BankID
Certificate Profiles for eIDAS

Version: 3.0

23 November 2018

TLP: WHITE

Document history

All changes in the document shall be identified here. A change shall be described with version number, date of change and a short text outlining the main issues that have been changed.

Version	Changes from previous version	Date	Editor
3.0	This document is a subset of the main document with the relevant parts for eIDAS certification.	23.11.2018	Andreas Havsberg

Table of Contents

1 Scope and Purpose

This document contains detailed information about the certificates used in BankID. This information is considered too detailed to be of interest for readers of policy documents, and is therefore distributed in this separate document. This document is not considered more sensitive than the rest of the policy documents.

The purpose of this document is to provide one single place for specification of certificate contents. This serves to avoid inconsistency and hopefully contributes to a significant reduction of the risk for errors and misunderstandings in the maintenance of certificate contents.

The contents of this document are approved BankID standards for certificate contents.

1.1 Document structure

Chapter 5 lists contents of BankID certificates intended to be externally visible.

Chapter 6 contains ASN.1 coding requirements for attributes and fields where BankID applies additional syntactical or semantical specifications in addition to what is found in the references.

Chapter 7 lists the BankID CRL profile.

This document contains integral annex A with COI profiling.

2 DEFINITIONS

<CA official>	The officially registered name of the CA organisation.
<CA org #>	The unique, business enterprise organisation number of the CA organisation.
<CA common>	The commonly used name of the issuing CA.
<CA type>	Indicator for type of Level 1 CA. Shall have the value ”Bank” or ”Utility”.
<Inst #>	An alphanumeric value with root or CA instance number within the issuing organisation.
<UniqueID>	An alphanumeric value, which shall ensure that the DN is unique, for human subjects this is defined as PID.

3 References

Short name	Document
[1]	BankID Object Identifiers, current version – maintained by Bits.
[2]	BankID: PID, Personlig Identifikasjonsnummer i sertifikater, versjon 2.3, 21. November 2007
[3]	RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (later replaced by RFC 5280)

4 Overview

Name of certificate	Category	In the cert. path
Root CA certificate	External	Yes
Level 1 CA bank certificates	External	Yes
Level 1 CA utility certificates	External	
VA certificates	External	
Subscriber certificates	External	Yes
BankID COI-required certificates	Internal	
Bank RA Server Certificate	External	
Bank RA Client Certificate	External	

Only certificates categorized as external and in the certification path of end user certificates are described in this document.

5 Certificates

The tables below list contents of certificates externally visible.

Standard certificate extensions not listed for a specific certificate type are not used.

5.1 BankID Root Certificates

5.1.1 Certificate-signing and CARL signing Certificate

These certificates are self-signed.

Certificate used from 2009

Certificates issued under the hierarchy of this root certificate, are issued from 28.09.2009.

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	FNH og Sparebankforeningen
	Organisation Unit (OU)	BankID
	Common Name (CN)	BankID Root CA
Attributes	Version	3
	Key type	RSA
	Key size	4096 bit
	Validity period	26 years
Extentions	Basic Constraints (critical)	Pathlength=1, CA=True
	Key Usage (critical)	KeyCertSign + CRLSign
	PolicyOID	2.16.578.1.16.1.4.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
Other	Signature algorithm	SHA-256 with RSA encryption

Keystore: HSM

5.2 BankID CA Certificates

5.2.1 Certificate-signing and CRL-signing Certificate

These certificates are signed by the root certificate named “Certificate-signing and CARL-signing certificate”.

Certificate used from 2019

These certificates are issued to BankID certification authorities since 2019 and are used to issue subscriber certificates from 2019.

