Policy for Packaging of Swedish BankID E-Signatures for Long-Term Validation

1 Policy ID and location

Policy ID	urn:signicat:packagingpolicy:bankid-se:1.2
As part of com bined policy ID[1]	urn:signicat:packagingpolicy:[LTV packaging policy name]:bankid-se:[LTV packaging policy version]:1.2
Name	Policy for Packaging of Swedish BankID E-Signatures for Long-Term Validation

2 Version

Date	Specification version	Change
2014-10-16	1.2	- Extracted the non signature specific rules from the combined packaging policy document for urn:signicat:packagingpolicy:ltv:bankidse:1.1:1.2, into a separate policy document for the LTV policy - Added profile rules by including the content of "LTV-SDO Profile for Packaging of Swedish BankID E-Signatures for Long-term Validation 1.3". There were no changes in profile rules. - Corrected and extended description of document-reference-list - Removed URL

3 Introduction

This packaging policy defines requirements for packaging of Swedish BankID e-signatures, in the context of signature creation and initial verification, for the purpose of implementing long-term validation support.

This policy needs to be combined by an LTV packaging policy.

3.1 About Packaging Policies

The purpose of a packaging policy is to specify requirements for the packaging process, and high-level

[1] This policy needs to be combined by an LTV packaging policy, and they may be referenced together using a combined Policy ID.

requirements for the prior signature creation and verification process.

The primary users of this policy will be e-signature users (relying parties). The policy will help e-signature users to better understand the information contained in a package, and on what basis it can be trusted and used.

The policy will also be useful for implementers of the packaging service.

3.2 The relation to a LTV packaging policy

This *signature packaging policy* will define requirements that are specific to the type of signature that is subject to packaging.

It needs to be accompanied by a general *LTV packaging policy,* defining requirements that are not specific to the signature type.

3.3 Scope

This packaging policy defines requirements for packaging of Swedish BankID e-signatures for long-term validation in context of with the signature creation and initial verification.

The policy also sets some high level requirements for the creation and verification processes, including collection of data needed by the packaging process.

The policy does not set detailed requirements for the signature creation and verification processes[2].

3.4 Structure

The normative parts of the policy are listed below.

1. **Signature creation requirement** defines requirements for the creation of the packaged signature (the “native” signature).
2. **Signature verification requirements verification** defines requirements for the verification of the native signature.
3. **Signature enrichment and hardening requirements** defines requirements for the signature enrichment and hardening process.
4. **LTV-SDO profile** defines how to use the LTV-SDO format.
5. **Trust anchors** used in validation of the native signature

3.5 Versioning and backwards compatibility

Packaging policy version numbers consists of a major and a minor number, denoting major and minor versions.

A change of minor version is always backwards compatible, and and the new policy may be brought into effect without notifying relying parties.

A change of major version may introduce non-backwards compatible changes.

[2] The detailed requirements for signature creation/verification are given by BankID.

3.6 Contents

3.7 Terms and acronyms

Term	**Explanation**
TSP	Trusted Service Provider - the entity implementing this policy by packaging the signature.
Long-term validation	The concept of validating an e-signature long time (months, and some times years) after it was created.
Native signature	The e-signature that is to be packaged for long-term validation
Original document	The document signed with the native signature
Signature enrichment	The addition of extra information about the document, the signer, the context or the signing and verification process.
Signature hardening	The addition of information that strengthens the non-reputability of the signature.
Native signature qualifying properties	A common term for information that strengthens the native e-signature and makes it suitable for long-term validation.
Seal	This is the Trusted Service Providers signature on the package. It is commonly referred to as the *Seal* .
XMLDSig	W3C XML Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/

3.8 References

Short name	Resource
XAdES	ETSI TS 101 903: “XML Advanced Electronic Signatures (XAdES)
BankID Relying Party Guidelines	BankID Relying Party Guidelines. Version 2.5 2014-06-17

4 Signature creation requirements (normative)

This section defines requirements for the creation of the packaged signature (the “native” signature).

1. The signer's certificate must have one of the following Certificate Policy Identifiers
   a) 1.2.752.78.1.1 (BankID on file)
   b) 1.2.752.78.1.2 (BankID on smart card)
   c) 1.2.752.71.1.3 (Nordea e-id on file and on smart card)
   d) 1.2.752.78.1.5 (Mobile BankID)
2. The document to be signed can be on one of the following formats:
   a) Plain text
   b) PDF
3. Signature creation is performed according to the BankID requirements and guidelines at signature creation time.
4. The document may be signed as part of a *document-bundle*, using a *document-bundle signature.* Process and format requirements for document-bundle signatures are defined below.
5. Signing of PDF documents is implemented as document bundle signatures (described below), with a single PDF document in the document bundle.

