BankID TSPS
Mobile Personal

Version 1.3. Last updated 23 Jun 2020

Contents

1 Introduction

Document history

Version	Date	Changes	Approved by
1.3	23.06.2020	Various smaller clarifying text changes	BankID Policy Board
1.2.1	26.11.2019	Corrected thumbprint for Nordea CA	Bits
1.2	13.11.2019	Various smaller clarifying text changes.	BankID Policy Board
1.1	21.05.2019	Various smaller clarifying text changes.	BankID Policy Board
1.0	29.11.2018	Final version for publishing document.	BankID Policy Board

1.1 Overview

For users not very familiar with PKI and the technical language used in this document, please see the more suitable version in the PKI disclosure statement (PDS), a simplified document to assist the end-user/subscriber (PKI users) in making informed trust decisions before applying for a BankID according to this document. The PDS is based upon the structure according to annex A in ETSI EN 319 411-1 [25] and merged with an earlier version of the general terms and conditions.

This document is the joint core part of the Trust Service Provider Practice Statement (TSPS) for Level 1 issuers of BankID. A Level 1 issuer of BankID may either be one single bank or a legal entity owned by and representing a group of banks. In the first case the Registration Authority will be the same legal entity as the issuer, in the latter case the RA will be any of the banks represented by the issuer.

This document describes the TSPS for BankID Certificates for natural persons (Personal Certificates). BankIDs can be issued by Banks affiliated to the Finance Norway Service Office, or Norwegian or foreign banks and credit institutions which have the consent of the Finance Norway Service Office and have agreed to comply with BankID Rules.

This document is unclassified and can be freely distributed. The descriptions of security and technical solutions are therefore at a relatively general level.

The document is organised in accordance with common practice and international standards for certificate Policy and Certification Framework IETF RFC 3647 [27].

This document is written for Mobile BankID, where private keys are secured on a SIM card on the customer's mobile phone, linked to a mobile phone subscription with a mobile network operator.

BankID can also support other solutions and other types of key bearers (smart cards, local storage in files on user's computer, netcentric, etc.). These solutions are described in other TSPS documents.

A Bank that issues a BankID shall enter into an agreement with the subject. The agreement shall be in the language the bank usually uses in communication with the customer and explain the rights and duties of the subject.

A BankID consists of one or two key pairs; each pair consisting of a private and a public key. BankIDs issued in accordance with this version of the TSPS consists of one key pair and one certificate.

When the CA-System creates a certificate, the TSP the link between the public key and the subject's identity. The certificate simultaneously ensures that the public key is protected against change (Integrity protection). Each individual key shall only be used in accordance with the function specified in the certificate.

Several parts of this document depend on, and refer to, whole documents or specific parts of documents [3] which describe internal procedures at the BankID COI Operator. This is unavoidable in a TSPS document, and the clear references are necessary for the purposes of audits and other quality assurance. For security reasons, these documents are not publicly available, but people with a valid business requirement will be granted access upon request. Parts of the documents referred to will have a higher confidentiality level than this document.

This TSPS is a standard document covering all Level 1 issuers of BankID who use the BankID COI Operator as service provider for common operational infrastructure. Where there is information specific to one or several TSPs, this is indicated under the heading “Issuer specific” throughout this document.

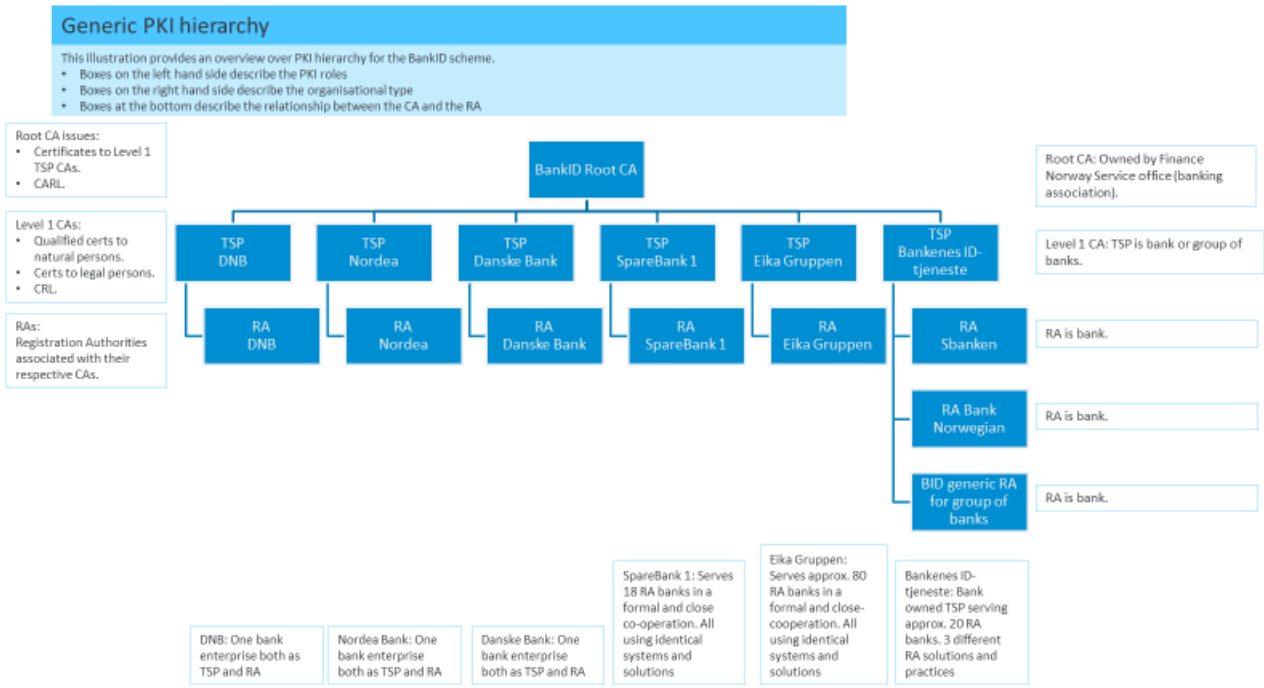
Issuers issue certificates in accordance with one or more certificate policies defined for BankID [10]. The corresponding Certificate Policy for Personal BankID is issued by Bits AS, see section 1.2. This document pertains to Bank-stored BankID where private keys are stored in a secure bank system on the BankID COI’s premises that protects the keys so that only the rightful owner can use them.

The banks take on the roles as responsible contracting partner and Registration Authority (RA). Banks are responsible for all customer follow-up of subjects, and for Employee BankID subject’s enterprise. Bank routines in this area must be documented in individual supplementary documentation over and above this document.

A bank may either be a BankID issuer with its own Level 1 CA system, or enter into an agreement with a joint issuer.

The BankID system is a two-step hierarchy where the CA of the individual issuer is placed under a common Root CA [16].

Root CA issues CA certificates for issuer’s CAs. The Root CA system is run by the BankID COI Operator as service provider on behalf of Root CA.



The structure (headings and subheadings) in this TSPS is organised in accordance with recommendations in [27].

The key words “MUST, MUST NOT, IS REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, CAN and OPTIONAL” in this document must be interpreted as described in [9]. The exact meaning of these words is modified in accordance with the requirements in the text where they occur.

When the words **MUST** and **MANDATORY** are used, this means that the definition is an absolute requirement in the specification.

MUST NOT or **SHALL NOT** means that the definition is absolutely forbidden in the specification.

SHOULD or **RECOMMENDED** means that there may be cases where there are strong reasons to ignore a particular subject, but in doing so, one must understand and take into account the full consequence of choosing another solution.

SHOULD NOT or **NOT RECOMMENDED** means that there may be cases where there are strong reasons to, or it would be useful to, perform a certain task, but in doing so, one must understand and take into account the full consequence of performing a task that is described with these words.

CAN or **OPTIONAL** means that the subject/element is optional. One supplier may choose to include an item because a particular marketplace wants it or because the supplier believes that it strengthens the product, while another supplier might omit the same item. An implementation that does not include a particular option must be prepared to interact with another implementation that includes this option, though potentially with reduced functionality. Likewise, an implementation that does include a particular option must be prepared to interact with another implementation that does not include this option (apart from functionality related to the relevant option).

1.2 Document name and identification

This Policy document describes the Certificate Policy for BankID certificates issued as Qualified Certificates for natural persons, where the end user's private keys are stored on the SIM card of a mobile phone (Mobile BankID).

All BankID certificates must contain a unique object identifier (OID) that indicates to which policy the certificate conforms. Based on this field, a relying party or certificate validation service shall automatically be able to determine whether a certificate is appropriate for a particular use. See section 7.1.6 for Object Identifier for this policy. The Object Identifier for this document version is 2.16.578.1.16.1.12.2.1.1.0, where the trailing two numbers designates the version number (major minor).

This certificate conforms to all related security requirements for QCP-n according to ETSI EN 319 411-2 [26], aimed to support the advanced electronic signatures based on a qualified certificate defined in articles 26 and 27 of the Regulation (EU) N° 910/2014 [23]. This policy does not require a QSCD - Qualified electronic Signature/Seal Creation Device.

1.3 PKI participants and responsibilities/obligations

1.3.1 Trust Service Provider

Issuers of BankIDs are organised into a hierarchy with a single Root CA and a subordinate level of issuers of BankID (Level 1). The Root CA issues certificates at Level 1 in accordance with BankID Rules [1].

The Root CA was established by the Financial Services Service Office and the Savings Bank Association Service Office. As of 1st January 2010, the Finance Norway Service Office assumed the role of Root CA previously held by the Service Offices. Procedures for operating the Root CA system must be approved by Bits AS (formerly the Norwegian Banks' Standardisation Office (BSK)).

The TSP issues BankIDs, but the agreement [20] with customer/subject regarding the issuance and use of BankID shall always be entered into with a bank performing RA activities.

A TSP might be either a single bank that have established its own Certification Authority System or a group of banks that have established a joint issuing entity performing the issuance of certificates.

The TSP issuing BankIDs in accordance with this document is committed to:

a) Operate in accordance with the terms outlined in this document
b) Create a document that outlines the bank acting as RA's own practices for subject identification, registration and certificate life cycle management.
c) Use system solutions approved by Bits AS. The approval shall also include the issuer's production environment and any use of service providers.
d) Define, document, implement and review Information security policy that is approved by management.

The TSP's information security policy practices

The Information security policy is part of the TSPs overall governance system, and the implementation and changes is approved by management. If there are changes to the information security policy of relevance to third parties, they will be notified, this includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies, TSP´s standard communication channel will be used to communicate changes. The information security policy is part of the TSPS quality system and is documented, implemented and controlled on regular basis either by internal audit or external audits.

TSP is overall responsible for the services set out in this TSPS and information security policies and will see to that the underlaying procedures are sufficient, even if these are carried out by third party. This means the TSP will ensure adequate and appropriate security controls and operating procedures for TSP facilities, systems and information assets providing the services, are maintained and publish and communicate along with the information security policy to all employees who are impacted by it. The TSP is overall responsible for the service provided and all services outsourced, appropriate security requirements are part of the contract agreement and continuous followed-up with contractor on in regular meetings.

Trust service practices under which the TSP operates are non-discriminatory.

Issuer specific

For Bankenes ID-tjeneste: Within this TSP, it is Bankenes ID-Tjeneste AS which is the internal management body responsible for implementing the practices within the organisation.

For Danske Bank: Danske Bank is not a Mobile BankID trust service provider, and do not fulfil this TSPS.

For DNB: Within this TSP, it is DNB Payments and Innovation which is the internal management body responsible for implementing the practices within the organisation.

For Eika: Within this TSP, it is the Payment Systems Department which is the internal management body responsible for implementing the practices within the organisation.

For Nordea: Within this TSP, it is the department "Fraud Management" which is the internal management body responsible for implementing the practices within the organisation.

For SpareBank 1: Within this TSP, the Issuer is a common issuer and responsible for facilitating an approved technical system. Each Registration Authority is responsible for implementing the practices within the organisation.

1.3.2 Registration authorities

The Registration Authority (RA) operates in accordance with the terms in this document.

The Bank performing the RA tasks is always responsible for the RA-function. This responsibility is defined in agreements between the bank performing RA tasks and the TSP.

The registration function for certificates issued under this policy is carried out by a unit subject to reporting obligation pursuant to section 4, first and second paragraphs, of the Money Laundering Act.

1.3.3 Subscribers/subjects

In this document the subject is a natural person.

A subscriber of Merchant BankID may be the recipient of a message secured with a Mobile BankID. In the interaction between a merchant and an individual, the subscriber of the Merchant BankID must adhere to a BankID policy for merchants. This document describes requirements applicable to subscribers only where this is important in understanding the rights, duties and trust levels of the owner of a BankID.

For Mobile Personal BankID, the Subject and Subscriber are always the same entity.

Mobile Personal BankID service is accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the terms and conditions, see section 2.

1.3.4 Relying parties

The relying party may be a BankID Merchant with a merchant certificate or the recipient of a message secured with a BankID belonging to the owner of a personal certificate. In interaction between a merchant and a natural person, the merchant subscriber must adhere to a BankID policy for merchants. This document describes requirements applicable to legal person subscribers only where this is important in understanding the rights, duties and trust levels of the owner of a BankID.

1.3.5 Other participants

The BankID COI Operator performs the physical, logical and administrative operations of the certification authority system. This can also include responsibility for specifying the characteristics of the interface between a bank that acts as RA, and the certification authority system

The mobile network operator

The mobile network operator is responsible for providing a key store, secured in accordance with the bank's requirements, on the SIM card. In cooperation with the bank, the mobile network operator shall also provide the necessary infrastructure for safe and secure issuance and use of Mobile BankID, referred to as the Security Channel.

A mobile network operator that enters into BankID agreements in accordance with this document shall:

- Operate their part of the Security Channel in accordance with the terms outlined in this document
- Create a document that outlines how certificates are issued, which refers to the relevant certificate policy
- Use system solutions approved by Bits AS. The approval shall include the mobile network operator's solutions and operating environment for critical components in the Security Channel, in addition to SIM cards and personalisation of these.

The mobile network operator’s role in the BankID agreement structure is as follows:

- The mobile network operator enters into framework agreements with Vipps to provide the Mobile BankID service to its subscribers
- The mobile network operator enters into agreements with the individual mobile subscriber to provide the Mobile BankID service
- The mobile network operator also enters into agreements with the individual BankID merchant regarding the use of the service for transactions with the operator’s subscribers.

1.4 Certificate usage

Substantial effort has been made to ensure the certificate usage is accessible to people with disabilities and comply with WCAG 2.0. No special configuration is needed to make the accessibility features available in the software for certificate use. Registration and issuing of certificates are non-discriminatory and support standards for universal accessibility.

1.4.1 Appropriate certificate uses

Certificates issued in accordance with this TSPS are used between natural persons using BankID and merchants to perform the following security services:

- Authentication
- Digital signing of short text messages (up to 120 characters)

Certificates issued under this TSPS can only be used on BankID merchant’s sites. The site may, for example, enable the use of web-based services or mobile-based services (e.g., SMS-based).

The merchant site that the subject communicates with must have entered into an agreement with his bank about the use of BankID. The merchant must also have entered into an agreement with the mobile network operator the subject subscribes to.

In addition to the BankID, the subject must use a mobile phone type, subscription type or the security equipment specified by the bank. The bank may add new requirements for mobile phone type, subscription or security equipment where this is necessary for security reasons or due to necessary BankID upgrades. The mobile phone and the subscription will be tested during the BankID issuance process. If BankID is enabled in a mobile phone environment that does not meet the BankID security requirements, this may leave it open to misuse. Banks will provide requirements and advice regarding appropriate user environments.

In addition to the uses mentioned above, subjects using Bank-stored BankID may use Mobile BankID as one of the two authentication factors to access their private key. The authentication will be done with Mobile BankID instead of another type of one time code device. In this case, the Bank-stored BankID infrastructure will act as a relying partner for Mobile BankID.

Certificates must be valid at the time of the use of the private key.

Customers will be notified if the bank expands or limits the scope of BankID, or limits the transactional amounts allowed. The scope is described in more detail in the PDS [20].

A BankID shall not be used as basis for issuance of physical or electronic identification. A Personal BankID which a participant has issued, or entered into an agreement about, can still be used by the same participant as an element required to issue identification instruments other than a BankID to customers.

1.4.2 Prohibited certificate uses

Everything which is not explicitly allowed, is prohibited.

1.5 Policy administration

Bits AS is responsible for defining and administrating BankID certificate policies, as set out in BankID Rules [1], section 4.1, which each BankID TSP has agreed to follow. Bits AS will manage the change process and review changes in a BankID Policy Board consisting of:

- Bits AS' administration
- Banks (in their capacity as contracting party to BankID and Registration Authority)
- Vipps AS
- The BankID COI Operator (in their capacity as service provider for Root CA)

Bits AS is responsible for the change approval process. Vipps AS is responsible for managing the control process for new versions.

Bits AS can make editorial or typographic changes without notifying any other party.

Key changes in applicability, certificate content, key storage, key sizes and retention of keys may result in a new policy being created. Major changes in other areas can also create a need for a new policy.

Changes to a TSPS can be made with 90 days' notice.

Changes that in Bits AS' view will not significantly affect a large number of subjects or relying parties can be made with 30 days' notice.

All changes will be notified in writing to registered issuers of BankID, and will be flagged up on BankID's web pages.

All changes, apart from editorial or typographical changes, will be embedded through consultation with the banks.

1.5.1 Organization administering the document

This document has been issued by Bits AS on behalf of participating issuers. Bits AS is also registered holder of BankID policies.

Bits AS
PO Box 2644 Solli
N-0203 Oslo
Norway
Telephone: +47 23 28 45 10
Web site: http://www.bits.no
E-mail: post@bits.no

1.5.2 Contact person

Contact information for each individual BankID TSP can be found in the relevant BankID PDS, see section 2.

Any questions regarding this document may also be addressed to:
Vipps AS
Dronning Eufemias gate 11
N-0150 OSLO
Norway
Telephone: +47 480 33 777
Web site: http://www.bankid.no

1.5.3 Person determining TSPS suitability for the policy

Bits AS is responsible for verifying that this TSPS is consistent.

Bits AS
PO Box 2644 Solli
N-0203 Oslo
Norway
Telephone: +47 23 28 45 10
Web site: http://www.bits.no
E-mail: post@bits.no

1.5.4 TSPS approval procedures

Each TSP issuing BankID is responsible for additions to the TSPS. The issuer specific parts of the TSPS shall comply with the policies and this document.

In practice, TSPS documents are compiled by the process of each issuer writing the addendum to the common parts of the TSPS. Any TSPS created within the scope of a BankID policy must be approved by Bits. The document must be approved when it is first produced and subsequently if any major amendments are made.

Before publishing new TSPS, Bits as the Policy Board secretary will update this TSPS, according to relevant changes, and document that the approval is recorded in the document history.

1.6 Definitions and acronyms

1.6.1 Definitions

In this document, the following terms are understood to mean:

Activation data: Data, other than cryptographic keys, required to access key stores, and which must be handled securely (e.g. a PIN or password/passphrase).