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<CA official>
	Organisation Unit (OU)	<CA org #>
	Common Name (CN)	BankID - <CA common> - <CA type> <CA Inst #>
Attributes	Version	3
	Key type	RSA
	Key size	4096 bit
	Validity period	12 years
Extentions	Basic Constraints (critical)	Pathlength=0, CA=True
	Key Usage (critical)	KeyCertSign + CRLSign
	Authority Information Access	Access method = CAIssuer URI = https://crt.bankid.no/bankidrootca.crt
	PolicyOID	2.16.578.1.16.1.3.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName = https://crl.bankid.no/bankidrootca.crl
Other	Signature algorithm	SHA-256 with RSA encryption

Keystore: HSM

5.3 Subscriber Certificates

The BankRegNumber extension is a BankID private extension and is used to identify the issuing bank. The BankRegNumber extension has the following OID: 2.16.578.1.16.2.1

The BankName extension is used to identify a member bank when the CA organisation is a group of banks. The BankName extension has the following OID: 2.16.578.1.16.2.2

5.3.1 End-user Certificates for human end-users

Qualified End-user Signing Certificate – human end-users

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	BankID - <CA common>
	Serial Number (SN)	<Unique ID>
	Common Name (CN)	<Commonly used name of subscriber>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	Maximum 2 years
Extensions	Key Usage (critical)	NonRepudiation
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	Authority Information Access	Access method = CAIssuer URI is TSP specific, see chapter 6.8.
	PolicyOID	Bank-stored: 2.16.578.1.16.1.12.1.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	SubjectDirectoryAttributes	contains one element: DateOfBirth = <Subscribers date of birth>
	QcStatements	QcCompliance QcEuLimitValue: currency = NOK amount = 100000 exponent = 0 QcType = id-etsi-qct-esign QcEuPDS is TSP-specific, see chapter 6.6 for details.
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName is TSP-specific - see chapter 6.7 for specific contents.
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Bank-stored

Qualified End-user Authentication Certificate - human end-users

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	BankID - <CA common>
	Serial Number (SN)	<Unique ID>
	Common Name (CN)	<Commonly used name of subscriber>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	Maximum 2 years
Extensions	Key Usage (critical)	NonRepudiation + DigitalSignature + KeyAgreement
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	Authority Information Access	Access method = CAIssuer URI is TSP specific, see chapter 6.8.
	PolicyOID	Bank-stored: 2.16.578.1.16.1.12.1.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	SubjectDirectoryAttributes	Contains one element: DateOfBirth = <Subscribers date of birth>
	QcStatements	QcCompliance QcEuLimitValue: currency = NOK amount = 100000 exponent = 0 QcType = id-etsi-qct-esign QcEuPDS is TSP-specific, see chapter 6.6 for details.
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName is TSP-specific - see chapter 6.7 for specific contents.
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Bank-stored

Qualified End-user Signing and Authentication Certificate – human end-users (mobile key store)

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	BankID - <CA common>
	Serial Number (SN)	<Unique ID>
	Common Name (CN)	<Commonly used name of subscriber>
Attributes	Key type	RSA
	Key size	2048 bits
	Validity period	2 years
Extensions	Key Usage (critical)	NonRepudiation and DigitalSignature
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	Authority Information Access	Access method = CAIssuer URI is TSP specific, see chapter 6.8.
	PolicyOID	Qualified on SIM: 2.16.578.1.16.1.12.2.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	SubjectDirectoryAttributes	contains two elements: DateOfBirth = <Subscriber's date of birth> telephoneNumber=<Subscriber's mobile phone number>
	QcStatements	QcCompliance QcEuLimitValue: currency = NOK amount = 100000 exponent = 0 QcType = id-etsi-qct-esign QcEuPDS is TSP-specific, see chapter 6.6 for details.
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName is TSP-specific - see chapter 6.7 for specific contents.
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	

Keystore: SIM

Note: telephoneNumber is mandatory and shall be on the format: "+4712345678"

5.3.2 End-user Certificates for human end-users, as employees

Qualified end-user Signing Certificate – human end users, as employees

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<employer name><,><employer enterprise org number>
	Organisation Unit (OU)	<employee identification within the employer enterprise> - optional attribute – can be an employee number, or an alphanumerical description
	Serial Number (SN)	<Unique ID of subject, unique on national level, e.g. PID>
	Common Name (CN)	<Commonly used name of subject>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	Maximum 2 years
Extensions	Key Usage (critical)	NonRepudiation
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	Authority Information Access	Access method = CAIssuer URI is TSP specific, see chapter 6.8.
	PolicyOID	Bank-stored: 2.16.578.1.16.1.13.1.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	SubjectDirectoryAttributes	contains one element: DateOfBirth = <Subscribers date of birth>
	QcStatements	QcCompliance QcEuLimitValue: currency = NOK amount = 100000 exponent = 0 QcType = id-etsi-qct-esign QcEuPDS is TSP-specific, see chapter 6.6 for details.
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName is TSP-specific - see chapter 6.7 for specific contents.
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Bank-stored