4.1 Document-bundle signature

A document-bundle signature is a native signature over a list of document references to the originals. The originals are cryptographically bound to the signature through the use of secure hash functions. The references, which are covered by the native signature, includes secure digests of the originals.

4.2 Process requirements for document-bundle signatures

1. Before the BankID client is launched, all documents in the bundle are shown to the user, with an option to explicitly sign these documents, typically a button labeled «sign».
2. If the user chooses to sign the presented documents, the service provider then produces the data to be signed directly by the BankID signature. The data to be signed will include a *visible signtext*, and a *document reference list*.

a) The *visible signtext* is a descriptive text identifying the documents that are signed. This text is to the RP Web Service Sign method in the parameter *userVisibleData*, and the BankID client shows it to the user.

b) The *document reference list* is a data structure containing references to the originals. It is sent to the RP Web Service Sign method in the parameter *userNonVisibleData*. It will not be shown to the user.

4.3 Signature format requirements for document-bundle signatures

The data to be signed by the BankID client will include a *visible signtext*, and a *document reference list* (also referred to as *attachments)*.

The visible signtext is sent to the RP Web Service Order method in the parameter *userVisibleData*. BankID will include it into the signature. Currently, BankID will include this text in the bankIdSignedData/usrVisibleData element, base-64 encoded.

The document reference list is a JSON structure containing the information defined in the table below for each reference, that is for each original. It is sent to RP Web Service Order method in the parameter *userNonVisibleData*. BankID will include it into the signature. Currently, BankID will include this text in the bankIdSignedData/usrNonVisibleData element, base-64 encoded .

4.3.1 Document reference list format

The document reference list is a JSON object with the following elements:

Element	**Syntax**	**Semantics**
attachments	JSON Array	The list of document references, or "attachments"
documentDescription	String	A short description of the document.
mimeType	String	The MIME-type of the document.
serialNumber	non-negative integer	The document's position in the bundle, counting from zero
digestValue	String (length depends on the digest algorithm)	The first secure hash of the document, calculated using the primary-digest-algorithm, Base64-encoded
digestMethod	JSON Object	Set of properties describing the method used to obtain the digest value
digestMethod/algorithm	URI	Identifies the hash algorithm used for producing the primary digest
secondaryDigestValue	String (length depends on the digest algorithm)	The second secure hash of the document, calculated using the secondary-digest-algorithm, Base64-encoded
secondaryDigestMethod	JSON Object	Set of properties describing the method used to obtain the digest value

secondaryDigestMethod/algorithm	URI	Identifies the hash algorithm used for producing the secondary digest

4.3.2 Bundle-Index

When packaging document-bundle signatures, the resulting package will represent the signature of one of the documents in a document bundle. In addition to the visible signtext and the document reference list, the package must contain an index into the reference-list defining which of the referenced documents this package is a signature on. This index is called a “bundle-index”, and is found in the element “//LtvSdo/NativeSignature/BundleIndex”.

4.3.3 OriginalDocument

When packaging document-bundle signatures, the NativeSdo will not contain the original document. It must therefore be stored separately, either by including it in the package directly, or by XMLDSIG references.

If included into the package directly, called *enveloped original inclusion mode*, the original will be in the element “//LtvSdo/NativeSignature/OriginalDocument”.

If included into the package by reference, called *detached original inclusion mode*, the original will not be in the LtvSdo XML, but referred to in a SignInfo reference in the package *seal*, and as such covered by the seal.

5 Signature verification requirements (normative)

This section defines requirements for the verification of the native signature.

1. Signature verification is done according to current BankID requirements and guidelines at signature verification time.
2. Signature verification is done by the BankID RP Service. The TSP must make sure that such verification was done, and that is was successful, using the API of the BankID RP service. This policy does not define the requirements for the verification done by the BankID RP service.
3. In addition, to ensure the quality and completeness of validation data included in the package, signature verification is performed separately by the TSP. Signature verification includes (but is not limited to) :
    a) verifying that the cryptographic signature was created over the expected signtext, including the original document, by using the signer private key corresponding to the public key in the included signer certificate.
    b) certificate path validation of the signer certificate, including revocation check. The trust anchors used in certificate path validation are specified in Appendix A.

6 Signature enrichment and hardening requirements (normative)

This section defines requirements for the signature enrichment and hardening done as part of the packaging.

6.1 Native Signature Qualifying Properties

The following information is included in the package as native signature qualifying properties:

1. The confirmed signing time, as collected by the TSP from a trusted time source.
2. Revocation information for the BankID end-user certificate at signing time, as an OCSP response. The OCSP response is signed by an OCSP signing certificate that is included in the OCSP response, and directly or indirectly issued by one of the end user certificate trust anchors in Appendix A.