Authenticate: Confirm/verify an alleged identity. The process ensures authenticity.

Bank: Banks attached to the Finance Norway Service Office, or Norwegian or foreign banks and credit institutions which issue BankIDs with the consent of the Finance Norway Service Office.

BankID: One or more key pairs or electronic certificates that can be used by a bank customer (subject) to secure electronic message exchange with a bank or a bank customer.

Bank-stored BankID: A BankID that stores private keys in a secure bank system that protects the keys so that only the rightful owner can use them, at any time, from a device connected to the internet.

BankID COI: BankID's Common Operational Infrastructure@

BankID COI Operator: The entity operating BankID's Common Operational Infrastructure and central storage

Certificate (Public Key Certificate): A data sequence containing the subject's public key along with other information, which cannot be falsified as the information is signed with a certificate issuer's private key.

Certificate Applicant: Personal customer who has applied for BankID, but who has not yet taken on the role of subject.

Certificate Policy (CP): A document containing rules for how certificates are issued and processed and thereby defining the trustworthiness of the certificates.

Certificate validation service: A trusted service which verifies certificate status for a relying party.

Certification Authority System: The system that generates the BankID. The Certification Authority system signs the subject's public keys and other certificate information with its private key.

Invalidate: To block a certificate and make it invalid. A certificate can be temporarily invalidated (suspended) or permanently invalidated (revoked).

Issue BankID: Sign BankID with a Level 1 CA certificate issued by Root CA.

Issuer of BankID: A bank or joint issuer that can issue BankIDs.

Joint issuer: A legal person who issues BankIDs on behalf of a group of banks and uses a Level 1 certificate issued by the Root CA for this purpose (see section 1.3.1).

Key store: The logically and physically defined environment where the subject's private key is stored.

Object Identifier (OID): A sequence of integers which uniquely identifies an object. Objects in this context, means i.e. a defined information structure or a specification.

Participant: Legal entity with the right to issue BankID certificates based on the common BankID Rules [1]

Possession Element: An authentication factor that shows that a subject or end user possesses a personalised physical or logical unit.

Registration Authority (RA): An entity that commits to correctly confirming the identity of a future subject. This must be performed by each individual bank or by a trusted supplier on behalf of the bank.

Relying party: The person who receives a signed document or message with its associated certificate, and who is required to verify and establish trust in the material received.

Service provider: An organisation or entity that carries out practical tasks related to issuance of certificates, or performs other services related to electronic signatures on behalf of banks.

Storage Entity: Centralised entity which stores data and software used during control and documentation of BankID. In Bank-stored BankID the subject's keys will also be stored in a storage entity, so that only the rightful owner can access and use it.

Subject: A bank customer who has registered for the certification service and has been issued with a BankID. In this policy the subject is a natural person having a Norwegian identification number registered in the National Population Register. A person who is a subject, can also fulfil the role of relying party.

1.6.2 Acronyms

Bits	Bits AS is the financial infrastructure company of the bank and finance industry in Norway
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CARL	Certification Authority Revocation List
CRL	Certificate Revocation List
DN	Distinguished Name
ETSI	European Telecommunication Standard Institute
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hyper Text Transfer Protocol
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
ISO	International Standards Organisation
ITU	International Telecommunications Union
KEK	Key Encryption Key
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PDS	PKI Disclosure Statement
PIN	Personal Identification Number

PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comment
RSA	Rivest, Shamir, Adleman
TCP/IP	Transmission Control Protocol / Internet Protocol
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement

2 Publication and repository recommendations

Any changes in terms or responsibilities for the issue and use of BankID shall be announced on https://www.bankid.no/personvern-og-regler/ without undue delay and, if necessary, in a new version of this document. In the event of changes to the terms between bank and customer (subject or subscriber), or in the scope of the BankID, this shall be announced by the bank without undue delay. Changes will be communicated through the TSP´s standard communication channel to the subject.

The TSP operates a database of all issued certificates as part of the technical CA-system operated by the CA Service Provider. This is regulated in the operational agreement between the TSP and the CA Service Provider. The information shall be available 24 hours per day, 7 days per week. Up-time shall be minimum 99.7%.

Below is the links to relevant documents for BankID, alternatively, these documents can be requested by email from post@bits.no or using the contact details in section 1.5.1. For questions regarding BankID contact your bank (the issuer of your certificate), you may also find some helpful information here: https://www.bankid.no/en/private/solve-my-bankid-problem/. Relying parties may request BankID certificates using the contact details in the PDS. Certificate information is not real-time online because subjects have not approved online publishing of their certificate.

Subscriber or relying party not able to verify expired certificate status information, usually revocation status information beyond the validity period of the certificates, or other terminated BankID services, can submit their questions using the BankID form: https://www.bankid.no/en/about-us/contact/

Direct links to relevant documents:

- BankID Rules: https://www.bankid.no/en/bankid_rules
- BankID Root CA certificate: https://www.bankid.no/en/rootca
  - Thumbprint: d79f0c6f28b50d4d9c5778acdb2b335afff91e5d
- Bankenes ID-tjeneste CA: https://crt.bankid.no/bankid-bankenesid-tjenesteas-bankca3.crt
  - Thumbprint: fdb263735b747390d5cb4b123cf88b928a8d16f1
- Danske Bank CA: https://crt.bankid.no/bankid-danskebank-bankca3.crt
  - Thumbprint: e63960f78f8fd970e8ec6a125f2592ab9b2bf6f5
- DNB CA: https://crt.bankid.no/bankid-dnb-bankca3.crt
  - Thumbprint: 5ee8a6aa681f520ddc3f1c376f4aa38128fadbb4
- Eika CA: https://crt.bankid.no/bankid-eikagruppenas-bankca3.crt
  - Thumbprint: 4007acc77d1d588853d851b9b3df03ab0b194296
- Nordea CA: https://crt.bankid.no/bankid-nordea-bankca3.crt
  - Thumbprint: e7b30c03fb02ee09c13daf630f40c9fd1f9713bd
- SpareBank 1 CA: https://crt.bankid.no/bankid-sparebank1-bankca3.crt

- Thumbprint: 8c322140d9979c0c717e940548b4b20b36ed356f
- BankID Certificate Profiles [13]: https://www.bankid.no/en/bankid_certificate_profiles
- PDS Mobile:
  - For Bankenes ID-tjeneste: https://www.bankid.no/en/bid_pds_mobile
  - For DNB: https://www.bankid.no/en/dnb_pds_mobile
  - For Eika: https://www.bankid.no/en/eika_pds_mobile
  - For Nordea: https://www.bankid.no/en/nordea_pds_mobile
  - For SpareBank 1: https://www.bankid.no/en/sparebank1_pds_mobile
- TSPS Mobile (this document): https://www.bankid.no/en/tsps_mobile

2.1 Repositories

The TSP makes information about revocations available to BankID Certificate Validation Services service providers, see section 4.9.

In order to maintain the trust hierarchy, CA certificates will continue to be made available until all underlying certificates have expired.

2.2 Publication of certification information

This TSPS with appendixes is registered with the Norwegian Communications Authority (Nkom) and published in their trust list: https://eng.nkom.no/technical/trust-services/qualified-providers/qualified-trust-service-providers

BankID terms and conditions regarding the use of the certificate are publicly and internationally available in the PDS document, see URLs provided in section 2.0 above.

2.3 Time or frequency of publication

Any new version of this TSPS is made public on the web site referred to in section 2 immediately after the version is approved as described in section 1.5.

2.4 Access controls on repositories

The Certificate database is protected according to security controls found in this sections 5 and 6 in this TSPS.

This TSPS document is not confidential and can be downloaded and read without restriction.

All policy documentation, including this TSPS with appendixes, CRLs, and other information about certificates stored in the storage entity is protected from unauthorised changes.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The certificate fields “subject” and ”issuer” shall contain information of the type “Distinguished Name” - (DN) as defined in the X.500 framework. A DN is a sequence of designations (attributes) about an entity (e.g. a natural person) which defines this entity uniquely. Note: A person can have more than one certificate with the same distinguished name.

SUBJECT NAME

This document deals with personal certificates tied to a person's identity.

Attribute	Importance	Content Requirement
Country (C)	Mandatory	Shall have the value “NO”.
Organisation (O)	Mandatory	Shall have the value “BankID” and the name of the issuer of the BankID.
Serial Number (SN)	Mandatory	Alphanumeric value that ensures that the name is unique (see section 3.1.2).
Common Name (CN)	Mandatory	The commonly used name used for the subject.

CERTIFICATE ISSUERS NAME

Attribute	Importance	Content Requirement
Country (C)	Mandatory	The country where the issuer of BankID is registered.
Organisation (O)	Mandatory	Must contain the officially registered name of the organisation that owns the Certification Authority System (bank or joint issuer)
Organisational Unit (OU)	Mandatory	Must contain a unique number from the Entity Register that identifies the organisation which owns the Certification Authority System (legal person).
Common Name (CN)	Mandatory	Must contain the text "BankID", commonly used name of CA, the text "bank" and an optional additional alphanumerical value to identify the individual CA if the issuer has more than one.

Further rules for the names in BankID Certificates available in BankID Certificate Profiles [13].

3.1.2 Need for names to be meaningful

A person who has applied to become a BankID subject is verified by the RA against the information in the National Population Register, either when the customer relationships is first established, at the start of the online banking agreement or when BankID is issued. When a Personal BankID is issued, the subject’s name is retrieved from the RA banks' customer records.

All individuals are assigned a unique National ID number or D number (temporary number for non-Norwegian citizens) from the national authorities.

The unique identifier in the subject’s serialNumber is a sequence of readable characters that uniquely identifies the subject (and the person’s employment relationship in the case of Employee BankID) within the certificates issued on this Certification Authority System. Bits AS defines the rules for the identifier format.

The format of the subject’s CommonName shall be:

<Family Name>,space<Given Names>

The Norwegian letters "æ, ø, å" can be used. Character representation otherwise must comply with Norwegian standard (ISO-8859-1).

3.1.3 Anonymity or pseudonymity of subscribers

Pseudonyms are not permitted in Mobile Personal BankID. Anonymous certificates will not be provided.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

The attributes that make up a subject’s DN uniquely identify the user.

The naming sequence includes a unique identifier that is assigned by the TSP issuing system and thus allows all individuals to be uniquely referenced.

If a person has multiple personal BankID certificates issued by the same Certification Authority System (CA), these will have the same DN.

The mobile number must be entered in the certificate so that the subject can be identified and reached via the Security Channel.

There may be at most one active (or suspended) certificate associated with a mobile number at any one time. If a person has more than one certificate for Mobile BankID, these must be associated with different mobile numbers.

3.1.6 Recognition, authentication, and role of trademarks

A trademark or logo should always be used with, or be attached to, the certificate, so users and others who come into contact with the certificate can connect the certificate to the trademark and vice versa. Likewise, the trademark should, as far as possible, be associated with the use of the certificate, including being visible on merchants' sites to show subjects that BankID may be used.

Vipps AS has the rights to the trademark and determines its design and use.

If a TSP or Vipps AS issues or enters into an agreement about an electronic certificate that is not a BankID, the issuer must ensure the certificate cannot be confused with a BankID.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

In this TSPS, the key pair generation is controlled by the certificate applicant.

When a certificate applicant has generated his key pair, the certificate applicant must prove that the private key is under his/her control. This is done by signing a request to the BankID CA. If the request can be verified correctly, the CA can issue a certificate based on the corresponding public key.

3.2.2 Authentication of organisation identity

It is possible to issue certificates to a person who has access to the account belonging to another legal entity (e.g. an enterprise), but this is handled at the authorisation level of the relying party. The certificate is issued to the person, and there is no reference in the certificate of the enterprise. Hence there is no need to authenticate organisational identity in the registration process.

3.2.3 Authentication of individual identity

In order to be issued with BankID, the person has to agree to and actively participate in the issuance process. This does not prevent the bank from initiating the issuance process as long as the personal customer is actively involved.

If the person is a new customer at the bank, he or she must physically present themselves to submit ID documentation that meets the bank's requirements and which unambiguously links the customer to a National identity number or "D number" (temporary number.). This may be done by a bank's subcontractor with the same obligations, such as "Postens PUM-tjeneste". The Bank has a duty, governed by laws and regulations on Anti-Money Laundering [19], to record the credentials of its customers. ID documents are scanned and verified by equipment that can detect falsifications. The following proof of evidence of the physical person shall be securely stored, according to section 5.5:

1. Full name (including surname and given names)
2. Date of birth, reference to a nationally recognized identity document, or other attributes which can be used to, as far as possible, distinguish the person from others with the same

name. The place of birth is not registered, as other details are sufficient to correctly identify the individual entity. BankID Rules requires that first time a BankID is issued to a natural person, the individual's identity will be verified on the basis of a valid Norwegian passport, documents equivalent to a Norwegian passport or a foreign passport. This requirement may be waived if the issuer is certain of the person's identity, and the requirement will entail an unreasonable additional burden on the person concerned, due to age, health or other special circumstances. If the requirement for passports is waived, the issuer must instead submit another form of ID according to the requirements for physical ID documentation in the Money Laundering Act and associated regulations.

3. Norwegian identification number

The bank and person shall agree on the point of contact information, such as phone number, email address and physical address and the bank stores the information. The certificate applicant must also confirm that he/she accepts the contractual terms and conditions in the BankID agreement.

Personal customers who already have a customer relationship with the bank, and who have previously been identified and unambiguously linked to a national identity number or "D number" (temporary number) through physical presence, can apply for BankID through a registration process based on secure procedures for online banking.

This assumes that the bank has already performed a full control of the person's identity and that the personal customers can submit information to the Registration Authority through a service (e.g. online banking) that uses an approved authentication method. The Registration Authority must verify the identity towards the Norwegian National Population Register ("Folkeregisteret") or towards information retrieved from the National Population Register within the previous month.

Bank customers who have not previously used online banking can either go through the bank's procedure for authorisation for online banking or register as a new customer.

BankID Rules state that issuers of BankID are not allowed to issue BankID certificates for new customers based on BankIDs issued by another bank.

The Bank processes registration data and other customer data in accordance with the Personal Data Act [14].

Subscribers employed in the TSP organization must follow the same authentication procedures as stated in this section and may not register themselves.

Subject information is retrieved from the Customer Ledger/Customer register which is compared and updated towards the National Population Register on a regular basis.

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

Not applicable for this TSPS

3.2.6 Criteria for interoperation

The certificate applicant must agree to and actively participate in the issuance process by accepting Terms and Conditions and using the Activation Data and Possession Element issued by the RA.. The customer shall be informed through the text in the agreement that content from the Personal Mobile BankID will be included in message exchanges with merchants. The customer's National ID number is not part of the contents of Personal Mobile BankID and will never be disclose by the issuing bank to merchants who do not already legally hold the customer's National ID number.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

For routine re-key the bank acting as RA shall offers a self-service solution that uses an approved authentication solution. Routine re-key is initiated by the customer, usually after prior notification from the bank.

The subject's identity is always verified against the National Population Register, as described in section 3.1.2.

3.3.2 Identification and authentication for re-key after revocation

After revocation the customer must submit a certificate request following the same process as at the initial registration. The procedures in sections 3.2 is followed.

3.4 Identification and authentication for revocation request

The subject must identify themselves in order to request revocation, in one of the following ways:

- By physical presence
- By signed request
- By phone

If the subject goes to a branch office, the subject must bring appropriate ID. If a subject wishes to revoke a certificate by unsigned electronic message, the subject must present ID approved by the bank. If the subject contacts the bank by telephone, the subject must go through a customer identity checking process to verify his/her identity and establish/authenticate that he/she is the correct customer.

The bank or Registration Authority may apply for independent confirmation before initiating revocation procedures.

Issuer specific

For DNB: The subject can revoke Mobile BankID on logged-in pages of the Internet banking service.

For Eika: The customer must contact the bank (RA) to ask for revocation. He or she can do this in person by bringing appropriate ID according to the Norwegian Anti-Money-Laundering Act, or by signed request (letter). If the customer phones the bank, the bank will verify the customer's identity in a secure way.

4 Certificate life-cycle operational requirements

The BankID CA-system and central servers and storage equipment are required to have a general availability of at least 99.7% measured over a one-month period.

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Persons with a customer relationship with a Bank acting as RA can submit a certificate application.

Applicants must be 13 years or older to apply for a BankID. Some RA Banks might limit this to 15 or 18 years. All applicants below 15 years must have permission from their legal guardian(s) to apply for BankID. Most RA Banks also require this for applicants below 18 years.

Applicants shall be identified at the RA as described in section 3.2.

The BankID COI verifies that all the necessary personal information required to issue the BankID certificate has been received from the bank acting as RA. If information is missing, the certificate can not be issued. In that case the bank acting as RA will be notified by the BankID COI Operator.

4.1.2 Enrolment process and responsibilities

Subscribers and parties relying on the mobile Personal BankID are informed of the related terms and conditions, as set out in section 2 in this TSPS, before entering into a contractual relationship. These terms and conditions are made available through the TSP's customer system. Changes to terms and conditions negatively impacting the subscriber must be actively accepted by the subscriber before going into effect. The subscriber will be notified if other significant changes implemented.

A mobile Personal BankID certificate applicant receives as part of the preparations:

- A copy of the agreement between the bank and the subject [20]
- Instructions for use and, if applicable, requirements for securing the user's device

The subscriber or subject does not give consent for publishing of the certificate.

The TSP will log and retain the signed BankID agreement with the Subscriber.

The subject has the opportunity to print out the agreement during the registration process.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

BankID is only issued following an order process that the customer has actively participated in. BankID is only issued when the Bank has approved the customer order.

As part of the BankID issuing process, the certificate applicant will receive a one-time code from the bank. The customer must enter his one-time code on the phone in connection with the certificate request.

The order shall contain the end user's mobile phone number. The BankID COI Operator checks which mobile network operator the mobile phone number is associated with. If the mobile phone number does not belong to a mobile network operator that has entered into an agreement about Mobile BankID, the bank acting as RA is notified of this.

The bank acting as RA shall provide a unique ID to ensure that the combination of "IssuerDN" and "subjectDN" is unique within the BankID domain.

The BankID COI Operator notifies the RA that the certificate application has been received.

Communication between the bank acting as RA and the BankID COI Operator is protected against unwanted disclosure and manipulation as described in section 6. A certificate request is always signed with the RA's private key. This signature is verified, logged and checked before the certificate request is forwarded to the CA-system on which the RA is entitled to issue certificates.

As part of the preparation, the bank shall create and distribute a one-time code (activation code) to the end user. Rules for the distribution of this code are governed by the associated certificate policy. The one-time code shall also be sent to the BankID COI Operator via the RA interface.

4.2.2 Approval or rejection of certificate applications

The RA will approve the certificate application if the following conditions are met:

- The person is a customer of the bank

- The person was successfully identified and authenticated, as described in 3.2.
- The person has approved the BankID agreement

If these requirements are not met, the application should be rejected. If the application is rejected, the applicant will receive a notification regarding this.

