the following BankID attributes and values:

- completionData.cert.notBefore = 2016-05-30T09-30-10Z
- completionData.cert.notAfter = 2018-05-30T09-30-10Z
- completionData.device.ipAddress = 85.229.202.232

The format for the notBefore and notAfter attributes should be the representation as given by the XML type xs:dateTime.

3. Identity Provider User Interface

This profile does not state any requirements on how the user interface for an Identity Provider implementing BankID services should be implemented other than the statements listed in the sub sections below.

3.1. General Requirements

The user interface for a BankID Identity Provider SHOULD use the recommended user and error messages as defined in sections 5, "Recommended User Messages", and 10, "Recommended Terminology", of [\[BankID_Spec\]](#).

The user interface for a BankID Identity Provider MUST display information about the Service Provider that sent the request. It is RECOMMENDED that this information is obtained from the `<mdui:UIInfo>` element from the Service Provider's metadata entry.

It MUST be clear to the whether an authentication or a signature process is ongoing.

When an error occurs during an authentication or signature operation, the Identity Provider MUST display an error message that can be easily understood by the end user, and offer the possibility to acknowledge the error so that an error response may be posted back to the requesting Service Provider (as specified in section 6.4, "Error Responses", of [\[EidProfile\]](#)).

3.2. Automatic Start of the BankID Client

When an operation is initiated where the BankID client (app or desktop program) is on the same device as the user agent (web browser) the Identity Provider SHOULD attempt to "auto start" the BankID client as described in [\[BankID_Spec\]](#).

For the above cases where the BankID client is automatically started from the Identity Provider, the Identity Provider user interface SHOULD NOT ask for the user's personal identity number. This information is available in the "BankID app" or "BankID Security Application".

Auto starting the BankID app from a mobile device requires the built-in web browser to be used to guarantee full support, see section 3.1 of [\[BankID_Spec\]](#). If the Identity Provider detects that the user is not using the platform's default browser it SHOULD ask the user to start the BankID app manually (and before that enter the personal identity number).

3.3. Prompting for Personal Identity Number (personnummer)

When the user agent (web browser) and the BankID client (app or desktop) is not on the same device the Identity Provider prompts the user for his or hers personal identity number (personnummer) in order to initiate an BankID authentication. It is RECOMMENDED that the personal identity number is saved in the user's web browser session storage (in a session cookie or more preferably using the HTML5 sessionStorage object). The reason for this is that if the user performs a signature operation after authenticating he or she does not expect to have to enter the personal identity number again.

See also section 4.2.2, "[Mobile BankID and the personNumber attribute](#)".

3.4. Cancelling an Operation

A BankID Identity Provider SHOULD include a Cancel-button in the user interface enabling the possibility for the user to cancel the BankID operation.

In cases where the BankID app is on another device than the user agent and the Identity Provider has received notification from the BankID-server that the app has been started by the user, it is RECOMMENDED that the Cancel-button in the Identity Provider user interface is hidden or disabled. The reason for this is that the BankID app itself has a Cancel-button, and if the user

cancels the operation using the Cancel-button in the Identity Provider user interface instead of in the app itself, the app will be left dangling until it times out and during that time the user may be prevented from using its BankID.

Another thing to pay attention to is the case where the user clicks the Cancel-button in the Identity Provider user interface before starting the BankID app. The session against the BankID-server may then have been started, but since there are no ways of cancelling a BankID-session, the user will be prevented from starting a new session until the previous session times out. A suggestion in the cases where a BankID-session was started, is that the Identity Provider initiates a new BankID-operation in order to "kill" the previous one (the newly created session will also be invalidated by the BankID-server).

4. Authentication Requests

4.1. Binding and Security Requirements

An Identity Provider conformant with this profile MUST require `<sam12p:AuthnRequest>` messages to be signed (by indicating this in its metadata, see section 6, "[Metadata](#)"). Thus, the Identity Provider MUST not accept messages that are not signed, or where the verification of the signature fails. In these cases the Identity Provider MUST respond with an error.

4.2. Authentication for Signature

An Identity Provider conforming to the Swedish eID Framework is obliged to handle requests received from Signature Services as described in section 7, "Authentication for Signature", of [\[EidProfile\]](#). This section further specifies how a BankID Identity Provider should support "authentication for signature".

A BankID Identity Provider that receives an `<sam12p:AuthnRequest>` message from a Signature Service MUST initiate a BankID **signature** operation. It MUST NOT initiate a BankID authentication operation for several reasons:

- the user interface in the BankID client (app or Desktop program) during authentication indicates that the user is logging on (and not signing which is the case when a request from a Signature Service is being processed),
- the user expects to be displayed a text describing what he or she is signing,
- and most importantly, BankID is PKI-based and has support for signing using a non-repudiation key, so there is no reason not to use this function.