Notes

- The certificate chain for the end user certificate and the OCSP certificate is included in the native signature
- Revocation information for the certificate chain is not included, as it is not available from the BankID infrastructure.

6.2 Signature creation context

The following information is collected from the *signature creation context*

Information about the client platform, including:

1. Client OS and browser as provided by the client browser.
2. Client configuration as provided by the BankID client

Information about the server platform:

3. List of important server software components with versions

Information about the BankID infrastructure:

4. Version of the BankID RP Web Service

6.3 Signature verification context

The following information is collected from the *signature verification context*:

Information about the server platform:

1. Name and versions of important server software components.

6.4 Signature external context

The following information is collected from the *signature external context*:

1. The description of the external context as provided by the user of the packaging service.

6.5 Additional information

None *additional information elements* are collected.

6.6 Audit trail

Audit trail entries are collected for important events, for the purpose of strengthening the non-reputability of the signature, and to support forensics.

7 LTV-SDO Profile (normative)

7.1 Introduction

This chapter defines the profile for use of LTV-SDO for packaging of Swedish BankID E-Signatures for Long-term Validation. See also the general LTV-SDO profile defined in the LTV Packaging Policy.

7.2 About LTV-SDO profiles

The LTV-SDO format is a generic format for packaging e-signatures for Long-term Validation. An *LTV-SDO Profile* specifies how the LTV-SDO format is used for a specific means, and in a specific context, by defining additional requirements and constraints to which XML Elements and attributes must be present, their possible values, and the semantics of these their values.

7.3 Description/SignerDescription

Element/Attribute	**Semantics**	**Format/possible values**	**Required**
SignerDisplayName	The signers name	A string with the signers name.	Yes
SignerUniqueId	An ID that uniquely identifies the signer in the scope of the signature type. For BankID, this is the "*personnummer*".	The *personnummer* for the signer.	Yes
SignerNationalId	The signers *national id* identifies the signer by some nation-wide ID-number. This value is tightly connected with *SignerNationality* and *SignerNationalIdType*.	The *personnummer* of the signer.	Yes
SignerNationality	The nationality for the *SignerNationalId.*	"SE"	Yes
SignerNationalIdType	The type of national id given in *SignerNationalId.*	"PERSNR"	Yes

Attribute *)	**Semantics/description**	**Format/possible values**	**Required**
bankid-se/firstname	First name of the holder, as found in the BankID certificate (Given Name attribute of the subject DN)	String	No
bankid-se/lastname	Last name of the holder, as found in the BankID certificate (Surname attribute of the subject DN)	String	No

*) Elements of type Attribute with the given values for attributes name-space/name

7.4 Description/DocumentDescription

Element/Attribute	Semantics	Format/possible values	Required
DocumentMimeType	Mime Type of the original document	A string with a valid MIME Type. *Example:* “application/pdf”.	Yes
DocumentTitle	Short description of the original document, suitable to be used as title.	A relatively short string with a document title. *Example:* “Loan Agreement”	Yes
DocumentDigest	Digest of the original, unsigned document. Algorithm must be SHA-256 or better.	String, containing the Base64-encoded hash of the document.	Yes
DocumentDigest@alg	The actual hash algorithm used to compute the value of DocumentDigest	A String containing the algorithm identifier. Possible values are algorithm identifiers defined by W3C, for example: http://www.w3.org/2001/04/xmlenc#sha256	Yes

7.5 Description/SignatureDescription

Element/Attribute	Semantics	Format/possible values	Required
SignatureTypeFriendlyName	Descriptive name of the e-signature type, suitable to present to the end user	Always “BankID”	Yes
SignatureFormatFriendlyName	Descriptive name of the e-signature format, suitable to present to the end user.	Always “XML Signature”	Yes
SigningTime	An approximation of the time the signature was created. Collected by the verifier from a secure time source immediately after the signature is received from the	xades:signingTime (XML DateTime) value.	Yes

	signature creation client.		

7.6 NativeSignature/NativeSdo

Element/Attribute	Semantics	Format/possible values	Required
(element content)	The e-signature as produced by the BankID Client.	String, containing the Base64-encoded XML Signature	Yes
@Format	The format of the signed data object, as a Signicat format identifier.	Always " urn:ksi:names:SAML:2.0:df:xmldsig"	Yes
@Version	The version of the format of the signed data object.	String containing the version number	Yes
@MimeType	The mime type of the signed data object.	Always "application/x-xml-dsig"	Yes

7.7 NativeSignature/NativeSignatureQualifyingProperties

Element/Attribute	Semantics	Format/possible values	Required
SigningTime	The signing time, as collected by the TSP from a trusted time source.	xades:signingTime (XML DateTime) value.	Yes
RevocationValues	Revocation information that was used during initial verification of the BankID signature.	Base64-encoded OCSP response for the BankID signer certificate. Follows the XAdES formatting rules for xades:RevocationValues	Yes