4.2.3 Time to process certificate applications

Issuing of Mobile Personal BankID is done with user interaction. If the certificate applicant satisfies all the requirements and hence is eligible for a Mobile Personal BankID, there will be no processing time at the RA for the certificate applications. After the certification request is forwarded from the RA to the CA, the certificate is issued in real time with user interaction, and is available for the end user within one minute.

The central storage entity receives the certificate order from the bank acting as RA via a dedicated interface. After successful validation of the certificate order details, the central storage entity will query the NRDB database for mobile network operator parameters. The central storage entity will forward a request to the mobile network operator for key generation. The key pair is generated in the subject's SIM card and the public key is then returned from the SIM-card and handset via the mobile network to the central storage entity which formats the PKCS#10 certification requests to the CA instance where the bank acting as RA is associated with. The CA instance provides a queuing system and issue the certificates in near real time. The certificates are encrypted and stored in the central storage entity database.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The end user must enter the one-time code (activation code, ref section 4.2.1) on the mobile phone before key generation can take place. The BankID COI Operator verifies the submitted one-time code before certificate generation can take place.

The key generation takes place on the end user’s SIM card. The end user selects a PIN (IDPIN or Sign-PIN) with 4-8 digits as protection for the private key. The public key is then sent via the mobile network and the mobile network operator to the certification authority system for certification.

There is no need for further interaction between the end user and the BankID COI Operator, and there is no need for distribution and installation of software on mobile phones to accomplish this.

The mobile network operator describes how the SIM card requirements are met in their security documentation.

The CA-system produces an end-user certificate based on information received from the RA (including the end user's mobile phone number) and the public key received from the end-user's mobile phone (via the mobile network operator). The issued certificates are stored in a central storage entity.

As part of this process, the end user is also asked to prove ownership of the private key by completing a mobile signature by a text string that the end user can read on the mobile phone. The signature is verified by the BankID COI Operator.

All communication between the central storage entity and the CA-system is protected by strong encryption and takes place in a closed network in a secure environment.

The production process for certificates consists of clearly separated parts (or functions) with corresponding subsystems:

The functions are:

1. Validation of certificate requests (unique name, syntax of elements in the certificate request, verification of sender)
2. Certificate generation
3. Distribution of certificate to central storage entity
4. Notification to mobile network operator that a certificate has been issued. The mobile network operator notifies the end user via SMS
5. Notification to RA that a certificate has been issued

If any problems occur during the certificate issuance, the issuer revokes any certificate that has already been issued as part of this issuance process and restarts the certificate issuance from the beginning. Depending on the error and its cause, the central storage entity can initiate a new certificate request based on available data.

The certificate issuer uses its certificate signing key to sign the certificates of the personal customer.

4.3.2 Notification to subscriber by the CA of issuance of certificate

After successfully generating BankID certificates, the certification authority system returns the certificates to the central storage entity.

The certification authority system notifies the central storage entity of the outcome of the issuance process and then makes the information available to the RA and the mobile network operator. Both RA and mobile network operator can notify the personal customer of the issuance of a Mobile BankID. When the subject has completed the activation process, he or she will be informed when the order is completed and Mobile BankID is ready for use.

After successful issuance and proof of possession, the subject will receive an SMS notifying that the Mobile BankID has been issued.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The TSP informs the bank acting as RA that the certificate has been generated. The bank acting as RA in turn is responsible for informing the subject. The bank acting as RA may choose to let the TSP notify the subject directly.

The personal customer has indirectly accepted BankID and certificates when:

- An agreement has been entered into, electronically or in writing.
- The certificate has been generated, and the personal customer has begun using it.

The personal customer thereafter has the status of BankID subject.

As part of activation the subject must perform a proof-of-possession of the private key. This constitutes certificate acceptance.

4.4.2 Publication of the certificate by the CA

The CA certificate is published according to section 6.8 in the BankID Certificate Profiles [13].

The complete and accurate certificate is available to the subject on the BankID website: https://www.bankid.no/en/private/solve-my-bankid-problem/view-your-bankid-on-mobile-certificate/

4.4.3 Notification of certificate issuance by the CA to other entities
Not applicable.

4.5 Key pair and certificate usage
BankID Mobile Personal use same key pair for authentication and signing.

4.5.1 Subscriber private key and certificate usage
Key Usage for the private key is NonRepudiation(1)/DigitalSignature(0).

4.5.2 Relying party public key and certificate usage
Key Usage for the public key is NonRepudiation(1)/DigitalSignature(0).

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal
Mobile Personal BankID supports renewal with or without certificate re-key.

Renewal without Subject involvement
Renewal without Subject involvement does not require a certificate re-key. Renewal without Subject involvement is used when Mobile BankID is renewed due to periodic expiration of the certificate. In addition, renewal without Subject intervention is used when there are systemic changes that do not affect the Subject's risk profile or user experience.

This includes if the cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised nor that the certificate has been revoked due to any other security breach.

The subject is notified of the renewal.It is not possible to change personal data in the certificate during this type or renewal.

The RA system does a periodic search for active mobile BankIDs and inform the service provider to renew the ones that expire in the next period without key changeover. A renew without key changeover is only done when the certificate has had a limited lifetime. The subject is not informed.

Renewal with subject involvement
Routine renewals with subject involvement require a certificate re-key. This type of renewal is used if there is a requirement to change the key size or hash function, or if there is a suspicion that the end user’s keys have been compromised. When renewing Mobile BankID when it has reached its expiration date, renewal with customer involvement may be used.

For renewals with customer involvement the bank shall offer a self-service solution that uses an approved authentication solution. Renewal is initiated by the customer, usually following prior notification from the bank.

If the information in the certificate changes, the bank must notify the customer to request the certificate is re-issued within a given time limit. The bank shall withdraw the certificate if the customer has not reactivated the certificate within this time limit.

If the subject fails to renew the certificate before it expires, he/she will have to follow the same procedure as for renewal after revocation.

In case of manual renew (change of names, etc.):

- Check for existence and validity of certificate to be renewed
- Verify correct identity based on the information from section 3.2.3

- Deliver new terms and conditions (if applicable)

Manual and auto renew:

- New key generation
- Certification of a new public key
- Revoking certificate for the old key pair (the certificate will be revoked from the time a new certificate is issued until it has expired)

Issuer specific

For Bankenes ID-tjeneste: Routine renewals with subject involvement using current customer information from the RAs customer ledger is offered via a self service solution similar to the one used for first time ordering (see section 4.2.1). If the information in the certificate changes (i.e. name changes) the customer is notified that the Mobile BankID certificate will have to be reissued.

For DNB: The subject has a self-service solution for deleting and re-order Mobile Personal BankID on logged-in pages at the TSP's Internet banking service. When the subject has deleted the Mobile Personal BankID, the customer go through same process as the initial certificate application process (4.2).

For Eika: Routine renewal of Mobile BankID for customers of Eika Gruppen follows the same process as for other Norwegian banks. The bank acting as RA with Eika Gruppen as TSP offers a self-service solution that uses an approved authentication solution. Routine re-key is initiated by the customer, usually after prior notification from the bank.

For Nordea: Revivification of subscriber identity is not required by Section 3.3.1.

For SpareBank 1: The certificate holder is notified in the internet bank about the forthcoming expire of the mobile BankID and is encouraged to renew the BankID with key changeover. The certificate holder is reminded to renew closer to the expire date if the BankID is about to expire.

4.6.2 Who may request renewal

The renewal function is only used for ordinary renewal of the BankID certificates to avoid expiration. Only the bank acting as RA may request ordinary renewal of the BankID.

4.6.3 Processing certificate renewal requests

Renewal without customer involvement

The renewal process consists of these elements:

- Re-certification of existing public key
- Revocation of the old certificate (the certificate will be revoked from the time a new certificate is issued until it has expired)

Renewal with customer involvement

The renewal process consists of these elements:

- Generating new keys and choosing an IDPIN
- Certification of a new public key
- Revoking certificate for the old key pair (the certificate will be revoked from the time a new certificate is issued until it has expired).

4.6.4 Notification of new certificate issuance to subscriber

Renewal without customer involvement
After renewal is requested from the RA to the CA, the renewal process will be processed by the CA as a background process. The Subject may be informed about the renewal from the bank acting as RA.

Renewal with customer involvement
The renewal process takes place as process where the Subject is actively involved. In this process, the renewal is requested from the RA to the CA, the renewal process will be processed by the CA in real-time after the Subject has generated a new key pair in the SIM toolkit application. The Subject is informed about the renewal in the dialogue.

4.6.5 Conduct constituting acceptance of a renewal certificate
For renewal without Subject involvement, acceptance of renewal takes place when the end user make use of the renewed certificate. The Subject may be informed about the renewal.

For renewal with Subject involvement, acceptance of renewal takes place, when the end user finalise the renewal procedure. the Subject will be informed about the renewal.

4.6.6 Publication of the renewal certificate by the CA
The renewed certificate is published to the central BankID database immediately after renewal.

4.6.7 Notification of certificate issuance by the CA to other entities
All entities in the BankID ecosystem will have access to the renewed certificate immediately after renewal.

The central storage entity will send a message to the mobile network operator when the new certificate is issued.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key
Ordinary re-key is performed as part of the renewal process with customer involvement.

This type of renewal may be used for ordinary renewals, but shall be used if there is a requirement to change the key size or hash function, or if there is a suspicion that the end user's keys have been compromised.

4.7.2 Who may request certification of a new public key
Only the RA may request certification of a new public key.

4.7.3 Processing certificate re-keying requests
See 4.6.3

4.7.4 Notification of new certificate issuance to subscriber
See 4.6.4

4.7.5 Conduct constituting acceptance of a re-keyed certificate
See 4.6.5

4.7.6 Publication of the re-keyed certificate by the CA
See 4.6.6

4.7.7 Notification of certificate issuance by the CA to other Entities
See 4.6.7

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

If the information in the certificate changes, e.g. if the Subject has changed their name, the issuer of BankID shall reissue a BankID with new information from the RA.

For this, the RA reissue function is used. The reissue function will generate a new certificate with changed content based on a new key pair generated in the end user's SIM card.

The banks have access to the National Population Register of Norway and any name change will be registered here and copied to the Banks registers. In case there is doubt about the identity of the person or a organisational change, the process in 3.2.3 and/or 3.2.5 will be followed.

4.8.2 Who may request certificate modification

The RA or the end user may request certificate modification.

4.8.3 Processing certificate modification requests

4.8.4 See 4.6.3.Notification of new certificate issuance to subscriber

For certificate modification the subscriber always takes part in the issuance of the new certificate.

After successful issuance, the subject is notified the Mobile BankID has been issued.

4.8.5 Conduct constituting acceptance of modified certificate

See 4.6.5

4.8.6 Publication of the modified certificate by the CA

See 4.6.6

4.8.7 Notification of certificate issuance by the CA to other entities

See 4.6.7

4.9 Certificate revocation and suspension

The bank acting as RA or the TSP may, in order to invalidate a certificate, choose either to revoke it permanently or to suspend it. A suspended BankID can be reopened, if the bank is certain of the identity of the owner and there no longer is any basis for the suspension. The TSP offers their subjects access to a service where they may request that their BankID is invalidated. This service shall be available 24/7/365. Alternatively, the subject may request the invalidation of one or more of the elements in the activation data necessary to activate the subjects BankID.

In general, the requirement for certainty and dialogue with the subject will be more stringent to revoke a certificate than to initiate a time-limited suspension.

The RA or BankID COI Operator shall log and archive all requests for invalidation, including how the request was received and what action the issuer initiated.

The mobile network operator shall log or archive all requests or incidents that may lead to a revocation.

Immediately after revocation or suspension of a subject’s certificate, the TSP will inform the Subject and Subscriber of the status change and reason, through the RA or it's operator according to agreed contact point.

The TSP is obliged to make correct and updated information available for the certificate validation service. Information about invalidated certificates shall be available 24/7/365. It shall contain all invalidated (revoked and suspended) certificates.

The TSP generates an updated revocation list at least once per hour and immediately makes the list available to certificate validation services. The CA-System's database of certificates and their statuses is available for the certificate validation services providing certificate status at the CA-system in real time. This list shall be archived for audit and control purposes.

Once a certificate is flagged as revoked in the central RA system it is not possible to reinstate the certificate.

Issuer specific

For SpareBank 1: Future revocation can be used in case of termination of agreement. Subscriber or TSP will set the date of revocation and the other party will be informed.

4.9.1 Circumstances for revocation

Certificates shall be revoked when the private key associated with the certificate is compromised or suspected to be compromised, or when the information in the certificate is known to be inaccurate.

Examples of causes for revocation are:

- Unauthorised or suspected unauthorised access to private keys
- Compromised activation data
- Known misuse of a certificate
- The subject has changed their name
- The subject is no longer entitled to have a certificate
- The subject terminates their customer relationship with the bank
- The subject terminates their customer relationship with the mobile network operator or other subscription conditions
- The SIM card or IDPIN is compromised or lost
- A new certificate is issued to the same mobile phone number
- The cryptography is no longer ensuring the binding between the subject and the public key.
- The certificate is no longer compliant with the CP under which it has been issued

4.9.2 Who can request revocation

The following can request revocation:

- Subject
- The bank that has entered into an agreement with the customer
- The TSP

Courts may rule to invalidate a certificate. The TSP must enact any such ruling.

Issuer specific

For Bankenes ID-tjeneste and DNB: Revocation can only be requested by the subject. Other persons may contact the bank on behalf of the subject to request suspension, the bank has a lower threshold for suspension than for revocation. See 4.9.14.

For Bankenes ID-tjeneste: Another operator or body may request revocation. Another operator or body may be the police, Nordic Financial CERT, Bankenes ID-tjeneste, Bits, Vipps, Finance Norway or another RA.

4.9.3 Procedure for revocation request

The subject may request revocation in the following ways:

- By physical presence, bringing appropriate ID, at the Registration Authority

- By signed request
- By phone

The bank or Registration Authority may apply for independent confirmation before initiating revocation procedures. If a subject wishes to revoke a certificate by unsigned electronic message, the subject must present ID approved by the bank.

If a bank is unable to maintain its obligations to other participants in the BankID partnership, there are routines for invalidating all certificates for the bank and its customers. This also applies to banks using a joint issuer.

The TSP, bank acting as RA, and their service providers log and archive all requests for invalidation, including how and when the request was received, what action the issuer initiated and the revocation reason. The request for invalidation is processed on receipt.

When the bank or RA has sent instructions to the service provider to revoke a BankID, the bank or RA must verify that the status of the relevant BankID has been changed in the certification authority system.

The bank shall send the subject written confirmation of revocation.

Issuer specific

For DNB and SpareBank 1: subjects can request revocation by phone.

For DNB: subjects can request revocation by self-service internet banking solutions.

For Eika: The customer must contact the bank (RA) to ask for revocation. He or she can do this in person by bringing appropriate ID according to the Norwegian Anti-Money-Laundering regulation, or by signed request (letter). If the customer phones the bank, the BankID will only be temporarily suspended, but even then the customer can ask the bank for revocation in special cases. In such cases the bank will still verify the customer's identity in a secure way.

4.9.4 Revocation request grace period

Relevant revocation/suspension information shall be available to certificate validation services no later than 15 minutes after the revocation request was registered and accepted. In some situations where operating deviations occur (see section 4.9.7), invalidation information may not be updated over a longer period.

4.9.5 Time within which CA must process the revocation request

Revocations have priority in the queuing application at the CA-system and will always be performed before issuing or renewing functions. After the CA-system has processed the revocation request from the RA, the CA-database is immediately updated with the certificate status.

In practice, the OCSP responder is set up to have real-time access to the CA-database, and hence always has real-time information about the status of any certificate issued by the CA.

The Subject is prohibited from using the private key if the status of the certificate in the CA-database is not active.

4.9.6 Revocation checking requirement for relying parties

The relying party is required to request a revocation status for all involved BankID certificates as part of a BankID transaction using authentication or signing keys.

In addition, the relying party is required to take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions in section 1.4 or the PDS and take any other precautions prescribed in agreements or elsewhere.

4.9.7 CRL issuance frequency

The certification authority system produces a signed revocation list (CRL) every 60 minutes. The CRL is archived on the certification authority system. All CRLs contain information about when the next CRL shall be made available. If necessary, it is possible to force the creation of a CRL before the next planned CRL.

A new CARL is generated at least once a year with a nextUpdate of 1 year after the issuing date. A new CARL is generated once a CA certificate has been revoked.

4.9.8 Maximum latency for CRLs

All CRLs from the CA-system is issued with a grace period of 24 hours.

4.9.9 On-line revocation/status checking availability

The TSP delivers an OCSP service which is available 24/7/365 for end users and BankID Merchants.

4.9.10 On-line revocation checking requirements

An on-line certificate status check shall be used where a response is obtained from a trusted Certificate validation service.

The Certificate validation service has direct access to the certificate status database in the CA system. Other subjects or relying parties cannot expect to directly access lists with suspension and revocation information. All BankID subjects and relying parties will have access to the Online Certificate Status Service to request information on the status of a certificate (validation).

The Certificate Status Service may have access to national identification numbers or other additional information about subjects, but will only make such additional data available to relying parties with legitimate requirements, and with whom they already have an agreement to this effect.

A request must be sent to the certificate Status service and be formatted in accordance with the OCSP protocol [11]. A certificate validation request from a merchant is signed with the relying party's private key. A certificate validation request from an end user is signed with the central storage entity's private key. The certificate validation service checks the signature in the request. The response from the certificate validation service is also in accordance with the OCSP protocol and signed with the certificate validation service's private key. Signatures shall be checked by both parties.

In accordance with the OCSP protocol, the certificate validation service will give the response "valid" for certificates that have not been revoked or suspended. If the certificate is marked as invalidated in the certification authority system's database, the certificate validation service will give the response "invalidated". The certificate validation service will give the response "unknown" for all certificates if the certification authority system's database is unavailable.

The certificate validation service can deliver additional information about the subject whose certificate the control request has been made for. The certificate validation service checks the authorisation of relying parties who request additional information. If the relying party has requested additional information from the certificate validation service, both request and response must be sent over a secure channel (TLS).

The Certificate validation service Servers and Database is synchronised with UTC at least every 24th hour.

4.9.11 Other forms of revocation advertisements available

Not applicable.

4.9.12 Special requirements re key compromise
Key compromise is described in section 5.7.

4.9.13 Circumstances for suspension
The TSP supports suspension (time-limited invalidation).

All conditions sufficient for revocation are also sufficient for suspension. Additionally, notification by phone to bank acting as RA or TSP is accepted. The bank acting as RA may also choose to offer its subjects the opportunity to suspend their own BankIDs through self-service solutions, i.e. in an online banking environment.

Suspension may be initiated when the subject asks for revocation but cannot present sufficient evidence of ownership to have BankID revoked. The same requirements apply for notification to the subject etc. for suspension as for revocation.

The bank acting as RA may also choose to suspend BankID when a person other than the subject calls on behalf of the subject, and he/she can justify why a suspension shall be initiated. The bank shall always control the identity of the contact person in accordance with standard practice.

The same requirements apply for notification from the bank to the subject etc. for suspension as for revocation.