The BankID client (app or desktop program) comprises a text box in which the signature message is displayed for the user. A BankID Identity Provider MUST NOT display the signature message in any other way than in this text box. How the signature message is assigned is specified below.

4.2.1. Input to BankID Signing

An Identity Provider that processes an `<sam12p:AuthnRequest>` from a Signature Service is not given the actual data that is being signed by the user via the Signature Service. However, in order to invoke the BankID signature function, the Identity Provider must supply the BankID-server with data to be signed. This section specifies the input to the BankID signature operation.

The "To-be-signed" data that is passed as input to the BankID `Sign`-method is a combination of the data from the `userVisibleData` and `userNonVisibleData` parameters (section 13.1.2 of [\[BankID_Spec\]](#)).

4.2.1.1. userVisibleData - Signature Message

The `Sign`-method parameter `userVisibleData` holds data that will be signed by the user but it is also displayed in the BankID application text box.

If the `<sam12p:AuthnRequest>` message contains a `SignMessage` extension, the contents of this message MUST be assigned to the `userVisibleData` parameter (after necessary encoding).

A BankID Identity Provider MUST only process `SignMessage` elements having their `mimeType` attribute set to `text`¹. For any other values (`text/html` or `text/markdown`), the Identity Provider MUST respond with an error.

If the `<sam12p:AuthnRequest>` message does not contain a `SignMessage` extension, the Identity Provider MUST assign a sensible default signature message to the `userVisibleData` parameter. How this message is constructed is the responsibility of the Identity Provider, but it must be obvious for the user who is the requesting party, i.e., the Service Provider that has ordered the signature operation².

[1]: If the `MimeType` attribute is not set, `text` is the default value.

[2]: For this purpose, the `<mdui:DisplayName>` element of the Signature Service's metadata entry, is a good and generic choice.

4.2.1.2. userNonVisibleData

In order to produce a BankID signature that contains a connection to the `<saml2p:AuthnRequest>` message that initiated this signature, a BankID Identity Provider compliant to this profile **MUST** assign the `userNonVisibleData` parameter with data that uniquely binds the signature to the `<saml2p:AuthnRequest>` message.

It is **RECOMMENDED** that the following function is used to produce this unique binding:

```
Base64Encode("entityID=" + URLEncode(<entityID of SP>) + ";" + "authnRequestID=" + URLEncode(<ID of AuthnRequest>))
```

4.2.2. Mobile BankID and the personNumber attribute

When Mobile BankID is being used to sign data and the user has initiated the signature operation against the Signature Service from another device (desktop och tablet) the `personNumber` parameter must be assigned in the BankID sign-call. This information is not passed in the `<saml2p:AuthnRequest>` message sent from the Signature Service. In these cases the Identity Provider **SHOULD** rely on the fact that the user, most likely¹, already has been authenticated at the Identity Provider, and use the personal identity number given when the user authenticated also for the signature operation (see section 3.3, "[Prompting for Personal Identity Number \(personnummer\)](#)", above). Only in cases when the Identity Provider can not obtain the personal identity number should a dialogue asking the personal identity number be displayed.

[1]: Almost all use cases where a user signs data is preceded by a login (authentication).

5. Authentication Responses

5.1. Attribute Release Rules

Section 2.1, "[Attribute Transformation](#)", specifies how BankID attributes should be transformed into SAML attributes defined in [\[EidAttributes\]](#). However, it does not specify the attribute release rules stating which attributes that are to be released based on a particular request.

A BankID Identity Provider compliant to the Swedish eID Framework MUST honor the attribute release rules specified in section 6.2.1, "Attribute Release Rules", of [\[EidProfile\]](#). This section further extends these rules with the following:

- A BankID Identity Provider SHOULD include the `transactionIdentifier`-attribute (a mapping of the BankID `orderRef`-attribute) in the `<saml2:AttributeStatement>` element independently of which attribute set that is requested. This attribute links the BankID operation to the assertion.
- It is RECOMMENDED that a BankID Identity Provider includes the `userSignature`-attribute (containing the BankID signature) in the `<saml2:AttributeStatement>` element when a BankID signature operation has been performed.
- Unless explicitly required¹ by the Service Provider the Identity Provider SHOULD NOT release any other attributes than those specified by the current attribute set(s)².

[1]: A Service Provider explicitly requests attributes by declaring them as requested attributes in the `<md:AttributeConsumingService>` element of the Service Provider's metadata entry. See section 6.1.

[2]: Based on the service entity categories that a Service Provider has declared in its metadata, an Identity Provider derives which attribute sets to apply during attribute release.

5.2. Error Responses

A BankID Identity Provider MUST map errors received from the underlying BankID-server into SAML error response messages where the top level status code is either:

- `urn:oasis:names:tc:SAML:2.0:status:Requester` - for errors that are due to authentication or signature failures or faults due to an error on the part of the Service Provider,
- `urn:oasis:names:tc:SAML:2.0:status:Responder` - for errors that are due to an internal, or technical, error in the BankID-server or Identity Provider.