7.8 NativeSignature/BundleIndex

Element/Attribute	Semantics	Format/possible values	Required
(element content)	Present when this LtvSdo is part of a document-bundle signature. Contains the index into the bundle of the signed document represented by this LtvSdo.	Zero-based non-negative integer	No

7.9 AdditionalInfo/SignerAttributes

Attribute *)	Semantics/description	Format/possible values	Required
(none)	-	-	-

*) Elements of type Attribute with the given values for attributes namespace/name

8 Appendix A (normative): Trust anchors used in validation of the native signature

The following certificates are used as trust anchor in Certificate Path Validation and OCSP Response validation when validating the native signature.

8.1 BankID Root CA v1

```
Subject: O=Finansiell ID-Teknik BID AB, OU=BankID Member Banks CA, CN=BankID Root CA v1
Not Before: Dec  7 12:43:45 2011 GMT
Not After : Dec 31 12:43:45 2034 GMT
```

```
-----BEGIN CERTIFICATE-----
MIIFwDCCA6igAwIBAgIIMR5YYFp1W4EwDQYJKoZIhvcNAQENBQAwYzEkMCIGA1UE
CgwbRmluYW5zaWVsbCBJRC1UZWtuaWsgQklEIEFCMR8wHQYDVQQLDBZCYW5rSUQg
TWVtYmVyIEJhbmtzIENBMRowGAYDVQQDDBFCYW5rSUQgUm9vdCBDQSB2MTAeFw0x
MTEyMDcxMjQzNDVaFw0zNDEyMzExMjQzNDVaMGMxJDAiBgNVBAoMG0ZpbmFuc2ll
bGwgSUQtVGVrbmlrIEJJRCBBQjEfMB0GA1UECwwWQmFua0lEIE1lbWJlciBCYW5r
cyBDQTEaMBgGA1UEAwwRQmFua0lEIFJvb3QgQ0EgdjEwggIiMA0GCSqGSIb3DQEB
AQUAA4ICDwAwggIKAoICAQDFlk0dAUwC63Dz6H/PN6BXL3XW7gFgMwmA9ZAJugBk
2B9OqDExybiZ86U7Q2Ha+5Q0JaHyLDRNz5hRB8hA/mgFYAcCSmHJTy2q5bTbFf2P
Y2SzW9VrY3x0ZR3s8D9+d8KLAWG2TpvYXfmqb+4LRd4SMskFhtBmL55uAoc5lKze
0wFi7O1o+cQP1TOG3Udjqu5jdZkGqZc7XTJzrQPSgyf4Y21tG1ohkHLgAVRDX0xT
nu8G+7Z1NJN7MX2AxyvOVl5kkepPtig+Z0UTyh0dXjdb7Fe/72BxeBqzEcib5Tvj
zqJFIBVqCFQG5iAVaDEblpgP4G6W7w0do7rCQNsAjxmpOuM7/pSi0q57pm2oIgsr
DPBKfugpuFVqUxtFlOw/2NUCoiydLRVJRitTqA49CDmXk56+cLg8Qn1fs9AoQTMg
w5ZYBo6Il79XvbgqV4Ov9tjM0DfQ1bWmB8GpKKUawaRDiikDvpSF6JMeFFQ1dF1b
w7hZYGgmZNaw1UWgYZjwogUgvJkWwYNPoqfgCHGk02bR46+ZErdipUdDsziMw2Ih
4pU3ERl2qxLN1X6I0AwsNotM96/fNENjwls6QhqG8Hgjf+/bR0bceg7mHJ2EwAxH
vPzi3RPD4xASfB3OMfRGwgnE1p+fc/pIwzLYUIVQtAQ7EIm+ArJ9BhQIroG6aHkv
hwIDAQABo3gwdjAdBgNVHQ4EFgQUZ4q6supIHHr1O2g3J3IG65Fjy1MwDwYDVR0T
AQH/BAUwAwEB/zAfBgNVHSMEGDAWgBRnirqy6kgcevU7aDcncgbrkWPLUzATBgNV
HSAEDDAKMAgGBiqFcE4BATAOBgNVHQ8BAf8EBAMCAQYwDQYJKoZIhvcNAQENBQAD
ggIBAFMeVmlLBIVAWAlmvqme34hG+k6c1HkPmgAGIZdtcJ1+XZ4MNUg9KKywTkNV
Aqcgy5gcIk3LM9HfHQ2JmUP54XSvXdr1B92m40Up4POH35mlmPZyqQVll0Ad5xrI
R86+HEk9BFmd+ukZ1AvSSSRZ/X7mcbBjcx34QaCVW2CeBdYSCzksjx0LOcEDgKNH
ToOQxrn8x//Ccc7Wf56Boq61JvjQAb1Q1E1BYKmXyJ8818SR1crvMU6xd68Akp0b
mJz7WDSvpjp10BrDyw1uTrn1qVlkOjllwPqHyUckTCAMmv0DkhmjcMSyzRWhAV9f
CTe17f7J+RYXBil9Z8/S4kCsatDGqLT5xgsCvsdca6haZUFh14npW3c8cmk3x6tg
0Nm1L0WxwyM2SOXJj/9vqaWMAq0qtv1izy/3rR0XuxSsw0fGv9LAG9KXcKPAobI/
itu2/3IbYFp2YOJ8GmQRZb8KsuIFxR7A4eB2ZcnlDgCCLIcyQhKt7e0JPkEp1cwM
prlCjCPu1KQrx/8zV5Z19muSw47ZHZ2hAciXKRe5dLsJySTShBqFfU4w8bV4pHfHE
thQ5CRGjBC6OFA7Fcd6rD8eByzaDyM5bDbkfgxBED5JQJrda1/mN1TxxtMrY6YeB
XDJdzaHTe7WXQRdXr5Jv+l1SIGJttNicNaam65wiiH7waAPH
-----END CERTIFICATE-----
```