4.9.14 Who can request suspension
The following can request suspension:

- Subject
- The bank that has entered into an agreement with the customer
- Registration Authority
- The TSP
- The mobile network operator
- Any other person related to the subject

Courts may rule to invalidate a certificate. The issuer of BankID must enact any such ruling.

Mobile network operator's obligation to request suspension
The mobile network operator shall promptly and without delay inform the bank of any suspicion or knowledge of the key store being compromised or lost or otherwise inaccessible to the subject. If this happens, the bank shall suspend the certificate. The mobile network operator shall notify the bank on a secured channel in the case of lost, compromised or inaccessible SIM cards, in accordance with the agreement between the bank and the mobile network operator.

The mobile network operator has implemented routines and application support for requesting suspension of the Mobile BankID associated with an MSISDN if any of the reasons for requesting suspension is fulfilled.

4.9.15 Procedure for suspension request
The subject may request suspension in the following ways:

- By physical presence, bringing appropriate ID, at the Registration Authority
- By signed request
- By phone

The bank acting as RA may also choose to offer its subjects the opportunity to suspend their own BankIDs through self-service solutions, i.e. in an online banking environment.

The bank acting as RA may also choose to suspend BankID when a person other than the subject calls on behalf of the subject, and he/she can justify why a suspension shall be initiated. The bank shall always control the identity of the contact person. The same requirements apply for notification from the bank acting as RA to the subject etc. for suspension as for revocation.

The mobile network operator will request suspension via the dedicated interface between the central storage entity and the mobile network operator system.

The mobile network operator has implemented system support for requesting suspension via the dedicated interface between the mobile network operator and the central storage entity.

Issuer specific

For Bankenes ID-tjeneste: Same procedure as for Revocation 4.9.3. Additionally, requests by telephone are accepted for suspension. The RAs will accept suspension requests by persons acting on behalf of the subject. On suspension the subject will be notified. Suspension may be performed as a self-service solution in some banks, based on secure login. If suspension is performed by a Service Provider, the Service Provider will inform the RA of the suspension, and the RA-application will show the certificate as suspended.

For Eika: All conditions sufficient for revocation are also sufficient for suspension. In addition, a request by phone is accepted, if there is reasonable reason to believe that the request represents the subject's wishes. The banks, Eika Service Centre and their Suspension Service Provider have a low threshold for suspension, and thus only ask for National ID number and name of the person requesting suspension. The suspension is then logged in the relevant follow-up system.

Eika has a service provider available for customers for suspension. Afterwards Eika informs the customer about the suspension.

For SpareBank 1: The subject may also request for suspension by phone and can use self-service in the internet bank.

4.9.16 Limits on suspension period

The certification authority system is designed to automatically track suspension periods. If the suspension period for a certificate exceeds 30 days, the certification authority system will revoke the suspended certificate and archive the relevant information in a central database.

The system supports reopening suspended BankID certificates within the 30-day suspension period. A suspended BankID will only be reopened if it has been proven within the suspension period that there no longer is any basis for the suspension.

To open a suspended BankID, the subject must appear in person in a bank office or contact the bank via phone. When appearing in the bank the subject has to show appropriate ID according to the Norwegian Anti-Money-Laundering regulation, and when contacting the bank via phone, he or she will be identified by the bank through a number of detailed security questions.

Reopening is initiated by the RA that has ordered the certificate after it is shown that the grounds for suspension are no longer present. All requests for the reopening of a suspended BankID are logged. The log entry documents how the subject was identified.

4.10 Certificate status services

4.10.1 Operational characteristics

The BankID COI Operator operates the certificate validation service on behalf of all the TSPs. The service is operated from two physically separated operational environments providing resilience and operational stability.

4.10.2 Service availability

The certificate validation service is available 24/7/365.

4.10.3 Optional features

The certificate validation service may optionally include in its response any of the following information items, if requested by a relying party - provided that the relying party has been granted access by the RA.

- Social Security number of the subject of the Person- or Employee BankID requested status for
- The associated BBAN account number of the Person- or Employee BankID requested status for
- The organisation number from the national number of enterprises of the Employee- or Merchant BankID requested status for

The RA will grant access for relying parties for one or more of the information elements above, according to National Law - i.e. the Personal data act.

4.11 End of subscription

The subscriber may without prior warning terminate the agreement with the TSP.

The TSP or bank acting as RA may terminate the agreement with 4 weeks warning for objective reasons. If the TSP terminates the agreement the reason shall be communicated.

The TSP or bank acting as RA may terminate the agreement with immediate effect if the subject has been found guilty of gross misconduct and breach of the agreement.

Upon termination, the subject shall immediately destroy all software and documentation that the subscriber has been given in order to use BankID.

The BankID certificates will at the same time be revoked.

If the end user subscription with the mobile network operator is terminated, the certificates associated with the subscription will be withdrawn.

If an agreement between a mobile network operator and a bank is terminated, all certificates associated with the subscriptions held with this mobile network operator will be withdrawn.

4.12 Key escrow and recovery policy and practices

The Mobile BankID end users creates the keys on the SIM and no copies are made.

4.12.1 Key escrow and recovery

BankID does not issue or support certificates with key usage encryption.

Private keys (authentication and signing keys) associated with Mobile Personal BankID are generated and used in a secure environment in the end user's SIM card. The private keys can not be exported outside the secure environment.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable

5 Facility, management, and operational controls

5.1 Physical controls

Physical security barriers and controls are implemented to control access to the certification authority system hardware and software. This includes central servers, HSMs that allow access to private keys and other limited data in the central storage facility, as well as any external cryptographic hardware module or smart card. All physical access to these areas is logged by the BankID COI Operator.

All private keys are physically protected as described above. This applies to Level 1 CA's own keys for signing certificates and CRLs, keys used for secure communication between the CA and the central infrastructure units, and private keys stored in the central storage entity.

The CA-system also has facilities for storing backups and distribution media that is sufficiently secure to prevent loss, forgery or unauthorised use of stored information. Backups are stored both for data repair reasons and for the purposes of archiving of important information. Backups are stored at an alternative location to enable reconstruction in case of a disaster at the primary location.

Periodic security checks are performed at the CA location and in the central storage entity.

The BankID COI Operator performs a visual monthly check to ensure that the CA system and all associated cryptographic devices that are not in use are securely stored, that the physical security systems (door locks and alarms) work as intended, and that there have been no attempts at break-ins or unauthorised access. The results of such checks are logged.

All physical, organisational and personnel-related security controls are approved by the TSPS approval body (Bits AS).

There are physical barriers and controls to control access to the RA applications' hardware and software and all physical access to these areas are logged.

5.1.1 Site location and construction

BankID COI

All production tasks take place in an environment with multiple layers of physical and logical security.

In the security rooms the walls are protected with an intrusion grid from floor to the ceiling. The area is monitored by cameras outside/inside the room.

5.1.2 Physical access

BankID COI

The production environment is divided into different security zones. Access rights and user roles are defined for each zone. Only defined user roles are granted access to their designated secure zones.

Access to the CA zone requires at least two people with different user roles to be present to operate as intended (ref. section 5.2). The access control system is able to recognise the individuals and their roles, and there is more than one authentication mechanism in place before access is granted to the CA-system or to devices that store confidential data associated with the certification service. The operation of production equipment for central storage equipment containing or handling end user keys and other strictly confidential data is governed by the same rules as for the CA-system.

Routines for access control are defined and enforced by the BankID COI Operator. Physical entrance logs are checked against the user logs once per month. The effectiveness of physical access controls is tested and checked at least annually

The BankID service is run inside dedicated security rooms in different datacentre. There is dual access for entering the security room. Physical keys for entering the security room are stored within a KeyWatcher and access are given to certified personnel only. Both certified personnel has to enter PIN code to take out the physical keys within the KeyWatcher. After opening the physical locks, they need to swipe their ID cards simultaneously and enter their personal PIN codes in order to enter the room. Once inside the room both certified personnel need to swipe their cards within a time limit, to prevent the intrusion alarm to be released. If this procedure is not followed, the alarm will be triggered and 24/7 onsite security personnel are alerted. Both the KeyWatcher and the security room are monitored 24/7 by cameras. Logs are regularly reviewed by the security officer.

All visitors have to be authorised by personnel that are responsible for physical access to the data centre, in order to achieve this access the visitor has to deposit their official ID card, fill in a visitor declaration including security instruction, and have certified personnel approving and accompanied the visitor throughout the visit. When inside the security room, a physical log book is updated with the name of the visitor, date, time in and time out, reason for the visit and a referral to the certified personnel accompanying them. The visitor is accompanied until checking out and leaving the BankID COI Operator premises.

RA applications

All production equipment is placed in a secured environment with multiple layers of physical and logical security. The production environment is divided into different security zones. Only defined user roles are granted access to their designated secure zones. The data halls are dimensioned to resist serious and long-term unforeseen events that can lead to disruption. Backup are contained in these data halls or in secured external locations.

5.1.3 Power and air conditioning

BankID COI

The production environment is equipped with an air conditioning system.

The equipment is protected against direct damage due to power outage and is equipped with additional power supply/circuits. The additional power supply also covers the air conditioning and the alarm system.

RA Systems

For Nordea: A supervision system monitors the state of technological systems (electrical and air conditioning systems) 24/7 all year round and allows to locate any anomaly quickly.

For SpareBank 1: For the RA system: Data centres have air conditioning system, Uninterruptible Power Supply and backup power generator.

5.1.4 Water exposures

BankID COI

The production environment is protected from water intrusion and water damage. Electronic sensors have been installed to trigger warnings in case of water intrusion.

RA Systems

For the RA system: Data centres are protected from water and both data centres can operate alone in case the other one is unavailable.

5.1.5 Fire prevention and protection

The production environment is protected against fire. Automatic fire alarm and extinguisher systems are installed that do not damage hardware or data.

5.1.6 Media storage

The TSP has policy and procedures for secure handling and protection of media from damage, theft, unauthorised access and obsolescence. The media management procedures shall also protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Media are stored in the same room as the certification authority system, e.g. to the same security standards. All media that are removed from the secure room are sealed and processed in accordance with ”BankID Internal Security Procedures” [3]. All media and storage objects containing sensitive data will be electronically shredded after use. Only Trusted roles have access to the media and are the ones that carry out these procedures.

Issuer specific

For Eika: Daily backups are stored according to the same security standards as the registration authority system.

For Nordea: All media storage containing software and data, audit logs, archives, or backup information are stored within the datacentres of the Nordea with adequate physical and logical access controls designed to limit access only to authorised personnel and protect such media from accidental damage. Encryption materials are protected by locked safes, cabinets and containers. The opening and closing of cabinets or containers is recorded for audit checks.

For SpareBank 1: Media are stored in the same room as the RA system or in a safe with limited access.

5.1.7 Waste disposal

BankID COI

All media containing sensitive information should be securely destroyed before disposal. This is described in “BankID Internal Security Procedures” [3].

RA Systems

For Eika: All media containing sensitive information are adequately deleted by approved software or equipment before it is disposed of.

For SpareBank 1: For the RA system: All media is destroyed as part of disposal procedures.

5.1.8 Off-site backup

BankID COI

For the central infrastructure, backups are managed in such a way that all data in the certification authority system are replicated to another location with the same security level to ensure that the system can be recovered after a possible disaster. Data traffic between locations is routed a secured and closed network.

RA Systems

For Bankenes ID-tjeneste: Secure copies of data used and generated in the RA Application are stored in a separate location to the production site.

For Eika: Backup systems ensure continued operation in cases of disruption. Backups are stored under the same security regime as the production environment.

For Nordea: Nordea performs backups of critical system data, audit logs and other sensitive information by means of a synchronous remote copy. The secondary site is in synchronous remote copy.

For SpareBank 1: For the RA system: Both data centres can operate alone in case the other one is unavailable.

5.2 Procedural controls

5.2.1 Trusted roles

Access to information and application system functions is restricted in accordance with the TSP's access control policy, and practices set out in this document. The TSP system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.

A role is, for the purpose of this document, defined as the right to perform certain tasks. The following trusted roles have been defined for operational tasks associated with BankID issuing systems and Registration Authority:

a) Security officer: Overall responsible for administering the implementation of security policy and practices which falls within the specific services delivered
b) System administrator: Authorised to install, configure and maintain the CA trustworthy systems
c) System operator: Responsible for operating the CA trustworthy systems on demand. Authorised to perform CA backup and recovery
d) System auditor: Authorised to view archives and audit logs of the CA trustworthy systems
e) Compliance manager: Responsible for testing and verification of compliance, in addition to also performing the system auditor role
f) Registration Officer, responsible for approving end entity Certificate generation and revocation
g) Revocation Officer, responsible for approving end entity Certificate revocation

Managerial personnel: Responsible for all Security roles and responsibilities, as specified in this TSPS are documented in job descriptions or in documents available to all concerned personnel. Trusted roles are named by the management and is accepted by the management and the person to fulfil the role. Managerial personnel are experienced or trained with respect to the trust service that is provided, familiar with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions. Regular review of user access privileges for trusted roles are carried out, when individuals change jobs internally or leave the company the access rights are removed. All TSP personnel use personnel user accounts with privilege access rights in order to identified and authenticated every user before using critical applications related to the service.

Key custodians: Responsible for secure storage and entry of components of cryptographic keys and passwords in accordance with a risk assessment for the type of key. May be people appointed by Bits AS, the Issuing banks or the trust service provider organisation.

Personnel with a trusted role has other access and higher privileges than general functions at the TSP. Access rights are approved by management for named individuals based upon the principle of segregation of duties and least privilege access. There are specific requirements that applies for trusted roles since these positions are very sensitive based on the duties that they perform and access levels they have, and access rights will be granted to personnel only after all necessary checks

are completely performed. See section 5.2 and 5.3 in this document for practices performed for background screening, skills, experience, training and awareness.

TSP management see to that all TSP personnel in trusted roles are free from conflict of interest that might prejudice the impartiality of the TSP operations. To comply with this requirement there are internal and external audits, as well as risk assessments carried out and approved by TSP management.

5.2.2 Number of persons required per task

BankID COI

At least two persons fulfilling two separate roles of 5.2.1 must be involved to obtain physical access to the CA trustworthy systems or perform security sensitive operations on those systems. For access to the CA system both persons must undergo multiple levels of authentication, and present evidence of identity including two factors, something they have and something they know.

At least two individuals must be assigned and trained to perform each role.

Personnel at the BankID COI Operator (both permanent and temporary) shall have job descriptions designed from the viewpoint of roles fulfilled with segregation of duties and least privilege. It shall however always be clear in which role the person performs a certain task at the CA trustworthy systems.

The tasks of key generation and initialisation of secured storage media for the CA trustworthy systems shall require at least three persons to be present, in the roles c), d) and f) listed above.

After the initial key generation, the person(s) in role f) – key custodian – will be equipped with a specific security element, e.g. a card that has to be entered and read into a security module. This will make it possible to distinguish security-sensitive tasks involving the key custodian from normal operation of the CA trustworthy systems.

If keys are to be split into components for storage, a key custodian must be present for each part that the key is split into.

When media or components that may contain secret keys, are disposed of, at least two trusted persons in two roles must be present to ensure that sensitive data contained in the components are securely shredded.

Issuer specific

For Bankenes ID-tjeneste: Handling of CA and RA security elements are regulated and documented through various routines, requiring at least two persons being involved in all handling of CA and RA security elements associated with the BankID system itself.

Bankenes ID-tjeneste has in its possession CA security elements that have been issued by BankID COI under the key ceremony for CA, securely stored in a safe requiring two person access, one of them being Bankenes ID-tjeneste's Key Custodian

The RAs have in their possession RA security elements that have been issued by BankID COI under the key ceremony for the RA. These are installed in HSMs requiring two-person access (operator and Security Officer). After installation they are stored in sealed security envelopes in safes.

For Eika: The operators and technical staff at Eika Gruppen and its operational supplier may, based on a risk evaluation, have access to the operational environment alone, and can perform tasks on the BankID solution. To access the systems, they must, however, undergo multiple levels of authentication.

For SpareBank 1: The TSP has the following practices:

- Two persons from different departments are needed for handling HSM backup
- Two persons from different departments are needed to access HSM backup keys
- Multiple persons are defined at Key Custodian
- Multiple persons are defined as personnel for handling HSM backup
- Multiple persons are defined as personnel with access to HSM backup keys
- Multiple persons are defined personnel as System administrator

5.2.3 Identification and authentication for each role

BankID COI

CA key pair generation and the subsequent certification of the public key is undertaken in a physically secured environment by personnel in trusted roles. The number of personnel authorised to carry out these functions is kept to a minimum with certified and named persons authorised to access the secure premises and perform the certification process.

- Authorised personnel need to be employed by the BankID COI Operator and thus identified by the HR department.
- Authorised personnel need to be authorised to a specific trusted role by senior management.

The detailed procedures for identification and authentication is described in the security documentation of the operator of CA and central storage entity.

Issuer specific

For Bankenes ID-tjeneste: Bankenes ID-tjeneste, RAs and RA-application providers use personnel with experience and training necessary for provision of services with the required quality, in accordance with functions and roles performed by the personnel involved.

Trusted roles will be held by personnel with required qualifications.

For DNB: The Key Custodian updates the standard procedure, and relevant objects when needs change. Key Custodian routines are confidential.

For Eika: Those who hold certain trusted positions within BankID in Eika Gruppen, will be personnel specially qualified for this. To be considered for some trusted roles, except RA Officer, it is a requirement to have prior experience from working with BankID in both a commercial and a technical sense. They will have competence on specific system functionality, processes, and security.

For SpareBank 1: For hiring and training, ordinary routines for identification at the TSP is used. All personnel are authenticated before performing any tasks.

5.2.4 Roles requiring separation of duties

BankID COI

The BankID COI Operator has established a segregation of duties through an organisational structure. The following roles need to be separated:

- Security Officer
- System Administrator
- System Operator
- System Auditor
- Registration Officer and Revocation Officer

Issuer specific

For Eika: Eika Gruppen's security policy for BankID establishes that employees cannot have other assignments that could conflict with duties and responsibilities arising from BankID roles. This is relevant e.g. for those who have control responsibilities internally in the bank. Naturally, they will not have tasks related to what they are supposed to review/revise.

For SpareBank 1: The TSP has a segregation of duties through an organizational structure. Multiple persons ensure control of changes. The following roles need to be separated:

- System administrator
- Product Owner

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Personnel working with the certification authority system or central storage entity are individuals with authorised trusted roles, solid PKI and BankID expertise. All personnel at the BankID COI Operator are employed for at least 6 months and given proper training before they can access the certification authority systems.

The BankID COI Operator has established and shall maintain recruitment screening processes and training processes for personnel who will work on the system. This is documented HR routines and IT training plans. In addition, the BankID COI Operator has specific training for new employees or consultants.

Issuer specific

For Bankenes ID-tjeneste: Requests for Mobile BankID is usually performed by self-service by the Certificate Applicant. Critical activities on the RAs part are those that concerns ordinary tasks like authenticating new customers and maintaining the customer's records. Those are basic processes of an bank and audited internally, as well as through audits by The Financial Supervisory Authority of Norway.

RA Officers operating the RA-application are required to have knowledge, experience and training to perform that role.