Qualified End-user Authentication Certificate – human end users, as employees

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<employer name><,><employer enterprise org number>
	Organisation Unit (OU)	<employee identification within the employer enterprise> - optional attribute – can be an employee number, or an alphanumerical description
	Serial Number (SN)	<Unique ID of subject, unique on national level, e.g. PID>
	Common Name (CN)	<Commonly used name of subject>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	Maximum 2 years
Extensions	Key Usage (critical)	NonRepudiation + DigitalSignature + KeyAgreement
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	Authority Information Access	Access method = CAIssuer URI is TSP specific, see chapter 6.8.
	PolicyOID	Bank-stored: 2.16.578.1.16.1.13.1.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	SubjectDirectoryAttributes	contains one element: DateOfBirth = <Subscribers date of birth>
	QcStatements	QcCompliance QcEuLimitValue: currency = NOK amount = 100000 exponent = 0 QcType = id-etsi-qct-esign QcEuPDS is TSP-specific, see chapter 6.6 for details.
	CRLDistributionPoints	Only distributionPoint is used, DistributionPointName is TSP-specific - see chapter 6.7 for specific contents.
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Bank-stored

5.3.3 Merchant Certificates

Merchant Signing Certificate

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<Officially registered name of merchant organisation>
	Serial Number (SN)	<Officially registered organisation number of merchant organisation>
	Organisation Unit (OU)	Used to distinguish between different units or functions within the merchant organisation - optional attribute
	Common Name (CN)	<Commonly used name of merchant>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	4 years
Extensions	Key Usage (critical)	NonRepudiation
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	PolicyOID	Soft: 2.16.578.1.16.1.6.1.1 HSM: 2.16.578.1.16.1.6.2.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	BankRegNumber (private ext.)	<4 digit bank number>
	BankName (private ext.)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Soft / HSM

Merchant Authentication Certificate

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<Officially registered name of merchant organisation>
	Serial Number (SN)	<Officially registered organisation number of merchant organisation>
	Organisation Unit (OU) (optional)	Used to distinguish between different units or functions within the merchant organisation - optional attribute
	Common Name (CN)	<Commonly used name of merchant>
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	4 years
Extensions	Key Usage (critical)	DigitalSignature + KeyAgreement
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	PolicyOID	Soft: 2.16.578.1.16.1.6.1.1 HSM: 2.16.578.1.16.1.6.2.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included
	BankRegNumber (private ext)	<4 digit bank number>
	BankName (private ext)	<Officially registered name of member bank>
	optional attributes:	
	SubjectAltName	e-mail address of the subject

Keystore: Soft / HSM

5.4 Bank RA certificates

5.4.1 Bank RA signing certificate

Section	Key	Value
Distinguished name	Country (C)	NO
	Organisation (O)	<Officially registered name of member bank>
	Serial Number (SN)	<4 digit bank number>
	Common Name (CN)	<Commonly used name of certificate> Used to identify multiple certificates within one bank.
Attributes	Key type	RSA
	Key size	2048 bit
	Validity period	4 years
Extensions	Key Usage (critical)	NonRepudiation
	Authority Information Access	Access method = OCSP URI = <URI to VA service>
	PolicyOID	HSM: 2.16.578.1.16.1.14.1
	SubjectKeyIdentifier	160-bit SHA-1 hash of public key.
	AuthorityKeyIdentifier	160-bit SHA-1 hash of public key. No name or serial number included