Before a `<saml2p:Response>` message is posted back to the Service Provider the Identity Provider MUST display a relevant error message to the user.

It is RECOMMENDED that authentication/signature errors and failures to start the BankID client are represented using the second level status code `urn:oasis:names:tc:SAML:2.0:status:AuthnFailed`.

If the user cancels a BankID operation, either by clicking the Cancel-button in the Identity Provider user interface or the Cancel-button in the BankID app/Security Application, the Identity Provider SHOULD respond with a `<saml2p:Response>` message where the second level status code is `http://id.elegnamnden.se/status/1.0/cancel`.

In cases where the Identity Provider receives the BankID error code `ALREADY_IN_PROGRESS` in response to an `Auth`- or `Sign`-call the Identity Provider MAY display a warning to the user that someone may have initiated a BankID operation using their personal identity number¹. If this warning is displayed, it is RECOMMENDED that the second level status code `http://id.elegnamnden.se/status/1.0/possibleFraud` is included in the error response message posted back to the Service Provider.

s> [1]: There have been reports where fraudsters remotely try to convince people of using their Mobile BankID to log in to a service. In these cases, the fraudster initiates a BankID authentication prior to the person he tries to trick into logging in to the service, and is waiting for the user to enter his or hers personal code, thus authenticating the fraudsters session.

6. Metadata

This section extends section 2 of [\[EidProfile\]](#) with requirements specific for BankID.

6.1. Service Providers

As stated in section 5.1, "[Attribute Release Rules](#)", a Service Provider may request additional attributes, other than those implicitly requested via the use of service entity categories, by declaring requested attributes under the `<md:AttributeConsumingService>` element.

```
<md:AttributeConsumingService index="0" isDefault="true" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:ServiceName xmlns:xm1="http://www.w3.org/XML/1998/namespace" xml:lang="sv">E-myndigheten</md:ServiceName>
  <md:ServiceName xmlns:xm1="http://www.w3.org/XML/1998/namespace" xml:lang="en">The e-Authority</md:ServiceName>
  ...
  <md:RequestedAttribute Name="urn:oid:1.2.752.201.3.2" isRequired="false"/>
  <md:RequestedAttribute Name="urn:oid:1.2.752.201.3.13" isRequired="false"/>
</md:AttributeConsumingService>
```

Example of how a Service Provider declares that it wishes to receive the transactionIdentifier and authServerSignature attributes in assertions.

A Service Provider requesting an attribute that is not supported by all Identity Providers that it may communicate with MUST NOT set the `isRequired` attribute of the `<md:RequestedAttribute>` element to true.

It is RECOMMENDED that Service Providers communicating with BankID Identity Providers include the `transactionIdentifier` attribute as a requested attribute.

6.2. Identity Providers

A BankID Identity Provider MUST require authentication request messages to be signed. This is indicated by assigning the `wantAuthRequestsSigned` attribute of the `<md:IDPSPDescriptor>` element to a value of true.

6.3. Signature Services

It is RECOMMENDED that a Signature Service explicitly requires release of the `userSignature` attribute (`urn:oid:1.2.752.201.3.11`) in assertions. The reason for this is that the BankID-signature may then be part of the assertion that is included in the resulting signature created by the Signature Service giving a non-repudiation proof of the BankID signature process.

```
<md:AttributeConsumingService index="0" isDefault="true" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  <md:ServiceName xmlns:xm1="http://www.w3.org/XML/1998/namespace" xml:lang="sv">E-myndighetens underskriftstjänst</md:ServiceName>
  <md:ServiceName xmlns:xm1="http://www.w3.org/XML/1998/namespace" xml:lang="en">The e-Authority's Signing Service</md:ServiceName>
  ...
  <md:RequestedAttribute Name="urn:oid:1.2.752.201.3.11" isRequired="false"/>
</md:AttributeConsumingService>
```

Example of how the userSignature attribute is explicitly required.

7. References

[RFC2119]

Bradner, S., Key words for use in RFCs to Indicate Requirement Levels, March 1997.

[SAML2Core]

OASIS Standard, Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2Meta]

OASIS Standard, Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0, March 2005.

[SAML2MetaAttr]

OASIS Committee Specification, SAML V2.0 Metadata Extension for Entity Attributes Version 1.0, August 2009.

[BankID_Spec]

BankID Relying Party Guidelines, version 3.1.

Check www.bankid.com/rp/info for latest version.

[EidProfile]

Deployment Profile for the Swedish eID Framework.

[EidAttributes]

Attribute Specification for the Swedish eID Framework.

8. Changes between versions

Changes between version 1.0 and 1.1:

- Section 3.4, "Cancelling an Operation" was extended with a suggestion of how to avoid dangling sessions after user cancel.
- The profile now references the BankID Relying Party Guidelines that makes use of JSON.