For DNB: Both the service providers' and the TSP's personnel are required to have the requisite knowledge, experience and qualifications to perform their roles properly. It is deemed acceptable for an operator to have a Mobile Personal BankID issued by the Registration Authority in which the person in question works.

For Eika: Those who hold certain trusted positions within BankID in Eika Gruppen, will be personnel specially qualified for this. To be considered for some trusted roles, except RA Officer, it is a requirement to have prior experience from working with BankID in both a commercial and a technical sense. They will have competence on specific system functionality, processes, and security.

The level of training is adapted to individual roles and areas of responsibility. Persons with specific tasks related to BankID at Eika Gruppen will receive thorough training both before and after starting their tasks.

Personnel will not have access to the trusted functions until any necessary checks are completed and formally appointment is confirmed.

For SpareBank 1: Specific routines, guidelines and training material have been created for the BankID area.

5.3.2 Background check procedures

The TSP will perform certain background checks. Personnel will not have access to the trusted functions until any necessary checks are completed and formally appointment is confirmed. Personnel working with BankID COI will always be subject to a security meeting conducted at the start of the assignment and then annually.

The BankID COI Operator is not authorised by law to require an employee or job-seeker to submit a police clearance certificate but will, in the event of doubt, conduct an extended reference check.

5.3.3 Training requirements

No personnel are granted access to the BankID production system until they have reached a sufficient level of proficiency in the pre-production system.

All personnel who require access to the production systems must have been employed for a minimum of 6 months and have demonstrated their knowledge and skills in the test environment. The security officer will meet with the relevant personnel to convey instructions about security and knowledge related to the value chain.

All personnel have received extensive PKI and BankID training.

Personnel receive training according to the BankID COI Operator routine descriptions for new personnel. On call personnel must comply with additional requirements and routines and must be evaluated to have sufficient competence level before they are given access to the system.

Issuer specific

For Bankenes ID-tjeneste: Employees of the RA performing tasks related to establishing and maintaining customer data, authentication procedures and maintaining certificate status are given training in products, procedures and applications used.

For DNB: All RA Officer routines that includes BankID are closely described in work description. All RA officers get training in BankID, how to use and risk connected to Personal BankID and Mobile Personal BankID. Training consists of digital course, tasks for finding answers in routines, problem solving in the system applications, discussion tasks, customers cases and communication training.

For Eika: The level of training is adapted to individual roles and areas of responsibility. Persons with specific tasks related to BankID at Eika Gruppen will receive thorough training both before and after starting their tasks.

Line management is responsible for initiating necessary training concerning BankID for employees who need this.\

For SpareBank 1: RA officers has to complete a digital training course before getting access to the RA system.

5.3.4 Retraining frequency and requirements

All BankID personnel working with BankID on a daily basis are also involved in changes to the infrastructure. For releases of new software in production, the people who have followed the release through test environments must be present.

In addition, periodic training updates on new threats and current security practices are conducted at least every 12 months to establish continuity and updates in the knowledge of the personnel and procedures.

5.3.5 Job rotation frequency and sequence

There is no formal job rotation scheme deployed for personnel in trusted roles. Changes in roles do occur and is managed through training and competences management with respect of segregation of roles where applicable.

Issuer specific

For Bankenes ID-tjeneste: HR guidelines for each participant Bank applies.

For SpareBank 1: System administrators are rotated to make sure enough personnel have good knowledge of the system.

5.3.6 Sanctions for unauthorized actions

All personnel are responsible for their actions. Authorised personnel working for the BankID COI Operator who seriously violate policies and practices described in this TSPS, either negligently or intentionally, shall:

a) Have their access revoked
b) Be subject to internal disciplinary proceedings
c) Potentially face criminal prosecution

Issuer specific

For Danske Bank: Danske Bank has disciplinary sanctions in place in the Group HR policy and practices.

For Eika: Breach of the BankID and ICT guidelines and directives can lead to consequences for the user's rights and employment conditions with Eika Gruppen. Violation of these guidelines and directives can lead to dismissal or that the user is being refused access to all of or parts of the ICT system. In addition, Eika may implement sanctions according to other rules.

External hired consultants can be subject to similar sanctions.

For SpareBank 1: TSP have routines for handling unacceptable actions by employees. Standard routines are used for BankID related cases as well.

5.3.7 Independent contractor requirements

Contract staff performing trusted roles and tasks must have been in employment with their current employer for at least 6 months. Contract staff may be subject to the same sanctions as employees in the event of violation of instructions.

During training there are specific topics on the BankID COI Operator security framework and Secure Software Development Life Cycle. In addition, there is a separate review of NDA with consultants and employees.

Issuer specific

For Bankenes ID-tjeneste: All contracting personnel at RAs or Service Providers performing trusted roles and tasks, are subject to the same regulations as permanent employees.

For DNB: Security checks are covered in the agreement with the providers and are in conformity with current regulations and the TSP's requirements for security solutions.

For Eika: Contract staff in Eika Gruppen performing trusted roles and tasks must have been in employment with their current employer for at least 6 months. Eika can make exceptions for staff that is known to them from previous engagements.

For SpareBank 1: TSP has routines for handling security sensitive information that also applies to BankID related matters. All employees and hired personnel must sign a confidentiality agreement.

5.3.8 Documentation supplied to personnel

All personnel are given the necessary documentation to perform their tasks.

Documentation regarded as particularly sensitive shall be kept within the BankID COI Operator 's premises. Personnel employed by the bank, registration authority, issuer, Vipps AS, Bits AS or the BankID COI Operator who legitimately need to know, can be granted permission to read these documents in areas approved by BankID COI Operator, provided they sign a non-disclosure agreement.

5.4 Audit logging procedures

BankID COI

These procedures apply to all devices involved in the issue of certificates and CRL.

The audit log is a tool for documenting and retrieving information about events concerning security in BankID. The audit log can be seen as a distributed set of data located at RA, Certification Authority System and central storage entities. The individual parties will provide additional information about local requirements for implementation in their security documentation.

The audit log is used to maintain a secure production environment.

The logs are stored securely and in such a way that they can be made available for review in a timely manner.

All audit logs are backed up by sending all logs to a central log repository. In the central log repository, all logs are rotated and kept according to section 5.4.3. Central log repository is replicated in two separate locations inside secure rooms. All sensitive information is stored in the security rooms. There are two separate disc cabinets in two separate data centres. Only authorised personnel can access the information. All access to this information are requested and logged in the BankID COI Operator Change management system.

Issuer specific

For Bankenes ID-tjeneste: The RA Application Service Providers have logs for management of RA keys.

All Messages between RA and COI are logged and securely stored for a minimum of 10 years.

For DNB: Access to the log is protected by the bank’s authorisation system and the logs may only be accessed by authorised personnel

Important events during the operation of certification authority systems shall be stored for a minimum of 10 years.

For Eika: All audit logs are kept for as long as the BankID regulations and the Norwegian laws requires. Logs of status modifications to the certificate are stored for 10 years. Backup are normally also stored for 10 years.

The logs are stored securely and in such a way that they can be made available for review in a timely manner. All log information is stored according to legal requirements in the BankID regulations or Norwegian law. If the Eika Gruppen terminates as TSP, the logs will be preserved in a readable way for as long as Eika Gruppen's legal requirements are still valid.

Eika Gruppen also has various security systems to protect their solutions and systems, including logs.

All security policy changes in Eika Gruppen are revised in a traceable manner.

Eika produces electronic event logs that, among other things, log all status modifications to BankID certificates and various security events.

Eika also has logs attached e.g. to document handling, CA and RA security elements, and various revisions.

Eika has event logs also for reported events.

Manual logs are stored securely protected, if this is considered necessary.

For SpareBank 1: These procedures apply to all RA system components:

The audit log is a tool for documenting and retrieving information about events concerning security in BankID.

The audit log is used to maintain a secure production environment.

The logs are stored securely and can be made available for review in a timely manner.

5.4.1 Types of events recorded

BankID COI

The following events are recorded in the CA-system and at the certificate validation service. The log function also includes failed attempts at triggering these events.

- System (operating system) starting and stopping
- Starting and stopping of all applications in the certification authority system
- User administration in the certification authority system
- All changes to software/parameters in the certification authority system
- Login/logout to/from operating system and applications in the certification authority system
- All requests and associated messages
- Issued Certificates
- Renewals and associated messages
- Changes and renewals of key materials in the certification authority system
- Revocation messages and associated messages

Most of these events are automatically logged in the certification authority system. Some events are logged manually, such as software changes, policy changes, and renewal of Level 1 key material.

The following events are logged by the BankID COI Operator:

- System (operating system) starting and stopping
- Starting and stopping of all applications
- All changes to software/parameters
- Renewal of key materials
- User administration
- Login/log out information
- Information about the end user and relying party
- Relevant information about the transaction (identity validation/signing)

All firewall and router activities are logged.

- NTP sync

Most of these events are automatically logged in the central storage entity. Some events are manually logged, such as software changes.

Issuer specific

For DNB: All communication between the issuer and ODS (order and distribution system) is logged by means of activity controls in the RA system. This also includes status requests, the initiation of revocations and suspensions of certificates.

Required documentation e.g. passport is stored on customer profile in our internal customer handling system.

For Eika: Eika produces electronic event logs that, among other things, log all status modifications to BankID certificates.

Eika also produces electronic event logs that, among other things, log different system and hardware events.

Eika has logs attached e.g. to document handling, CA and RA security elements, and various revisions.

Eika has event logs also for reported events.

For SpareBank 1: The TSP has the following practices:

The audit log record relevant events:

- Events on the RA
- Events during the operation of the RA system

The following events are logged:

- System (operating system) starting and stopping
- Starting and stopping of all applications
- All changes to software/parameters
- Login/log out information
- Information about the end user and relying party
- Relevant information about the transaction (identity validation/signing)

The events are automatically logged. Some events are manually logged, such as software changes.

5.4.2 Frequency of processing log

BankID COI

The logs are created in real time and can be inspected at any time by an operator with sufficient access rights. CA system and central servers in the operating infrastructure are either automatically monitored on a continuous basis, with alerts for security-sensitive events and traces of hostile behaviour, or reviewed by an operator with sufficient privileges, at least once a day.

For the CA-system the following applies

The CA system signs all database entries with its own internal CA key, related to Issuing, suspending and revocation of certificates, as well as tasks done in the CA Operator software by an authorised operator. All archived logs are kept in 2 separate secure room in two separate data centres for 10 years.

Audit logs from certification authority systems are monitored continuously and alarms are sent to the Security Officer in case of suspicious events. The Security Officer conducts weekly random checks

to look for abnormal events. Every 6 months an extended verification of audit logs for the certification authority systems takes place.

For the RA-system

For the RA bank systems, the following applies:

RA systems have routines for automatic reviews that shall recognise specific negative events and trends.

Issuer specific

For Bankenes ID-tjeneste: Logs concerning certificate events are available for each RA in their RA-application. RAs are responsible for controlling their logs.

Logs will contain information that indicate abnormal activities.

For Eika: Eika Gruppen has various security systems to protect their solutions and systems, including monitoring of a number of different system and customer events based on the threat level at any given time.

Eika Gruppen's BankID solution is monitored. The logs are constantly available for operators with sufficient right of access.

Eika Gruppen will further retrieve and review event logs as needed. The logs will be reviewed by an operator with sufficient right of access.

All security policy changes in Eika Gruppen are revised in a traceable manner.

5.4.3 Retention period for audit log

Logging and use of BankID certificates is stored for 10 years after the certificates expires.

Audit logs are stored for 10 years.

5.4.4 Protection of audit log

BankID COI

Audit logs on the CA system are signed with the issuer's private key and timestamped. Section 5.2 contains a description of who has the authority to read logs on the certification authority system.

Audit logs are protected at the same level as the data in the CA-system. Manual logs are stored in the same physical security zone as the certification authority system. Only personnel with authorised access to the certification authority system can therefore access these logs.

Central log repository is replicated in 2 separate data centres inside corresponding secure rooms, and all access to them is monitored and logged.

Issuer specific

For Bankenes ID-tjeneste: The RA-Application logs are integrity protected.

For DNB: Access to the log is protected by the bank’s authorisation system and the logs may only be accessed by authorised personnel.

For Eika: Current data records and logs are stored securely in the ICT systems. Eika Gruppen also regularly performs backups of all their data records and electronic event logs for the RA solutions.

Manual logs are stored securely protected, if this is considered necessary.

For SpareBank 1: RA Security logs are kept in a safe environment. Only approved personnel can access the logs.

5.4.5 Audit log backup procedures

BankID COI

For the CA-system and central servers and storage equipment, server and application generated logs are backed up at least once every 24 hours. All logs are integrity protected.

Backups are stored in a separate location, subject to the same access control as the original.

Audit logs are processed by the normal routines for backups that exist within the certification authority system.

Manual logs are backed up routinely.

All audit logs are backed up by sending all logs to a central log repository. In the central log repository, all logs are rotated and kept for 10 years. Central log repository is replicated in 2 separate locations inside secure rooms

Backups are taken every day, and copied to the security room in the secondary data centre.

Issuer specific

For Bankenes ID-tjeneste: The RA-Application logs are backed up and backups available at a physically separate backup site.

For Eika: Current data records and logs are stored securely in the ICT systems. Eika Gruppen also regularly performs backups of all their data records and electronic event logs for the RA solutions.

Manual logs are stored securely protected, if this is considered necessary.

For SpareBank 1: All RA logs are generated by the system and backups are made according to ordinary backup routines.

5.4.6 Audit collection system (internal vs. external)

BankID COI

The audit collection system is internal.

5.4.7 Notification to event-causing subject

BankID COI

There is no requirement to notify the Subject who caused an audit event.

5.4.8 Vulnerability assessments

The operation of the CA and central storage entity is subject to periodic vulnerability assessments and whenever a critical part of the operation is changed. The assessment covers the operational infrastructure, cryptographic equipment, the physical environment, data storage, software, personnel, processes and procedures and communication.

The BankID COI Operator perform a regular vulnerability scan on public and private IP addresses and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

The BankID COI Operator conducted a penetration test on the CA and the central storage infrastructure at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant. The BankID COI Operator keeps records of evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

Issuer specific
For Bankenes ID-tjeneste: Vulnerability assessments are performed regularly for RA systems.

For DNB: Vulnerability assessment is part of the annually Risk assessment of BankID and RA solution

For Eika: Eika Gruppen performs vulnerability assessment of the BankID solution according to the continuous threat situation.

For SpareBank 1: As part of major changes in services and infrastructure, a vulnerability assessments is conducted.

5.5 Records archival

5.5.1 Types of records archived
Each RA archives information about the following:

- The type of ID document presented by the applicant during registration. This is usually a the subject's passport.
- A copy of the ID document's page, including name, picture and other identification data of the subject and document.
- Any specific choices in the subscriber agreement
- The identity of the employee accepting the application
- Method used to validate identification documents

BankID COI
All events related to management of CA keys will be signed and stored in the CA database (by the CA Operator credentials) and also in written copies in the Key Ceremonies performed on the BankID Root CA.

All order messages exchanged between the bank/RA and the certification authority system are stored in a permanent archive.

Information to be stored in records in the archive:

- Registration of new subjects
- Certificate requests
- Technical checks of mobile telephone, subscription and SIM card in connection with certificate issuance
- Events in connection with key generation on SIM cards
- Issued Certificates
- Agreements about certificates and protection of keys and activation data
- Renewals of certificates and associated messages
- History of Key Changeovers on the Registration Authority System
- Invalidation requests (revocation or suspension) with associated messages
- Events at the mobile network operator that may result in revocation of a certificate
- Historical invalidation and revocation information
- Current and expired policies and CPSs

The RA is the party handling subscriber information, and responsible to keep the following records:

- The subject's identity, see section 3.2.3
- The subscriber agreement

Issuer specific

For DNB: The TSP keeps logs, as described in section 5.4. Current and expired CPS and policies are stored by Bits AS. The issuance and use of OTP mechanisms are logged in the bank. The bank archives current and expired CPS (TSPS).

For Eika: Eika Gruppen stores all confirmed copies of identification documents and signed agreements in a secure and retrievable way for as long as the legal regulations require.

Eika Gruppen copies and stores the following registration information:

- Copy of the original identification document with certain additional information. This copy is then archived at the bank so that it is retrievable.

Eika produces electronic event logs that, among other things, log all status modifications to BankID certificates and various security events.

Eika also has logs attached e.g. to document handling, CA and RA security elements, and various revisions.

Eika has event logs also for reported events.

5.5.2 Retention period for archive

Archived records are stored for 10 years.

Expired certificates and associated public keys are available for 10 years after expiration. Expired private keys are not archived.

The CRLs issued by the CA is kept in archives for 10 years.

The Certificate Validation Service keeps the revocation status information online at least until the certificates expire. After the certificate expiration, the CRLs are kept archived on media according to section 5.1.6 for at least 10 years. There are 3 copies of the media, 2 kept at the BankID COI Operator's 2 different locations and 1 at the Issuers location.

Important events during the operation of certification authority systems are stored for a minimum of 10 years. Other items in the audit log are stored for a period between 3 months and 10 years depending on risk-demand assessment.

All log information is stored according to legal requirements in the BankID regulations or Norwegian law. Logs of status modifications to the certificate are stored for 10 years.

5.5.3 Protection of archive

BankID COI

Only authorised personnel at the Bank, Registration Authority or BankID COI Operator shall be allowed to read archived data. All archived data is integrity protected.

Issuer specific

For Bankenes ID-tjeneste: See 5.4.4.

For DNB: The requirements for making security copies of archived data are observed. The standard procedures for this are described in the document "BankID - Internal Security Procedures".

For Eika: Current data records and logs are stored securely in the ICT systems. Eika Gruppen also regularly performs backups of all their data records and electronic event logs for the RA solutions.

Manual logs are stored securely protected, if this is considered necessary.

For SpareBank 1: Security requirements for the archiving systems are agreed upon in the service vendor agreement. Accesses are granted and withdrawn according to ordinary access routines.

5.5.4 Archive backup procedures

For the central PKI system, archived data must be written to media suitable for long-term storage.

Two copies of archived electronic information shall be stored, in two different places.

Issuer specific

For DNB: Requirements for backups of archived data must be met. The standard procedures for this are described in the document “BankID - Internal Security Procedures".

For Eika: See section 5.5.1 – Types of records archived.

For SpareBank 1: Live backups are stored on both data centres.

5.5.5 Requirements for time-stamping of records

Not applicable

5.5.6 Archive collection system (internal or external)

BankID COI

The records archival system is internal.

Issuer specific

For Eika: See section 5.5.3 – Protection of Archive.

For SpareBank 1: The records archival system is internal.

5.5.7 Procedures to obtain and verify archive information

Issuer specific

For Bankenes ID-tjeneste: See 5.4.5.

For SpareBank 1: TSP adheres to Norwegian laws regarding confidential information in the Money Laundering Act and the Personal Data Act.

All necessary information registered in the RA system are stored centrally and is independent of any RA going out of business. All information will be kept according to requirements for storage time. Information is secured with access control.