8.2 BankID Root Certification Authority

```
Subject: O=Finansiell ID-Teknik BID AB, OU=BankID Member Banks CA, CN=BankID Root Certification
Authority

Validity
   Not Before: Oct 16 11:48:59 2002 GMT
   Not After : Oct 16 08:39:59 2019 GMT

-----BEGIN CERTIFICATE-----
MIID7DCCAtSgAwIBAgIQYx3dkWp0t1B/Gnb8ppQFGzANBgkqhkiG9w0BAQUFADB1
MSQwIgYDVQQKDBtGaW5hbnNpZWxsIElELVRla25payBCSUQgQUIxHzAdBgNVBAsM
FkJhbmtJRCBNZW1iZXIgQmFua3MgQ0ExLDAqBgNVBAMMI0JhbmtJRCBSb290IENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTAyMTAxNjExNDg1OVoXDTE5MTAxNjA4
Mzk1OVowdTEkMCIGA1UECgwbRmluYW5zaWVsbCBJRC1UZWtuaWsgQklEIEFCMR8w
HQYDVQQLDBZCYW5rSUQgTWVtYmVyIEJhbmtzIENBMSwwKgYDVQQDDCNCYW5rSUQg
Um9vdCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBALecO8FL34c7WioHQPQhv+HWCRGoQYuMzen7qrE/4tqdca3E
+gEqMwqdGJlvp2Ud4g8f7uofnOMQ3yHrZLv9DZJxXcWM8Vj42jZSrqoECkcws2NP
JBVKtXMq4f0yfdBLH53GLgqB61lEsan0Ohu4p4bvmrGCjpJSX06zmpRZhRFki/aQ
OA/85VpCPN6ip4HvYuUcb8FJeSDpzRdpQA2OpEM62ANr7tFCmvoavRrv2gFCS3Ho
AZX8PW75LRtrhozn2dGocRgZxS5k1eQYVdWGnllnFWPFPmAqa9jqV0qQXol5DuDk
eOQ6CNgz0QocdhUha+M44IyqVxVJrzr3Iw0VfSsCAwEAAaN4MHYwDwYDVR0TAQH/
BAUwAwEB/zATBgNVHSAEDDAKMAgGBiqFcE4BATAOBgNVHQ8BAf8EBAMCAQYwHwYD
VR0jBBgwFoAUJGG/aBGrBzjpfU8UhDM3uzbl1IcwHQYDVR0OBBYEFCRhv2gRqwc4
6X1PFIQzN7s25dSHMA0GCSqGSIb3DQEBBQUAA4IBAQAWV4HPWiLTITOhX16jH3Mz
QDkkgB+GNQXAZJXBJyploQMmY38gFaR2agLcXOilKXExTo7sW6awU9cfCMaw3slb
DMJfqFBQ374V39PgBPucm7lN082jhEdD+ptpOE9n9HcE/6f6J2TIDffw/b9rNp62
/FgUJiPHGIUgHeyDx0XYhus9XE6X9OLfPin6dq6cwLzEsxa01VHv1QiNPChhH476
qyhsKp2cpNYaLcekSFONlbxjS5er1iARtvI9j5W78vZw0XxiXuzxVhIjK7TDV7qK
E4Z1MPW1VUIKRnZO9tcaueHkbPCNnR5V8021vvqaFEUEpSlGqovjn+mKO06JrV2w
-----END CERTIFICATE-----
```