5.5 BankID VA certificates

Section	Key	Value	Edit	Mand	Crit
Distinguished Name (DN)	Common Name (CN)	BankID [Commonly used name of VA service provider] VA <Inst #>	True	True	
	Organisation Unit (OU)	<Officially registered organisation number of VA service provider>	True	True	
	Organization (O)	<Officially registered name of VA service provider>	True	True	
	Country (C)	NO	False	True	
Attributes	Version	3	False	True	
	Key type	RSA	False	True	
	Key size	2048	False	True	
	Not Valid Before	Between time of issuance and CA expiry Default = Time of issuance	True	False	
	Not Valid After	Maximum 4 years, not exceeding CA expiry date and time.	True	True	
Extensions	Authority Key Identifier	160-bit SHA-1 hash of public key No name or serial number included	False	True	
	Subject Key Identifier	160-bit SHA-1 hash of public key	False	True	
	Key Usage (critical)	Digital Signature Non-repudiation	False	True	True
	Certificate Policies	Policy Identifier: 2.16.578.1.16.1.5.1	False	True	
	Extended Key Usage	OCSP Signing (1.3.6.1.5.5.7.3.9)	False	True	
	OCSP Nocheck	Nocheck (1.3.6.1.5.5.7.0.81.5)	False	True	
Other	Signature algorithm	sha256WithRSAEncryption	False	True	
	Directory string encoding	UTF8	False	True	

6 ASN.1 usage

This section contains requirements for ASN.1 coding for attributes and fields where BankID applies additional syntactical or semantical specifications in addition to what is found in the references.

6.1 BasisConstraints

BasicConstraints is mandatory and shall be critical for CA certificates.

ASN.1 syntax:

```
-- Root CA certificate
BasicConstraints ::= SEQUENCE {
      cA                BOOLEAN TRUE,
      pathLenConstraint INTEGER 1
}
-- Level 1 CA certificates
BasicConstraints ::= SEQUENCE {
      cA                BOOLEAN TRUE,
      pathLenConstraint INTEGER 0
}
```

BasicConstraints shall not be used in certificates for end entities

6.2 CertificatePolicies

CertificatePolicies is mandatory in all certificates and shall be non-critical.

CPSPointer and UserNotice should not be used, which leads to the following ASN.1 syntax:

```
PolicyInformation ::= SEQUENCE {
      PolicyIdentifier  CertPolicyID
}
```

6.3 SubjectDirectoryAttributes

SubjectDirectoryAttributes is optional and shall be non-critical.

When used it shall contain one element only the dateOfBirth attribute.

The dateOfBirth attribute SHALL, when present, contain the value of the date of birth of the subject.

```
SubjectDirectoryAttributes ::= SEQUENCE SIZE (1..) OF Attribute

Attribute       ::=     SEQUENCE {
        type            AttributeType,
        values  SET OF AttributeValue
                -- at least one value is required -- }

AttributeType           ::=   OBJECT IDENTIFIER
```

```
AttributeValue          ::=   ANY

dateOfBirth          AttributeType ::= { id-pda 1 }
DateOfBirth       ::= GeneralizedTime
```

6.4 AuthorityKeyIdentifier

AuthorityKeyIdentifier is mandatory in all BankID external certificates and shall be non-critical.

```
AuthorityKeyIdentifier ::= SEQUENCE {
      keyIdentifier             [0] KeyIdentifier           OPTIONAL,
            authorityCertIssuer       [1] GeneralNames            OPTIONAL,
     authorityCertSerialNumber [2] CertificateSerialNumber OPTIONAL  }

KeyIdentifier ::= OCTET STRING
```

The keyIdentifier is composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits), as decribed in method 1 of section 4.2.1.2 in RFC3280 [3].

6.5 AuthorityInformationAccess

AuthorityInformationAccess is mandatory for end entities' certificates and shall be non-critical.

AuthorityInfoAccess is optional for CA certificates.

```
AuthorityInfoAccessSyntax  ::=
           SEQUENCE SIZE (1..MAX) OF AccessDescription

   AccessDescription  ::=  SEQUENCE {
           accessMethod          OBJECT IDENTIFIER,
           accessLocation        GeneralName

}
```

where accessLocation shall be encoded as uniformResourceIdentifier.

6.6 QcStatements

QcStatements is mandatory for end entities' certificates issued as qualified certificates and shall be non-critical.

QcStatements shall comply with ETSI EN 319 412-5

```
      QCStatements ::= SEQUENCE OF QCStatement
      QCStatement ::= SEQUENCE {
          statementId   QC-STATEMENT.&Id({SupportedStatements}),
          statementInfo QC-STATEMENT.&Type
          ({SupportedStatements}{@statementId}) OPTIONAL }

      SupportedStatements QC-STATEMENT ::= {esi4-qcStatement-1, esi4-qc-
Statement-2, esi4-qc-Statement-5, esi4-qc-Statement-6}
```

6.6.1 QcCompliance

Ref ETSI standard chapter 4.2.1.