5.6 Key changeover

New Root CA keys must be generated, and a new Root CA certificate must be issued well before the old Root CA certificate expires. The old and new Root CA certificate must coexist in an overlapping period that lasts at least the duration of a Level 1 CA certificate.

New Level 1 keys shall be generated, and a new Level 1 certificate shall be issued well before the old Level 1 certificate expires. The old and new Level 1 certificate must coexist in an overlapping period that lasts at least the duration of the validity period of the end user certificate that has been issued with the longest validity period. More information about key changeover for a Level 1 CA is available in the CP/CPS for BankID Root CA [16].

Bits AS and the BankID COI Operator keep a track record of all key validities and organise key generation of Root CA keys and Level 1 CA keys well before expiration.

Root CA keys are generated and certified on the Root CA by representatives from Bits AS on behalf of Finance Norway.

Level 1 CA keys are generated on the Level-1 CA by representatives from the TSP, and certified on the Root CA by representatives from Bits AS on behalf of Finance Norway.

The following validity periods are defined for BankID:

- Root CA's keys are valid for 26 years. New keys are generated every 14th year.
- Level-1 keys are valid for 12 years. New keys are generated every 8th year.
- Keys for Mobile Personal BankID are valid for a maximum of 2 years and must be renewed every 2 years.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Several layers of security and monitoring of security measures combined with procedures is in place to reduce the impact and damage from security incidents and malfunctions.

TSPs, banks acting as RA and the service providers are obliged to notify each other of any security incidents related to issuing and use of BankID. Bits AS and Vipps AS shall provide guidelines for incident handling and distribution of warnings. Shared information shall not identify individual customers except when it is shared to limit or prevent misuse of BankID or financial losses for the individual customer.

There are four types of incidents described here:

1. Certification Authority (TSP) key compromise
2. Registration Authority key compromise
3. Other security breaches
4. Disruption of service (loss of availability)

Key compromise of the Root CA is a highly unlikely event, but with very severe consequences. It is described in the Root CA's CP and CPS [16], section 4.8.3.

If the private key of a CA has been compromised, the BankID COI Operator shall follow the following procedure:

1. BankID certificates from the relevant CA system shall be rendered unusable. There are a number of ways to technically achieve this. The certificate validation service will immediately be notified that this CA is no longer valid. All certificates signed with the CA system's private key will thereafter be declined by the certificate validation service. Root CA will also revoke the issuer's certificate
2. The TSP affected by the key compromise shall immediately inform all registration authorities, subjects and other issuers of the incident. The TSP shall inform competent authorities according to Norwegian law.
3. Key changeover for the CA system shall take place in accordance with the CP/CPS for Root CA [16]
4. The registration authority must flag all Personal BankIDs and Employee BankIDs issued under the compromised key for renewal. These can no longer be used in the normal way
5. The issuer produces new certificates in the certification authority system for all its end users who must follow the established routines for renewal. This means that the central storage entity generates keys and that these are certified with the issuer's new key.

If one layer of protection keys in the central storage entity is compromised, a new key must be generated. The new key shall be used to re-encrypt the impacted parts of the database. A compromised key will not have direct consequences for end users' private keys.

If the private key of a registration authority has been compromised, the procedure below shall be activated:

1. The compromised key must no longer be used. The RA must stop operations until new keys are generated and ready to use
2. RA must investigate to determine the earliest possible time of the RA private key compromise. All certificates issued after that time shall be invalidated
3. A fallback procedure for handling revocation and suspension of end user certificates (not invalidated in step 2), must be established
4. RA or TSP must inform all relevant parties: Subjects, other issuers and competent authorities
5. Generation of new RA keys
6. Resume operations and produce new certificates for subjects who got their previous certificates invalidated or revoked.

The TSPS and Bits will annually confirm that the key sizes and algorithms used are still adequate. If the used cryptography is no longer ensuring the binding between subject and public key, an emergency procedure will be initiated. If another security breach occurs, the entity discovering the breach is responsible to inform TSPs, scheme owners and relevant competent authorities, according to Norwegian law and plan. Where the breach of security or loss of integrity is likely to adversely affect the subject to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay. The breach will be communicated through the TSP´s standard communication channel to the subject.

If the service of critical parts in the infrastructure is disrupted for a significant time:

1. The COI operator shall inform TSPs, scheme owners and competent authorities, according to Norwegian laws and to the "BankID Disaster and Recovery plan".
2. Every available measure shall be initiated to resume operations, at one or two sites.
3. TSPs and associated RAs shall make information available to their customers.

BankID operations are continually divided between two separate physical locations. If one location is forced to halt operations, e.g. as a result of a natural disaster, BankID operations will continue in the other location. This means the solution is very robust in the face of a number of different disaster situations. Tests must be done on a regular basis to verify that it is possible to run operations from one location. The systems are configured to be able to handle operations from one location for several days, provided traffic loads are normal.

This is covered in the disaster/recovery plan, "BankID Disaster and Recovery plan".

The operator of the CA and central storage entity has deployed ITIL procedures for incident handling, and has on-call personnel to handle issues within 30 minutes.

As a result of monitoring the given system, components and logs the TSP has implemented procedures to handle with any discovered vulnerability in 48h or to create the plan to mitigate the vulnerability or to document the reason why not requiring remediation.

If the encryption technique for all keys are compromised, disaster and recovery procedures shall be followed, including TSP or mass revocation process.

Issuer specific
For Bankenes ID-tjeneste: The TSP has Key Compromise Procedures ensuring coordination with RAs and central authorities.

For DNB: The TSP guidelines for crisis management and incident management applies.

For SpareBank 1: TSP has a high-level crisis management plan for handling all crisis that can arise within the TSP. The plan details escalation, decision making structure and communication with service providers, authorities, third parties and the public in connection with different types of crisis and catastrophic situations.

In case of physical catastrophes, TSP have agreements for catastrophe readiness with service providers and have plans for re-establishing the systems that are operated by TSP.

5.7.2 Computing resources, software, and/or data are corrupted

BankID COI
All essential software and information are kept and backed up in a version control system. Any system failures will be restored from this repository. All changes in the production environment are first committed to the version control system before deployed in production.

In the event of a logical disaster, it is possible to roll the system back to the last successful transaction, correct any mistakes and then continue operating the system.

Issuer specific
For Bankenes ID-tjeneste: The RAs are aware of procedures for notification of events and consequences and relevant actions to be considered, and have recovery plans covering

- Responsibilities for decisions, and implementations of, mass revocation
- Information and communication to subjects and customers
- Responsibilities for IT and/or BankID Security in general

For Eika: All systems data necessary to resume CA and RA operation are backed up and stored safely.

Only qualified personnel at Eika Gruppen and IT Operations service providers are allowed to perform backup and restore functions.

The production environment for Eika Gruppen's BankID solution is dualized, so that the backup systems will ensure continued operation in cases of disruption.

Eika has continuity and disaster recovery plans as part of their banking operations, with a view to maintaining all production systems in a discontinuance situation.

For Nordea: Nordea has Business Continuity Plan in place, where contact details and escalation procedures described in details, including internal Crisis Response Team (CRT) and external notifications to customers, partners, BankID, Bits AS, Finance Norway, Nordic Financial CERT and other relevant instances.

For SpareBank 1: Routines are in place to restore from backup in case of disaster. In case of compromise, restore is done from trusted backup from before compromise.

5.7.3 Entity private key compromise procedures
If there is a breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein, the TSP will notify that appropriate parties in line with the applicable regulatory rules. The National Communications Authority (Nkom) and Norwegian Data Protection Authority if an incident affects personal data of the subjects within 24

hours the incident occurs. If a customer credential is compromised, revocation procedures shall be followed.

A mobile network operator must have a written procedure including warning routines and other measures that must be followed up with security officers in the BankID partnership, subjects and relying parties in case of a potential disaster such as if critical components of the Security Channel or a large number of SIM cards are found to be compromised. In such cases, the bank and mobile network operator shall ensure that it is impossible to use compromised certificates. This can be done by closing the Security Channel to the relevant certificates or by ensuring that certificate validation services always deny these.

5.7.4 Business continuity capabilities after a disaster

Vipps AS has a continuity and crisis plan known to all parties in the value chain. This plan covers the crisis management, participants, roles and responsibilities, action and communication plan. The crisis management team´s responsibility is to cover extraordinary incidents and crisis. Represented in the crisis team are all TSPs, Finance Norway, Bits AS and representatives from Mobile Network Operators.

Annually exercises for crisis and disaster is conducted in order to prepare the management and organisation for extraordinary incidents, crisis and disaster. Every such exercise or extraordinary incidents are handled according to the Business continuity and disaster recovery plan.

After every exercise or extraordinary incidents there is written a post mortem report to be used for improving the parts or issues that was identified to be causing the incident or crisis. Every improvement task is given a due date and a responsible person to follow-up and implement the change (improvement). This post-mortem report are important to continually improve the ability to handle such an incident, capacity issues, technical, communication or organisational challenges.

Annual disaster recovery tests are conducted on the technical infrastructure to verify that disaster recovery plan, procedures and backup is working like it is supposed to.

For BankID COI

The subjects' private keys are protected by multiple layers of encryption, including an individual encryption key.

For RA systems

For RA systems: All RAs have routines in place to restore from backup in case of disaster. In case of compromise, restore is done from trusted backup from before compromise.

5.8 CA or RA termination

In this context, Certificate Issuer Termination refers to a situation where all logical functions related to issuance of BankIDs are permanently terminated. A Key Changeover is not a termination.

The terms below apply when the issuer of BankID ceases operation in a controlled manner and has time to notify contacts of what is about to happen. The terms do not apply in emergency situations.

Before an issuer of BankID terminates their services, it shall:

- Inform the owner of the parent CA (BankID Root CA) about the planned termination at least 6 months in advance
- Inform the bank's customers (subjects, relying parties, subscribers) and other issuers of BankID at least 6 months in advance
- Publish information of the planned termination at least 3 months in advance

- Ensure that all relevant databases, archives and documents are kept in accordance with this document, for the defined retention period see section 5.4.3.
- Ensure that revocation status of the issued certificates is available on the Certificate validation service until the CA shuts down.
- Ensure the TSP's public key or its trust service tokens to relying parties are available for a reasonable period.

A TSP must also ensure that RA-banks that use its services receive the necessary information to move to another TSP.

The banking industry has prepared procedures that shall be followed if a participating bank or registration authority goes into administration, including transfer of the TSP obligations to other parties, see BankID Rules article 17. Bits AS may invalidate the TSP's CA certificate, thereby invalidating all subscriber certificates issued by the TSP. If the TSP enters into administration, bankruptcy or is subject to other insolvency proceedings, Bits AS may, at the request of the Norwegian Bank's Guarantee Fund, decide to postpone invalidating BankIDs issued by the relevant participant to natural persons, for up to three months. The Norwegian Banks' Guarantee Fund must then assume the participant's obligations and duties as issuer, including the liability arising from the Electronic Signatures Act and BankID Rules.

If a bank acting as RA wishes to terminate its relationship with a TSP and intends to start issuing certificates via another TSP, the old certificates remain valid until they reach their expiration date unless they are revoked.

The relationship between the bank acting as RA and the TSP can therefore not be terminated until all certificates have expired or been revoked. The parties' responsibilities under the agreement do not change during this period.

The operator of the CA and central storage entity has established operational procedures for termination of CAs, called "Termination of CAs".

The operator of the CA and central storage entity has operational procedures for offline backup of Level 1 CA. These procedures cover the BankID COI Operator' part of the termination procedures.

Issuer specific

For Bankenes ID-tjeneste: Procedures and agreements between Bankenes ID-tjeneste and RA Ensures this. The RAs have issued a guarantee of indemnity for financial responsibilities in these situations. Data and logs will be archived according to requirements in BankID Rules, and will be available for banks if they convert to other Issuers and Service Providers.

Bankenes ID-tjeneste as Joint Issuer will not be terminated as long as there are banks with active certificates issue by Bankenes ID-tjeneste. See also Termination Plan.

For DNB and SpareBank 1: TSP Termination Plan will be used in the event of an RA or CA termination

For Eika: Eika Gruppen has an up-to-date termination plan that applies when Eika Gruppen as issuer of BankID ceases operation in a controlled manner and has time to notify contacts about what is about to happen. The plan does not apply in emergency situations.

Eika does not outsource any functions relating to the process of issuing trust service tokens, so no notification regarding this is necessary.

Eika Gruppen will also ensure that banks that use its services receive the necessary information to move to another issuer of BankID in case of a controlled change of issuer

For Nordea: The service provider shall back up all data and enable storage for at least 10 years in an archive that is readable in accordance with the requirements in section 4.6.

6 Technical security controls

6.1 Key pair generation and installation

All certification authority systems use FIPS 140 [2] level 3/4 evaluated HSM for all cryptographic functions.

All central infrastructure and central storage entity components that handle BankID private keys also use HSM.

6.1.1 Key pair generation

CA key pair generation

Root CA

Root CA Key Ceremony is conducted by at least a System Administrator for the Common Operational Infrastructure (COI) issuing the commands, a Key Custodian from Finance Norway (Bits AS personnel is appointed by Finance Norway to this role) and a person in Trusted Role from the COI Operator acting as Key Custodian and Supervisor and an external auditor.

The Root CA credentials is split between COI Operator and Bits AS personnel, so that none of the parties may start the Root CA or reproduce the Root CA HSM without the other party. The Root CA HSM is switched off when not in use.

The BankID COI Operator is responsible for testing and documenting the Root CA Key Ceremony. The Root CA Key Ceremony document details all commands conducted during the Key Ceremony and is approved by the Security Officer before the Key Ceremony.

All 4 participants of the Root CA Key Ceremony signs 3 copies of the Root CA Key Ceremony document and confirms that the procedure is followed and that the integrity and confidentiality of the Root CA keys is ensured. The System Administrator, Key Custodian for Finance Norway and the Security Officer safekeeps one copy each of the signed evidence.

Level 1 CA

Level 1 CA Key Ceremony is conducted by at least a System Administrator for the Common Operational Infrastructure (COI) issuing the commands, a Key Custodian from the Issuer and a Security Officer from Vipps AS acting as Key Custodian and Supervisor.

The Level 1 CA credentials is split between and a person in Trusted Role from the COI Operator and the Issuers Key Custodian, so that none of the parties may reproduce the Level 1 CA HSM without the other party. The Level 1 CA HSM is placed in an online state, ready for issuing Subject certificates.

The BankID COI Operator is responsible for testing and documenting the Level 1 CA Key Ceremony. The Level 1 CA Key Ceremony document details all commands conducted during the Key Ceremony and is approved by the Security Officer before the Key Ceremony.

All 3 participants of the Level 1 CA Key Ceremony signs 3 copies of the Level 1 CA Key Ceremony document and confirms that the procedure is followed and that the integrity and confidentiality of the Level 1 CA keys is ensured. The System Administrator, Key Custodian for Issuer and the Security Officer safekeeps one copy each of the signed evidence.

When the Level 1 CA keys are created, the System Administrator for COI, the Key Custodian for Finance Norway (Bits AS) and the Security Officer will certify the Level 1 CA on the Root CA according

to stringent procedures for starting, issuing and stopping the Root CA. The Key Custodian from the Issuer will confirm that the Level 1 CA certificate information elements is correct under this process.

A new CA certificate for signing subject keys will be made in time for all entities who rely on the certificate to update their certificate before the old expires. The general rule for updating the CA certificates is before the longest living certificates issued by the CA which is 4 years.

End-user key pair generation

Key Pairs are generated in a secure environment on the end user's SIM card in accordance with recognised principles for generating RSA keys. The end-user must have given their approval before the key generation can commence.

RA key par generation

The RA key pair used to encrypt the communication between the bank RA servers and the BankID COI Operator is generated by the CA and exported as a file.

The RA key pair used to sign the RA messages at the bank RA servers is generated in a HSM at the RA service provider. The public signing key is certified at the TSP CA by representatives from the TSP and Bits AS acting on behalf of Finance Norway.

Issuer specific

For Bankenes ID-tjeneste: The RAs keys for secure communication with COI are generated by Bankenes ID-tjeneste's Level 1 CA in a Key ceremony. The keys are securely transported to the RA Application Provider and installed in the RAs RA-Application.

Key Ceremony for the RA keys are performed with a representative from the RA, or somebody acting on part of the RA under written authority. The process is logged and archived, and keys installed in HSMs and safely stored.

For Eika: The key pairs are delivered to Eika Gruppen's Key Custodian in connection with the completed key ceremony.

In connection with Eika Gruppen's CA in BankID COI, RA issuances have been made to make BankID COI and Eika's CA accessible to the individual banks affiliated with Eika's BankID solution. This entails that one or more Registration Authority (RA) has been established under the group's CA on these occasions. In connection with this, security elements associated with RA have been issued. These security elements were delivered to Eika Gruppen's key custodian, so accordingly Eika has in its possession various security elements associated with RA. They too are stored under secure conditions with access limited to key custodians.

For Nordea: The registration authority's key pair is issued on the certification authority system on which the registry shall issue certificates and distributed to the registration authority in a secure manner. Nordea has internally procedures and routines for handling the RA password, how it is stored and how to access the encrypted secret. A key custodian is designated to distribute and load keys or key splits into a cryptographic module.

For SpareBank 1: The RA key pair is generated on HSM.

6.1.2 Private key delivery to subscriber

There is no delivery of the private key for the Mobile BankID, since the keys are generated and stored on the end-users SIM.

6.1.3 Public key delivery to certificate issuer

The public key is received encrypted from the mobile network operator via a closed data network. See the mobile network operators own security documentation for more information on how the public key is protected in the mobile network.

Within the BankID central storage entity, the end user's public key is protected in the same way as other production data within the secure zone. In practical terms, this involves both integrity protection and encrypted connections between different components.

6.1.4 CA public key delivery to relying parties

The public key for a BankID certificate issuer will be found in a certificate issued by the BankID Root CA (ref section 1.3.1). The main rule is that BankID certificate issuers are responsible for making a valid Level 1 CA certificate available, so that this certificate can be used by authorised certificate validation services.

All BankID transactions, whether authentication or signing will result in a data structure containing the end-user certificate and the CA-certificate. All Relying parties are provided access to the Root CA certificate as part of the installation of the BankID software. The Certification chain is always validated for every transaction.

The Root CA certificate and public keys for BankID certificate issuers will be distributed to parties which need access to them. It is not considered necessary to distribute these keys to all relying parties, because a relying party will always communicate with an authorised certificate validation service to verify the validity of a certificate. Relying parties will hence only need to have the public key for the certificate validation service. The certificate validation service will in turn be responsible for current and correct access to all certificate issuers' public keys.

Delivery of new CA certificates replacing expiring CA certificates is handled in the same way as initial CA certificate above.

6.1.5 Key sizes

The key size for Root CA and Level 1 CA is at least 4096 bits for RSA.

The key size for the Registration Authority is at least 2048 bits for RSA.

The key size for Personal Mobile BankID is at least 2048 bits for RSA.