8.3 Nordea CA for Smartcard users 12

```
Subject:
C=SE, O=Nordea Bank AB (publ), CN=Nordea CA for Smartcard users 12/serialNumber=516406-0120
Validity
       Not Before: Sep 12 11:11:32 2008 GMT
       Not After : Sep 12 11:11:32 2023 GMT

 -----BEGIN CERTIFICATE-----
MIIDjTCCAnWgAwIBAgIEAKasmzANBgkqhkiG9w0BAQUFADBuMQswCQYDVQQGEwJT
RTEeMBwGA1UEChMVTm9yZGVhIEJhbmsgQUIgKHB1YmwpMSkwJwYDVQQDEyBOb3Jk
ZWEgQ0EgZm9yIFNtYXJ0Y2FyZCB1c2VycyAxMjEUMBIGA1UEBRMLNTE2NDA2LTAx
MjAwHhcNMDgwOTEyMTExMTMyWhcNMjMwOTEyMTExMTMyWjBuMQswCQYDVQQGEwJT
RTEeMBwGA1UEChMVTm9yZGVhIEJhbmsgQUIgKHB1YmwpMSkwJwYDVQQDEyBOb3Jk
ZWEgQ0EgZm9yIFNtYXJ0Y2FyZCB1c2VycyAxMjEUMBIGA1UEBRMLNTE2NDA2LTAx
MjAwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCwbOHr0MqlrKxn4iiH
umjoIj8SkOJtVfQ4Hra8LaEeroy4wXqdx1/+7UWZlhl8+aXS101zF+2pb8bVmchy
RXKLK38Y1Wi+Czjs9tmbXmiGx2VFiUj+5eroREwrkmEZhnpaWLv9YtiwjXPHUUkZ
6Pa+n0fB9qnoYeaUEZkmbVQJQj8h7wHvGocL6hyI/8v6Wyhr9AJ5RyDcK3+bGpTJ
TrzYTUu0JtybhiD2K5AkFwIsoLv0yjhyCXWvOve/Jy+pSGS1vY7+sYyJqOE4RL78
adrCWuj6fYs9ez2k8volnp08kHoE+lmDkogMDqXCPikz3/o1oFnnP0FSbNmvNrMs
aK11AgMBAAGjMzAxMA8GA1UdEwEB/wQFMAMBAf8wEQYDVR0OBAoECEm0MPTjNR03
MAsGA1UdDwQEAwIBBjANBgkqhkiG9w0BAQUFAAOCAQEAdgLty02SGU6hnaMQVyen
L1A+SG0aWgGIjB4z8bMji1l3V79cP0MKP0HkrRaH9HeOSoIYLI1PUm2PRg3eodd5
Tu37uE5eQ4rolbEAjPMjmrJr1Z9NUAFcbokfNRyMuJInLLqxBSx6V0rOSdrST4BN
cRWNQ9bPyCdCrAnfIEngl6Z8aYrhtDoa9cQVOe4/1pQGbuUBsS2TODfauCk03kDP
bgtWfhGWUZVoAz/m/izV//Jfc5eQHuqunuJrqZFkRTiZ75gvMyyyRFz25tB+T5vf
W9OUgyCpmD4f2DY/PKsGO2IddeBRhjJOWSMlo5Xqfw9wmUM6+N3OFRE6czruUVpI
tA==
-----END CERTIFICATE-----
```