Syntax:

```
esi4-qcStatement-1 QC-STATEMENT ::= { IDENTIFIED BY id-etsi-qcs-
QcCompliance }
id-etsi-qcs-QcCompliance OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

Contents:

This statement shall be “present” for all qualified BankID certificates, indicating “The certificate is issued according to Annex I, III or IV of Regulation (EU) No 910/2014 [i.8] as of the types declared by the QC type statement in accordance with clause 4.2.3.”

6.6.2 QcType

Ref ETSI 4.2.3

Syntax:

```
esi4-qcStatement-6 QC-STATEMENT ::= { SYNTAX QcType IDENTIFIED
BY id-etsi-qcs-QcType }
Id-etsi-qcs-QcType OBJECT IDENTIFIER ::= { id-etsi-qcs 6 }
QcType::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-qct-
eseal |
id-etsi-qct-web, ...)
```

Contents for qualified BankID certificates for Personal/Employee BankID and Mobile BankID shall contain the value “id-etsi-qct-esign” for Personal BankID.

Contents for qualified BankID certificates for Merchants shall contain the value “id-etsi-qct-eseal”.

6.6.3 QcEuLimitValue

Ref ETSI 4.3.2.

Syntax:

```
esi4-qcStatement-2 QC-STATEMENT ::= { SYNTAX QcEuLimitValue IDENTIFIED
BY id-etsi-qcs-QcLimitValue }
QcEuLimitValue ::= MonetaryValue
MonetaryValue::= SEQUENCE {
currency Iso4217CurrencyCode,
amount INTEGER,
exponent INTEGER}
-- value = amount * 10^exponent
Iso4217CurrencyCode ::= CHOICE {
alphabetic PrintableString (SIZE 3), -- Recommended
numeric INTEGER (1..999) }
-- Alphabetic or numeric currency code as defined in ISO 4217
-- It is recommended that the Alphabetic form is used
id-etsi-qcs-QcLimitValue OBJECT IDENTIFIER ::= { id-etsi-qcs 2 }
```

Contents for qualified BankID Certificates shall have the MonetaryValue set to the following:
currency = NOK
amount = 100000
exponent = 0

6.6.4 QcEuPDS

Ref ETSI 4.3.4

Syntax:

```
esi4-qcStatement-5 QC-STATEMENT ::= { SYNTAX QcEuPDS IDENTIFIED
BY id-etsi-qcs-QcPDS }

QcEuPDS ::= PdsLocations

PdsLocations ::= SEQUENCE SIZE (1..MAX) OF PdsLocation

PdsLocation::= SEQUENCE {
    url        IA5String,
    language   PrintableString (SIZE(2))} --ISO 639-1 language code