6.1.6 Public key parameters generation and quality checking

Bits AS has to approve SIM cards that are going to be used as key stores for personal BankID certificates. The mobile network operator must document that the private key has satisfactory protection against compromise and misuse to obtain such approval. Central components on the SIM card must be certified by a recognised authority. Bits AS can clarify documentation requirements.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Mobile BankID has one key pair which is used for authentication and signing. The solution is designed in such a way that it explicitly indicates to the user whether the private key is used for authentication or signing. The BankID COI Operator produces certificates for Mobile BankID for authentication and signing.

Key Usage for the private key is NonRepudiation(1)/DigitalSignature(0).

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

For CA-systems

TSP private keys are stored in a FIPS 140, level 3/4 [2] certified HSM, and it is not possible to export these from the HSM as plain text. To export a backup of a CA's private key the requirement is that the key must be encrypted and divided into parts that are distributed between two or more physical components.

Appropriate security controls are in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle. In internal security procedures documentation for security control are described.

The HSMs are packed and sealed by the manufacturer and System Administrators in COI will follow a written unboxing routine for checking the seal and serial number.

Transportation of HSMs follows routines for Transportation of equipment, controlled and accompanied by 2 System Administrators.

Uninstalled HSMs are stored in the same protected area as the Production HSMs.

CA Signing keys are only used for issuing certificates, signing revocation requests and issuing CRLs.

For end users as subjects

A subject's private keys are stored on a SIM card controlled by the subject. The keys are physically and logically protected by the access mechanisms of the SIM card. The keys are protected by an ID-PIN, and the subject is required to enter the correct ID-PIN before the keys can be used. The keys will be permanently invalidated if the ID-PIN verification fails three times in a row.

Issuer specific

For Eika: Eika Gruppen uses commonly accepted cryptographic techniques and algorithms for protecting any keys and similar devices. Furthermore, Eika Gruppen stores certain elements protected inside a Hardware Security Module (HSM).

For SpareBank 1: RA HSMs are certified in accordance with FIPS 140 level 3 / 4.

6.2.2 Private key (n out of m) multi-person control

For CA-systems

Any access to the system that holds the issuer's private keys requires the involvement of at least two individuals. This means that no single person will have all the information required to access the environment where the private key is stored.

The issuer’s service provider is in full control of all the HSM devices during all phases of the HSM device’s "life cycle", and has procedures in place to safeguard the integrity of the device from transportation and storage through initiation and use to controlled removal or destruction of secret keys when the device is decommissioned.

A subject's private key shall only be available for use by the subject. No-one employed by the central storage facility or issuers of BankID have access to either use or read the subject's keys in plain text. The subject's keys is protected by firewalls and other network security (against external attacks) and with several levels of cryptography (against external and internal attacks.)

For RA-systems

Registration Authorities operation is with single-person control.

Issuer specific

For Bankenes ID-tjeneste: Secure elements in Bankenes ID-tjeneste's possession are stored under secure conditions with access controlled by Key Custodian.

For Eika: During initial and subsequent key ceremonies for Eika Gruppen's CA in BankID COI, various security elements associated with CA and RA functions, have been issued. Security elements in Eika's possession are stored under secure conditions with access limited to key custodians.

For end users as subjects

Natural persons who are subjects, operation is with single-person control.

6.2.3 Private key escrow

There is no private key escrow in BankID.

6.2.4 Private key backup

For CA-systems

A backup of private keys must be done for Level-1-CAs. All Certification Authority Systems must be recoverable in case of operational issues. This includes the recovery of secret key values in HSM. Key material shall never be exported in plain text, but under a key encryption key (KEK).

Backups of key material shall be divided into at least two components. Neither component shall contain enough information about the key material to be used on its own. The different components shall be distributed to trusted individuals in different organisations. Both organisations have to be present to assemble the data.

KEK must be split into two parts as well, and each key custodian is responsible for one of the parts.

For end users as subjects

There is no backup of the Mobile BankID keys, since the keys are generated and stored on the end user's SIM.

For RA-systems

Issuer specific

For Bankenes ID-tjeneste: RA Private keys are stored in HSMs at dispersed locations.

For DNB: The separate standard procedure for dealing with security copies of private keys is set out in an internal document describing the rules for managing BankID keys.

For Eika: See section 6.1.1 - Key pair generation.

For SpareBank 1: RA Private keys are backed up as cryptograms. The KEK is split and 2 of 3 types of personnel is required.

6.2.5 Private key archival

There is no archives of the Mobile BankID keys, since the keys are generated and stored in the end-users SIM.

6.2.6 Private key transfer into or from a cryptographic module

Not applicable for this TSPS.

6.2.7 Private key storage on cryptographic module

For CA systems
TSP private keys on the Certification Authority System are generated within a cryptographic module (HSM). If it becomes necessary to restore this, it will arrive as a cryptogram, encrypted using a KEK.

For end users as subjects
The subject's private keys are generated and used within a secure environment on the subject's SIM card. The private key never leaves the secure environment.

For RA systems
See section 6.2.1 – Cryptographic module standards and controls.

6.2.8 Method of activating private key

The CA private key
The TSP private key is protected against disclosure and unauthorised use. This key can only be accessed by algorithmic features within the HSM. Only personnel from the issuer can activate the private key.

The subject private key
The subject's private is protected by an IDPIN. The subject must enter the correct IDPIN in order to use the private key. It is not possible to perform operations with the private key without entering the correct IDPIN.

The subject is obliged to protect the IDPIN and ensure that it is never disclosed to anyone else.

6.2.9 Method of deactivating private key
Private keys are temporarily deactivated when they are not in use, and until the correct activation data has been entered.

6.2.10 Method of destroying private key
When the TSP private key is no longer valid, it must be securely removed from the HSM. All parts of backups of the key must also be destroyed. This is the responsibility of the key custodian.

The subject has to request a revocation in order to deactivate the keys permanently. A key that has been revoked, suspended or expired cannot be used.

The mobile network operator must describe how to invalidate or delete keys on the SIM. This is described in more detail in the mobile network operators' own security documentation.

6.2.11 Cryptographic Module Rating
Not applicable for this TSPS.

6.3 Other aspects of key pair management

6.3.1 Public key archival
All public keys are archived by the issuer for a minimum of 10 years.

Archived public key information for end users are protected in the same way as public key production data on the central storage entity.

Public keys are archived for subsequent verification of signatures.

6.3.2 Certificate operational periods and key pair usage periods
A Level 1 CA key pair has a life span of 12 years.

A key pair for a Mobile Personal BankID has a maximum life span of two years.

The certificate of corresponding public keys shall be valid for the same period of time.

6.4 Activation data

6.4.1 Activation data generation and installation

The user selects an ID-PIN at the time of the key generation to protect his or her private keys. This is entered via the SIM toolkit client on the phone. IDPINs shall contain between 4 and 8 digits. The mobile network operator must describe how this is controlled in the mobile network operator's own security documentation.

6.4.2 Activation data protection

This is described in the mobile network operator security documentation.

6.4.3 Other aspects of activation data

Not applicable

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All unnecessary features are deactivated on the Certification Authority System and RA's systems. The latter includes both the bank's RA system and service provider devices that communicate with these for the purpose of issuing BankIDs.

There is authentication, access control and traceability down to the individual level across all operations and transactions that affect the use of the Level 1 CA's private key. Distinction must be made between the roles defined in section 5.2.1.

The CA system login requires a username and password, and the password must consist of at least 8 characters. Every person who logs on to the system has his/her own account.

Central storage devices are hardened by turning off unnecessary functionality, at the same level as the certificate issuing devices.

The central storage entity function that handles secret keys is protected by the same type of access control, confidentiality and integrity as the certification authority systems. This also applies to the certificate validation service.

The devices that run certificate validation checks are behind several layers of firewalls and are subject to access control that requires two persons in different roles to be present to perform sensitive operations.

All production data related to certificate issuance or operation of central storage entities are stored on storage entities that are protected against errors or loss of data.

All access to the systems is handled through the access control system, as well as routines for access to secured rooms. Only certified personnel have access to the data inside the security rooms. Employees are only granted for access to information on a job related "need to know basis".

There is continuous monitoring and alarm systems to detect, register and react in a timely manner upon any unauthorised or irregular attempts to access resources.

Certificate Status Service

The BankID Certificate status service is protected by the OCSP-protocol as described in section 6.7. The database in which the certificate status information is stored, is kept in secure premises with dual access control and only available for the Certificate status service as Read-only. To physically access the database, 2 persons in Trusted roles must be present.

CRLs which is used for later proof of validity is protected the same way.

Anti-malware protection

Anti-virus/malware system are installed to protect the integrity of TSP systems and information against viruses, malicious and unauthorised software.

Dissemination service

The Mobile BankID users have their keys on SIM and the certificates stored in a central database with dual access control. The end-user may view it's own certificates through the BankID client, which have read-only access to the certificate database.

Issuer specific

For Bankenes ID-tjeneste: Bankenes ID-tjeneste and RA Application Providers have procedures for the safe management and storage of CA and RA Keys.

All data related to BankID registration and issuance is protected through commonly accepted technical and procedural security measures.

For Eika: Eika Gruppen protects all data information related to BankID registration and issuance. This is achieved through commonly accepted technical security measures combined with thorough operational routines.

For SpareBank 1: Unnecessary features are deactivated on the RA's systems.

There is authentication, access control and traceability down to the individual level.

The RA system login requires a username and password, and the password has complexity requirements. Every person who logs on to the system has his/her own account.

The RA servers are behind several layers of firewalls and the HSMs are subject to access control that requires two persons in different roles to be present to perform sensitive operations.

All production data related to certificate issuance are stored on storage entities that are protected against errors or loss of data.

6.5.2 Computer security rating

For the CA-system and central storage entity

The BankID COI Operator Security Framework contains security requirements to be followed during the design and requirement specification stage, to ensure that the security is built into the system.

For RA-systems

Issuer specific

For Eika: Eika Gruppen protects all data information related to BankID registration and issuance. This is achieved through commonly accepted technical security measures combined with thorough operational routines.

For SpareBank 1: No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

For the CA-system and the central storage entity

Software development for CA-Systems and the central storage entity is performed in a controlled environment that, together with at least one of the underlying conditions, may protect against software or version control errors:

a) The software vendor must work within a quality system that complies with international standards, or
b) The software vendor shall have a quality system available for inspection on request.

Software used for issuing BankID must be verified to ensure it is genuine and as it was provided by the supplier.

The requirements listed above shall also apply to critical components of the Security Channel.

The BankID COI Operator is certified in accordance with the ISO 27001 Standard [6] and all system development is performed in accordance with this standard. All third-party software has a security evaluation in accordance with the corresponding standard [International Standards]

The operator of the CA and central storage entity has deployed a quality system that comply with relevant ISO 9000 standards.

The BankID COI Operator has established procedures for release and change handling according to ITIL principles. All processes are documented by written reports during test and documented in the ITIL tool for all changes. All changes are documented before application.

The operator shall monitor capacity demands and project future capacity requirements to ensure adequate processing power and storage are available.

For the RA-system

Software development for Registration Authorities is performed in a controlled environment that, together with at least one of the underlying conditions, protects against software or version control errors:

a) The software vendor must work within a quality system that complies with international standards, or
b) The software vendor shall have a quality system available for inspection on request.

Issuer specific

For Bankenes ID-tjeneste: Service Providers are declared at Bits AS according to Bits ASs regulations and has documented quality systems to ensure release and change handling according to recognized principles and practices.

For Eika: Eika has a Change Management process applying to all changes in all software in the company group. This outlines the change process in a given number of different processes, and also defines various roles with responsibility for the various processes.

Eika Gruppen uses common accepted security techniques when developing systems.

6.6.2 Security management controls

The BankID COI Operator has implemented a security framework for policy and procedures.

The BankID COI Operator has policy and procedures for applying security patches within a reasonable time after they come available, security patches are not applied if they introduce additional

vulnerabilities or instabilities that outweigh the benefits of applying them, and the reasons for not applying any security patches are documented.

Issuer specific
For SpareBank 1: TSP Security management is done according to requirements, routines and procedures set forth in the Information Security Management System.

6.6.3 Life cycle security controls
No stipulation.

Issuer specific
For SpareBank 1: The TSP is in full control of all HSM devices during all phases of the HSM's "life cycle", and makes sure that the integrity of the device is safeguarded throughout, from transportation and storage through initiation and use to controlled removal or destruction of secret keys when the device is decommissioned.

6.7 Network security controls
The infrastructure for the CA system and central storage, is segmented into networks or zones based on security classification considering functional, logical, and physical (including location) relationship between trustworthy systems and services. The same security controls applies to all systems co-located in the same zone.

There are separated zones for development, test, pre-production and production systems, in addition there is a dedicated network for administration of IT systems. Dedicated systems are used for administration of the security policy implementation and not used for other purposes.

There is established trusted secure communication channels within the central infrastructure and between the central infrastructure and the distributed RAs, these channels are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure. The external network connections is redundant to ensure availability of the services in case of a single failure.

This TSPS covers network security for the outer firewalls at the BankID COI Operator.

Mobile network operators shall disclose how network security is handled in their systems including interfaces with BankID COI Operator, in their own security documentation.

The local network components are located in the security rooms. Configuration compliance on new platform are performed regularly. Configuration of network components are audited on a regular basis.

The Root CA is not connected to the network, and turned off. The Root CA is only started when needed.

The certification authority systems are protected by multiple layers of firewall and cannot be accessed directly from open networks. All firewalls are configured to deny all traffic, and then only opened for necessary communication.

The certification authority systems shall also be configured to provide the minimum functionality required for the issuing service. All communication ports that are not clearly required shall be disconnected and software processes using these ports shall be turned off.

The certificate validation service is protected by multiple layers of firewalls that only allow OCSP requests with valid formatting and signature.

The BankID COI Operator and the mobile network operator are connected via closed network and all communication is also encrypted with SSL. Communication within the BankID COI Operator's network is secured in the same way as other production data within the security zone with a combination of integrity protection and encrypted connections between different components.

The security measures between the SIM card and the mobile network operator's systems are described by the mobile network operator in its own security documentation.

The central storage entity is not directly accessible from any open networks. There are dedicated VLANs within the security room, separating the services.

Data from RA to the Certification Authority System are transferred via a closed network where only known machines have access.

The BankID PreProduction system allows third parties to test and verify the different BankID certificates.
BankID Support provides the necessary certificates for testing purposes.

The PreProduction system issues certificates from a CA clearly named Test in the Common Name.

For the TSP RA systems

Issuer specific
For Bankenes ID-tjeneste: Networks between bank and Service Providers are secure and network security is audited.

For DNB: The RA-systems are protected by multiple layers of firewalls and cannot be accessed directly from open networks. All firewalls are configured to deny all traffic, and then only opened for necessary communication. The network between the BankID COI Operator and the TSP are a closed, none public, network.

For Eika: Eika Gruppen and our suppliers and service providers have a variety of protective measures.

The host computers used in Eika Gruppen's BankID solution are not directly accessible through open networks. The BankID solution and the communication between CA and RA are protected.

Eika Gruppen and its service providers have procedures for applying security patches when they come available.

For SpareBank 1: RA system is placed in a network zone separated from other internal networks, guarded by firewall with stateful packet inspection. Only defined personnel have access to the separated network zone. All network communication is encrypted.

6.8 Time-stamping
All servers are set to automatically sync clocks several times an hour using NTP service. In, addition there are daily scheduled tasks to verify the connection with the NTP server. These tasks are stored according to section 5.4.

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile
This section is by no means a specification, but an overall explanation of some of the fields included in certificates and revocation lists used in BankID policies.

BankID Root CA only issues certificates to individual Level 1 CA's in the BankID CA hierarchy. The Level 1 CA issues certificates for Merchants, OCSP and RA. The Level 1 CA also signs and issues CRL's for later proof of a certificates status at a given time.

Issued certificates and usage:

1. Root issues Level 1 CA certificate
2. Level 1 CA issues the following certificate
    1. OCSP certificates
       Used for Certificate validation services. The OCSP certificate signs the OCSP requests related to the specific Level 1 CA only. The Certificate validation service connects to the Level 1 CA database and verifies the certificate status directly.
    2. RA certificates (consist of 2 different types)
       RA SSL certificate - enables the Issuers RA to connect to the COI and perform certificate ordering and revocation services.
       RA XML Signing certificates - used by the RA to sign all orders and revocation messages in an XML format sent to the COI, to safeguard the RA system and provide traceability through the RA process.
    3. Mobile BankID certificates is used for electronic ID (authentication) and signing electronic documents in merchant sites.

BankID subject certificate profiles are based on and comply with ETSI EN 319 412-3 certificate profiles, see document "BankID certificate profiles" [13].

7.1.1 Version number(s)
The version number is 2, indicating that the format X.509, version 3 [21] is being used.

7.1.2 Certificate extensions
The QC statement is included in the certificates issued according to this TSPS.

7.1.3 Algorithm object identifiers
The algorithm identifier is sha256RSA (identifies algorithms used to sign the certificate content)

7.1.4 Name forms
This is described in section 3.1.

7.1.5 Name constraints
This is described in section 3.1.

7.1.6 Certificate policy object identifier
The object identifier is included in the certificatePolicies field of the certificate.

Mobile BankIDs shall use the following identifier:

{joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) bankenes-standardiseringskontor(16) policy(1) qualifiedCertificates(12) mobile(2) 1}

7.1.7 Usage of Policy Constraints extension
The Mobile BankID is issued to a natural person which must be a customer in a Norwegian Bank.

7.1.8 Policy qualifiers syntax and semantics
All mobile Personal BankID certificates contains the QC extension as defined in ETSI EN 319 412-5.

7.1.9 Processing semantics for the critical Certificate Policies extension
Not applicable

7.2 CRL profile

7.2.1 Version number(s)
Standard format X.509 and RFC 5280, version 2 integer 1 is used for the revocation lists [21].

The time of the next update is always be included in the revocation lists.

7.2.2 CRL and CRL entry extensions
According to RFC 5280.

Expired certificates are removed form the CRL.

CRLs shall not include the X.509 “ExpiredCertsOnCRL” extension.

7.3 OCSP profile
The OCSP profile is according to RFC 6960.

7.3.1 Version number(s)
The version number is version 1, with integer 0.

7.3.2 OCSP extensions
For Personal BankID and Employee BankID the extension defined by the Norwegian SEID-2 standard is used for delivery of 'fødselsnummer' (National Identity number) to Relying Parties.

https://www.nkom.no/teknisk/elektronisk-signatur/elektronisk-signatur/kva-er-seid-prosjektet/_attachment/1532?_ts=14110f4b878

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment
TSPs, banks acting as RA and their service providers, including the BankID COI Operator are subject to periodic compliance audits. Compliance audits shall are performed at least once every three years. In addition, compliance audits will be carried out when new TSPs commence operations or when there are major changes in the solutions of established TSPs. This will ensure that their operation complies with the TSPS.