8.4 Nordea CA for Smartcard users 13

```
Subject: C=SE, O=Nordea Bank AB (publ), CN=Nordea CA for Softcert users 13/serialNumber=516406-0120
Validity
            Not Before: Sep 12 12:30:10 2008 GMT
            Not After : Sep 12 12:30:10 2023 GMT
```

```
-----BEGIN CERTIFICATE-----
MIIDizCCAnOgAwIBAgIEAKatAjANBgkqhkiG9w0BAQUFADBtMQswCQYDVQQGEwJT
RTEeMBwGA1UEChMVTm9yZGVhIEJhbmsgQUIgKHB1YmwpMSgwJgYDVQQDEx9Ob3Jk
ZWEgQ0EgZm9yIFNvZnRjZXJ0IHVzZXJzIDEzMRQwEgYDVQQFEws1MTY0MDYtMDEy
MDAeFw0wODA5MTIxMjMwMTBaFw0yMzA5MTIxMjMwMTBaMG0xCzAJBgNVBAYTAlNF
MR4wHAYDVQQKExVOb3JkZWEgQmFuayBBQiAocHVibCkxKDAmBgNVBAMTH05vcmRl
YSBDQSBmb3IgU29mdGNlcnQgdXNlcnMgMTMxFDASBgNVBAUTCzUxNjQwNi0wMTIw
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAs63cz2+9B3mIyfI5ND0P
CfLAV2O/s5pr0Md3ysx+KdqTepivHZzJ+/D0vlcz7MbauPsNdB134bcJusL69fAL
DzlG5W/GXBAEFolStQ37mIBUIUNCKPLlaMhxLsITxYm02JlCTB9RTe14wZ3YAxEI
iI/PGqPLojnVqShFmYI7UrhOKxp42EXcXQ+Jp8Zx7NRxRaxJKvGDWetD8AGdOb2J
43VzEtev/529jmm4v2BsEeVp9+oQakSWWlR5HpbJltD8IqUMauahvkXcVCP3+ZL3
1SzWqlg/zwiSoADwQJ/Q/ukBcN2JipzQfie0YsxFzkjrmnE7Xo/xqOiqRBS/nOLD
iQIDAQABozMwMTAPBgNVHRMBAf8EBTADAQH/MBEGA1UdDgQKBAhGHylDookDmzAL
BgNVHQ8EBAMCAQYwDQYJKoZIhvcNAQEFBQADggEBAKyEcwMYuxyMw3Cq646fldN8
3GH//NJWll7qbTopfXF1jlFjCCPTPgYMFfn0phsQ5wjbphuMr2VXrHX+UZuZZFYA
FM0qbzZt3fxjMax2Jrw+w+yEUm+gMPpeRCEPNEC6xq/jFCURaWMegfF6axJRw1QP
Zkq49pXATrUfLA+bZUZA1JcZ74WzLxwP3jsRrlqjFMuqNkpxb1weOAv7Uqo3W6Ro
S87x5+DTh3R0FGOoH3EN8VfryrhL614tyhHWl2PV4zxu7r2Js3+/jHLx0CIPXYGM
VFnl7ywSZPuSPB89VfO2L9HrG9h8niDOhmMovPRxsI8DV4ihM2b1CyDevyEF5aU=
-----END CERTIFICATE-----
```

9 Appendix B: Packaging Swedish BankID Signatures for Long-Term Validation

This appendix explains the rationales behind the rules in the normative part of the policy.

9.1 Trusted Services

Trusted services are

1. The BankID Root CA, operating under a given certificate policy
2. The TSP, operating under this packaging policy
3. The CA of the TSP Certificate

9.2 Validation Data

The **Validation Data, will be**

For validation of the End-user signature:

ID	Information element	Were it is located in the package	Derives trust from
1	EU Certificate	In the XMLDSig ("Native SDO")	2,4
2	EU Intermediate CA Certificates	In the XMLDSig ("Native SDO")	3
3	BankID Root Certificate	Native Signature Qualifying Properties	Trust Anchor.[3]
4	EU Certificate revocation data	OCSP response, in Native Signature Qualifying Properties	6
5	EU Certificate chain revocation data	*Not included*	
6	OCSP Certificate	Included the OCSP response (4)	2

Note: Revocation data for the EU Certificate chain is not included. The rationale behind this is discussed in a separate section.

9.3 TSP Signature

The **TSP Signature**

ID	Information element	Were it is located in the package	Derives trust from
1	TSP Certificate	In the XAdES Signature	2, 4
2	TSP Certificate chain	In the XAdES Signature	3

[3] A Trust Anchor is trusted in itself

3	TSP Certificate Root CA	In the XAdES Signature	Trust Anchor[4]
4	TSP Certificate revocation data	OCSP response in the XAdES Signature	6
5	TSP Certificate chain revocation data	CRL in the XAdES Signature	7
6	OCSP Certificate 2	In the OCSP response in the XAdES Signature	2/3
7	Crl Certificate for TSP cert	In the CRL in the XAdES Signature	2/3

The **trusted signing time** will be

1. The TSP signing time included in the Native Signature Qualifying Properties. This can be validated through validation of the TSP Signature.
2. As additional evidence, the OCSP Response signing time is available. This can be validated as part of the OCSP response. But note that trust to the relation between the OCSP response and the signature depends on trust to the TSP Signature and the TSP.

9.4 EU Certificate chain revocation data

In general, the revocation status of intermediate issuer certificates also need to be checked as part of a certificate path validation. However, the availability of revocation information services (CRL/OCSP) for intermediate certificates vary between different PKIs. A PKI may choose to not offer revocation checking service for intermediate certificates, but this has the effect that a compromise of the intermediate CA will have a potentially damaging effects for the PKI as a whole.

BankID do not offer revocation checking on intermediate issuer certificates. This packaging policy therefore does not require inclusion of such revocation data.

If an intermediate CA should be compromised, a relying party will have to either remove trust to the BankID Root certificate, or implement special validation rules that takes the compromise into account. If the time of the compromise is known, the trusted time and the TSP seal over the signature will be useful in such a validation algorithm.