id-etsi-qcs-QcPDS OBJECT IDENTIFIER ::= { id-etsi-qcs 5 }
```

Contents for qualified BankID certificates shall have PdsLocation set to different values for each Issuer and profile as follows:

For CA1:
Merchant: url = https://www.bankid.no/en/sparebank1_pds_merchant
Mobile: url = https://www.bankid.no/en/sparebank1_pds_mobile
Personal: url = https://www.bankid.no/en/sparebank1_pds_personal
All: language = EN

For CA2:
Merchant: url = https://www.bankid.no/en/dnb_pds_merchant
Mobile: url = https://www.bankid.no/en/dnb_pds_mobile
Personal: url = https://www.bankid.no/en/dnb_pds_personal
All: language = EN

For CA3:
Merchant: url = https://www.bankid.no/en/danskebank_pds_merchant
(Mobile profile is not supported by this issuer currently)
Personal: url = https://www.bankid.no/en/danskebank_pds_personal
All: language = EN

For CA4:
Merchant: url = https://www.bankid.no/en/nordea_pds_merchant
Mobile: url = https://www.bankid.no/en/nordea_pds_mobile
Personal: url = https://www.bankid.no/en/nordea_pds_personal
All: language = EN

For CA6:
Merchant: url = https://www.bankid.no/en/eika_pds_merchant
Mobile: url = https://www.bankid.no/en/eika_pds_mobile
Personal: url = https://www.bankid.no/en/eika_pds_personal
All: language = EN

For CA7:
Merchant: url = https://www.bankid.no/en/bid_pds_merchant
Mobile: url = https://www.bankid.no/en/bid_pds_mobile

Personal: url = https://www.bankid.no/en/bid_pds_personal
All: language = EN

6.7 CRLDistributionPoints

Each Issuer has its own distribution point for CRLs.

For the third (2019) generation of CA certificates, these are defined to be:

CA1: DistributionPointName = https://crl.bankid.no/bankid-sparebank1-bankca3.crl

CA2: DistributionPointName = https://crl.bankid.no/bankid-dnb-bankca3.crl

CA3: DistributionPointName = https://crl.bankid.no/bankid-danskebank-bankca3.crl

CA4: DistributionPointName = https://crl.bankid.no/bankid-nordea-bankca3.crl

CA6: DistributionPointName = https://crl.bankid.no/bankid-eikagruppenas-bankca3.crl

CA7: DistributionPointName = https://crl.bankid.no/bankid-bankenesid-tjenesteas-bankca3.crl

6.8 CA certificate URLs

Each Issuer has its own CA published.

CA1: URL = https://crt.bankid.no/bankid-sparebank1-bankca3.crt

CA2: URL = https://crt.bankid.no/bankid-dnb-bankca3.crt

CA3: URL = https://crt.bankid.no/bankid-danskebank-bankca3.crt

CA4: URL = https://crt.bankid.no/bankid-nordea-bankca3.crt

CA6: URL = https://crt.bankid.no/bankid-eikagruppenas-bankca3.crt

CA7: URL = https://crt.bankid.no/bankid- bankenesid-tjenesteas-bankca3.crt

6.9 Private extensions

Two private extensions are defined:

BankRegNumber is a private extension that is non-critical and is mandatory in all end-user certificates.

OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) bankenes-standardiseringskontor(16) at(2) bankregnumber(1) }

BankName is a private extension that is non-critical and and is mandatory in all end-user certificates.

OBJECT IDENTIFIER ::= {joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) bankenes-standardiseringskontor(16) at(2) bankname(2) }

Both private extensions shall be encoded as OCTET STRING.

BankRegNumber is a 4 digit number which must be in accordance with ”Bankplassregister for Norge”.

7 CRL Profile

Validation services need to ensure that most recent CRL is available.

CAs and RAs shall be able to suspend a certificate, and subsequently either revoke or reinstate it.

7.1 Version number(s)

The version of CRLs shall be version 2.

7.2 CRL and CRL entry extensions

Name	Format	Description		Necessity
Version	INTEGER	Version shall be v2, i.e. value 1		M
Signature	AlgorithmIdentifier	Defines the algorithm used to sign the CRL		M
Issuer	Name	The field shall contain the subject DN of the CA that issued the CRL		M
ThisUpdate	UTCTime	Specifies when the CRL was generated		M
NextUpdate	UTCTime	Specifies when the CRL expires. The next CRL shall be issued before the current CRL expires		M
RevokedCertificates				O
.certSerialNumb	INTEGER	The serial number of the revoked certificate		M
.revocationDate	UTCTime	The date of revocation		M
.crlEntryExtensions	Extensions	ReasonCode may be used InvalidityData is not used		O
CrlExtensions	Extensions	AuthorityKeyIdentifier (with KeyID only) CRLNumber IssuingDistributionPoint	M M O	M

Note that revokedCertificates may be empty.

Expired certificates should be removed from the CRL.

For definition of EntryExtensions and CRLextensions see RFC2459 [10].

None of the Extensions are marked as critical.

ANNEX A. COI Specific Details

The implementation at BankID Common Operational Infrastructure (COI) is compatible with the standards described in this document.

A.1 Validity period – a general note

This document states a certificate's validity period as *n* years.

The BankID COI implementation is using a product which encodes the validity period as *365n* days, without considering leap years. A consequence of this is that the actual certificate validity may be a few days shorter than *n* years.