[4] A Trust Anchor is trusted in itself

10 Appendix C: BankID signature creation and verification process

The following is descriptions of the signature creation and verification process that is done in connection with (directly before) packaging.

The signature creation and verification process is outlined in the diagram *PDF signature process* on page 19

The process for text signatures will be similar, but simpler. The process for document-bundle signatures will be similar, but it will be several documents that needs to be read and confirmed.

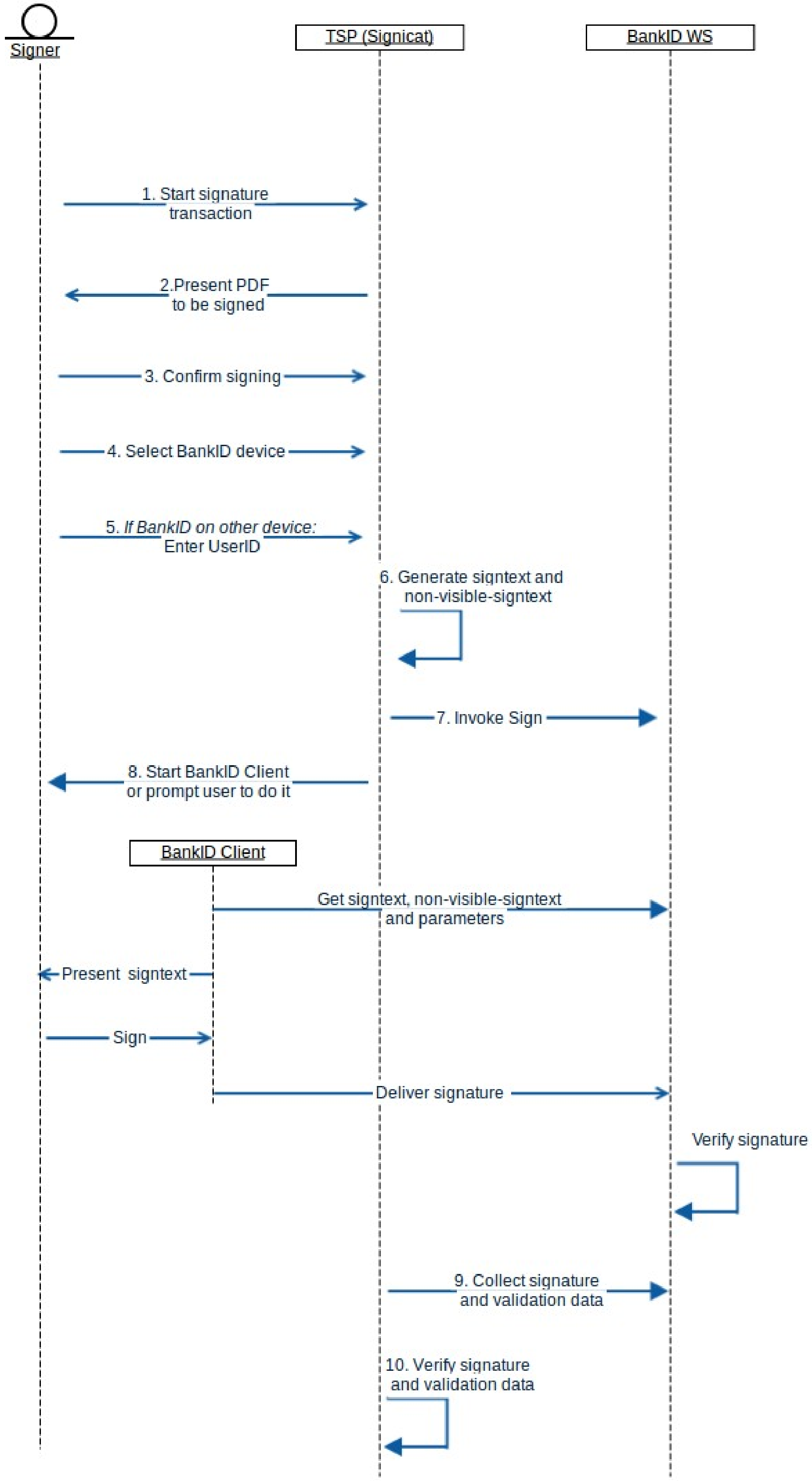
Signer
TSP (Signicat)
BankID WS
1. Start signature transaction
2.Present PDF to be signed
3. Confirm signing
4. Select BankID device
5. *If BankID on other device:* Enter UserID
6. Generate signtext and non-visible-signtext
7. Invoke Sign
8. Start BankID Client or prompt user to do it
BankID Client
Get signtext, non-visible-signtext and parameters
Present signtext
Sign
Deliver signature
Verify signature
9. Collect signature and validation data
10. Verify signature and validation data

Illustration 1: PDF signature process