Audits of the TSPs, banks acting as RA and their service providers to verify that they meet requirements other than those in the BankID TSPS (e.g. from Public Authorities) may come in addition to the above-mentioned compliance audit. The banks and their service providers will be audited and controlled by:

- The Financial Supervisory Authority of Norway or similar supervisory authority for foreign banks
- Potentially self-imposed external audit against quality standards in the ISO 9000 series
- Potential self-imposed external audit against standard for security and good practice
- The Norwegian Communications Authority (re. issuance of qualified certificates)
- Bits AS
- Internal audit and control functions

8.2 Identity/qualifications of assessor
Bits AS has the right to approve the auditor. The auditor should be selected in agreement with the issuer of BankID, the BankID COI Operator and Bits AS

8.3 Assessor's relationship to assessed entity
Compliance audits are performed by an independent auditor not employed by or associated with the TSP, bank acting as RA, or any of the service providers involved in operating BankID services on behalf of these entities.

8.4 Topics covered by assessment
The audit should determine whether the requirements and practices in the BankID TSPS and referred ETSI standards are met by the TSP practices, covering the TSP, bank acting as RA and any service provider involved in operating BankID Services on behalf of these entities. This TSPS is a mandatory underlying document. Further confidential security documentation may be submitted and taken into account during compliance audits.

8.5 Actions taken as a result of deficiency
Any discrepancy between regulations, rules defined in the policy and the written TSPS, and the way the bank acting as RA, TSP, BankID COI Operator or mobile network operator actually operate, shall be reported to the management team of the relevant party and Bits AS. The parties will jointly define corrective measures and set a deadline for implementation. Bits AS shall assess whether banks shall be informed immediately of matters relating to the joint issuer, BankID COI Operator or mobile network operator used by the bank.

The party that has been audited decides who can access the results of compliance audits. A final summary shall however not be classified, and shall be made available on request. This summary should contain information about any deviations of significance that could impact relying parties' trust in the certificates, but shall exclude details that can be used to attack the system.

In the event of a discrepancy between requirements laid down in the relevant certificate policy and practical implementation, the BankID COI Operator will take immediate action to correct the discrepancies.

8.6 Communication of results
The party that has been audited decides who can access the results of compliance audits. A final summary shall however not be classified, and shall be made available on request. This summary should contain information about any deviations of significance that could impact relying parties' trust in the certificates, but shall exclude details that can be used to attack the system.

9 Other business and legal matters

9.1 Fees

9.1.1 Certificate issuance or renewal fees
No applicable fees.

9.1.2 Certificate access fees
No applicable fees.

9.1.3 Revocation or status information access fees
No applicable fees.

9.1.4 Fees for other services
No applicable fees.

9.1.5 Refund policy
No applicable fees.

9.2 Financial responsibility

9.2.1 Insurance coverage
The TSP maintains sufficient financial resources and/or obtain appropriate indemnity declaration from participating banks, in accordance with national law, to cover liabilities arising from its operations and/or activities. See section 16 in BankID Rules for further information.

9.2.2 Other assets
Not applicable

9.2.3 Insurance or warranty coverage for end-entities
Provided that a Mobile Personal BankID is issued by a TSP according to this TSPS and BankID Rules [1], and that the end user has used the BankID according to the end user agreement, the TSP is liable for up to NOK 100,000 per transaction.

9.3 Confidentiality of business information
The issuer of BankID shall communicate its current rules and procedures for processing personal data. The TSP and bank acting as RA have a duty of confidentiality in accordance with the rules of the Norwegian Financial Business Act §9-6, unless otherwise directed by statutory disclosure obligations. Any service providers of the TSP and the bank acting as RA, is be subject to corresponding confidentiality requirements by agreement with the TSP. The Act on Electronic Trust Services [15] and the Personal Data Act [14] will also apply.

9.3.1 Scope of confidential information
The TSP, the bank acting as RA, and any service provider involved in the operation of BankID are amongst other things responsible for keeping the following types of information confidential:

- Data concerning subjects that cannot be found in the certificate or any publicly available directory service
- Issuer's and Registration Authority’s private keys
- One-time codes and other activation data, provided the information is held by the bank, issuer or mobile network operator
- Log data
- Documentation providing additional details of the operational procedures of the issuer and its service provider.

Other types of data in central storage entities to be kept confidential include information about activation and authentication data for subjects, transaction data and technical security in the infrastructure.

9.3.2 Information not within the scope of confidential information
The following types of information processed by BankID issuers are not considered confidential:

- Certificates
- Revocation status for a certificate
- TSPS documents for qualified certificates

Information about subjects (name, date-of-birth, etc.) that can be found on certificates, are not considered to be confidential.

It shall not be possible to avoid appearing on a revocation list, or to avoid that the certificate status of BankID is shared with authorised certificate validation services.

9.3.3 Responsibility to protect confidential information

The TSP, the bank acting as RA, and any service provider involved in the operation of BankID, including mobile network operators have a duty of confidentiality as stated in section 9.3.1. Disclosure of information may occur as a result of statutory disclosure obligations.

Disclosures over and above the imposed obligation to provide information or access requires permission from the subject.

9.4 Privacy of personal information

9.4.1 Privacy plan

Subjects information is managed by the RAs according to Norwegian Personal Data Act [14].

Issuer specific

For Bankenes ID-tjeneste: Subject information is managed by the RAs according to Norwegian laws and regulation, see 9.3.

For DNB: Subjects information is managed by the RAs according to Norwegian Personal Data Act [14].

The TSP guidelines for handling of personal data applies. The object of these guidelines is to describe the principles that apply to the handling of personal data in all companies in the TSP. The guidelines shall help ensure that the TSP always handles personal data in accordance with fundamental principles for privacy protection, The TSP's own internal requirements and special external and internal requirements that apply for individual companies in the Group. When handling personal data, the TSP shall place great emphasis on ensuring that rules are followed and that the privacy of individuals is thereby protected. The manner in which the TSP handles personal data should instill confidence both within and outside the TSP.

For SpareBank 1: Only necessary personal information is handled within the system. Access to the information is limited to personnel in need of it for error handling and normal operation. User actions are logged. Operation is done in accordance with the privacy act.

9.4.2 Information treated as private

The TSP, the bank acting as RA, and any service provider involved in the operation of BankID, including the mobile network operators are amongst other things responsible for keeping the following types of information private:

- Subject's or subscriber's data that cannot be found in the certificate or any publicly available directory service

9.4.3 Information not deemed private

Information elements found in the Mobile Personal BankID certificates are not deemed private.

9.4.4 Responsibility to protect private information

The TSP, the bank acting as RA, and any subcontractors involved in the operation of BankID are obliged to protect private information according to Act of 14 April 2000 No. 31 relating to the processing of personal data [14] and Act of 25 June 1999 on financial contracts and financial assignments [Financial Contracts Act] [28].

9.4.5 Notice and consent to use private information
The end user's consent to use private information is included in the standard agreement template [20] used between the bank acting as RA and the end user.

Certificates are not generally available for retrieval from the TSP and information in the BankID certificates is only available when the subject has actively used the certificate.

9.4.6 Disclosure pursuant to judicial or administrative process
Disclosure of private information by court order or prosecution attorney order with reference to ongoing investigation.

9.4.7 Other information disclosure circumstances
Not applicable.

9.5 Intellectual property rights
The subject has right of disposal over their certificate, including the right to request invalidation (revocation/suspension).

The BankID scheme owner owns the BankID software and documentation that is distributed in connection with the BankID service.

9.6 Representations and warranties

9.6.1 CA representations and warranties
The TSP shall:

- Issue, invalidate or renew certificates
- Perform all technical controls described in sections 4 to 6 in this document
- Create and maintain a database of certificates
- Create and periodically maintain information about revoked and invalidated certificates and make information about invalidated certificates available to Certificate Validation Services
- Protect their private keys as described in sections 4 to 6
- Produce event logs and system status information for archiving
- Comply with the provisions of the "BankID Rules" [1], relevant parts of the Root CA CP/CPS [16], this TSPS

The tasks listed above must be performed correctly by both the TSP and the bank acting as RA. In addition to the tasks above, TSP's representing independent banks acting as RA must:

- Be approved by Bits AS
- Fulfil the equity ratio requirement in the Act on Electronic Trust Services [15]
- Enter into agreements with the banks acting as RA

A TSP's private key for issuance of certificates shall only be used to sign certificates and CRLs.

9.6.2 RA representations and warranties
The bank acting as RA shall:

- Check and verify the identity of certificate applicants as described in section 3
- Guide and assist the personal customer during the registration process
- Compile and forward relevant certificate applicant information that is necessary to issue BankID to the issuer
- Ensure that a unique identifier is used or assigned to identify the subject

- Collect the mobile phone number of the applicant
- Have the opportunity to initiate invalidation of certificates
- Comply with the provisions of the "BankID Rules" [1], relevant parts of the Root CA CP/CPS [16], this certificate TSPS.

9.6.3 Subscriber representations and warranties

Key obligations for subjects shall also be documented in the agreement between the bank and the customer [20].

The Subject shall:

- Follow the procedures provided when applying for a certificate
- Provide correct and complete information when applying for a certificate
- Read and understand the terms and conditions for issuing and using BankID, and confirm acceptance of terms to the bank
- Only use keys and certificates in connection with the Security Channel and in accordance with the intended use
- Protect IDPIN and ensure it is kept secret
- Inform the bank of any matters of importance to the contractual relationship, including changes to information supplied at the time of issuance
- Report to the bank (or its service provider) if a private key is suspected to have become known to others
- Report to the bank or the mobile network operator if the key store is lost, stolen, destroyed or mislaid
- Report to the bank if IDPIN is suspected to have become known to others and follow the bank's instructions
- Immediately stop using a BankID if the private key or IDPIN is suspected to have become known to others.

9.6.4 Relying party representations and warranties

The relying party may be a bank, a legal person or a natural person.

The relying party shall:

- Check the certificate's validity and decline it if it is invalidated, expired or otherwise terminated
- Check for, and take into account any usage restrictions for the certificate arising from signed agreements or the certificate policy the certificate is issued under
- Only use the certificate and associated public key data for the purpose specified in the certificate (e.g. through the use of the certificatePolicies field)
- Act in accordance with the Bank's policy of tagging transactions so that the current Key Usage is clearly visible to the subject.

9.6.5 Representations and warranties of other participants

Service providers for issuing systems

A service provider may perform all or part of a TSP or bank acting as RA functions. The service provider must act in accordance with this document as well as written agreements between the parties.

The main point of contact for both subject and relying party shall always be the bank acting as RA with which they have entered into a contract.

Service provider for central storage and usage entity

Service providers for the central storage entity shall:

- Create and maintain event logs and archives in accordance with this TSPS
- Make logs and archives available on receipt of a valid and authorised request from a bank

Mobile network operators

The relationship between the mobile network operator and the bank is regulated by a separate agreement.

The Mobile network operator shall:

- Equip its subscribers with SIM cards that meet requirements for key storage for Mobile BankID as described in sections 4 and 6
- Inform the customer of specific terms related to the use of Mobile BankID
- Provide necessary components in the Security Channel in accordance with this certificate policy
- Ensure that private keys for Mobile BankID are only used as specified in this certificate policy
- Immediately notify the bank if the key store is lost, or if it can no longer be used for reasons such as subscription conditions
- Create and maintain event logs and archives in accordance with this TSPS
- Make logs and archives available on receipt of a valid and authorised request from a TSP or RA.

9.7 Disclaimers of warranties

This is described in the BankID Rules document.

9.8 Limitations of liability

TSP liability

The TSP liability in relation to the customer and vice versa, both for Personal BankID and Employee BankID, is governed by agreements, both when the customer is a subject and a relying party.

In the case of Employee BankID, the liability relationship between the TSP and the enterprise is governed by agreements, both when the enterprise enters into an agreement on Employee BankID and when the enterprise is a relying party.

Regardless of whether the TSP is the same legal entity as the RA, or the bank acting as RA is a separate legal entity, the TSP and RA liability is governed by the agreement between the bank acting as RA and the subject [20]. The TSP is also always be liable for damages under the liability rules in the Electronic Signature Act concerning liability for qualified certificate.

The TSP and bank acting as RA liability also applies where the RA or TSP has used a service provider.

The TSP can also be held liable based on standard contractual provisions. When BankID is used for financial transactions covered by the Financial Contracts Act [28], the TSP liability for these transactions will be governed by the liability rules in the Financial Contracts Act.

Distribution of responsibility between TSP's, including Right of Recourse, is governed by agreements between the banks.

Bank acting as RA liability

The bank assumes liability in relation to the customer in accordance with the agreement between the two parties, and also for Registration Authority tasks undertaken by a service provider. If the bank uses a service provider as Registration Authority, the Registration Authority's responsibility in relation to the bank shall be further regulated by agreement between the Registration Authority and the bank.

Subject liability

The subject's liability is governed by the agreement [20] between the bank and the subject. If the customer uses BankID, software or documentation in violation of the signed agreement, including unauthorised modification or manipulation of BankID or software, the bank may hold the customer liable for any losses the bank suffers in consequence.

The customer will also in accordance with common legal practice, be held responsible for dispositions made by anyone who has been able to use the customer's BankID due to an intentional or negligent act or omission by the customer.

9.9 Indemnities

The TSP's financial liability is limited to NOK100.000 per transaction. This limit does not apply if the TSP, its service provider or any other entity the bank is liable for, has acted wilfully or grossly negligently.

If the subject (and relying party) fails to fulfil the obligations in sections 9.6.3 and 9.6.4, they can be held liable for any losses that may arise, or their claims against the bank may be reduced or fall away as a result of breach of obligations.

Banks acting as RA that use a TSP that is a separate legal entity from the bank must ensure that the TSP has sufficient financial resources in accordance with the equity ratio requirements in the Act on Electronic Trust Services [15]. Liability of the bank acting as RA in relation to the TSP or vice versa, or in relation to other service providers and vice versa, is governed by agreements between these entities.

The TSP and service provider are not liable for a subject's incorrect use of a certificate.

9.10 Term and termination

9.10.1 Term

This TSPS remains in force until it is explicitly replaced by a new version of the TSPS in accordance with section 1.5.

9.10.2 Termination

This TSPS, even if replaced by a new version of the TSPS remains in effect for all BankIDs issued while the TSPS was in force.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this TSPS that are not deemed substantial may be made and approved by Bits AS without further notice.

The TSP, bank acting as RA or any of their service providers involved in operation of BankID shall be informed that there is a new version available.

Bits AS will send the amended TSPS to the National Competent Authority (Nkom) without delay.

9.12.2 Notification mechanism and period

In case of amendments to the TSPS not deemed substantial, the National competent authority shall receive a one month prior notice that a new amended version of the TSPS will be in effect from a given date. The notice will include a short summary of the nature of the amendment.

No later than on the effective day of the amended TSPS, the National competent authority shall be sent the amended TSPS.

9.12.3 Circumstances under which OID must be changed

According to ETSI EN 319 401 [24] for any changes that affect the applicability of the certificate policy, the OID should be changed. For any change in requirement or practices, that are deemed substantial and affect the applicability of the TSPS the principles for policy administration as outlined in section 1.5 will be followed. If a new OID is required, Bits AS will allocate a new OID from the range. As this requires technical changes in both the CA-system setup, the central storage entity and for the merchants the new OID will be noticed at least 6 months in advance of effective date.

9.13 Dispute resolution provisions

Disputes in connection with the issue and use of BankID are governed by Norwegian law. Any cases must be brought before Norwegian courts. Disputes between a consumer and a bank about services provided by a bank can usually be brought before The Norwegian Financial Services Complaints Board.

9.14 Governing law

The European eIDAS regulation [23] and the Norwegian Personal Data Act [14] applies.

9.15 Compliance with applicable law

This TSPS is written to comply with Norwegian Law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

The TSP holds an authorisation from the Root CA owner; Finance Norway granting authorisation to issue BankID certificates according to the scheme rules (BankID Rules).

The TSP has an agreement with the bank acting as RA detailing the obligations and liabilities between the parties.

A template has been made for the agreement between the bank acting as RA and the subject/subscriber. All banks acting as RA are obliged to use this template when issuing BankID according to this TSPS.

Agreements with relying parties are made by Vipps AS, and includes interoperability of BankID use between BankID certificates issued by different TSP's.

The TSP has entered into an agreement with Vipps AS for access to the interoperable scheme, the central storage entity and the operational infrastructure, including operation of the common BankID certificate validation services.

The TSP has entered into an agreement with the service provider of the TSP CA-system for operation of the CA.

The Bank acting as RA has entered into agreement with service providers for operation of RA-system and authentication elements (i.e. one time password mechanisms).

The TSP has entered into an agreement with the mobile network operator where the subject's SIM card is registered with at mobile subscription.

9.16.2 Assignment
No stipulation

9.16.3 Severability
No stipulation

9.16.4 Enforcement (attorneys' fees and waiver of rights)
No stipulation

9.16.5 Force Majeure
No stipulation

9.17 Other provisions

9.17.1 Termination of the BankID scheme
Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

The TSP has established a termination plan with the following procedures:

- Information to all subscribers and service providers involved in the operation of BankID
- Information to all banks acting as RA
- Information to all relying parties
- Information to all mobile network operators
- Information to other TSP's issuing BankID certificates
- Information to national authorities
- Backup and storage of all evidence of certificates and transactions with a trustworthy service provider
- Information to all relying parties on how the revocation status will be provided for the retention period stated in section 5.5.2.
- Destruction of all TSP private keys

If the TSP is not able to fulfil these obligations due to financial or other circumstances (such as bankruptcy), Vipps AS and Bits AS will perform the tasks deemed necessary to fulfil the tasks.

Vipps AS and Bits AS will keep backup of the TSP public key or any other trust service tokens for verification purposes.

Issuer specific

For Bankenes ID-tjeneste: Bankenes ID-tjeneste as Joint Issuer will not be terminated as long as there are banks with active certificates issued by Bankenes ID-tjeneste. Bankenes ID-tjeneste's owners have established agreements and procedures that ensures that the last bank using Bankenes ID-tjeneste as Joint Issuer under agreement (Bruksrettsavtale) and with active certificates will be the sole owner of the company and can terminate Bankenes ID-tjeneste as Issuer only after revocation of the Bank's certificates issued by Bankenes ID-tjeneste. This is a part of the shareholder's agreement and ensures that the company can be terminated in a controlled way. The shareholder's agreement also commits the owners to continue the operations of the company as long as there are RAs with a valid Bruksrettsavtale and active Certificates. Termination of a Bruksrettsavtale implicates that all certificates issued by the RA shall be revoked.

9.17.2 Risk management

The TSP has an inventory of all information assets and assign a classification consistent with the risk assessment, in order to ensure appropriate level of protection of primary (Information and Business process) and supporting assets (site, personnel, hardware, software, network etc.).

The TSP has established a process for yearly risk assessment of its TSP operations to determine all security requirements and operational procedures which are necessary to implement the risk treatment measures chosen.

The TSP risk assessment is based on an aggregation of risk assessments made by:

- The BankID COI Operator.
- The service provider of the bank acting as RA, and their service providers.
- The service provider of any authentication elements (i.e. one time password tokens and related services)
- The mobile network operator mobile network operator where the subject's SIM cards are registered with a mobile subscription
- The TSP own organisation and operation

The risk assessment procedures are revised on a yearly basis.

The risk assessment is followed by identification of risk treatment measures to ensure that the risk level is kept at an acceptable level.

The TSP management has approved the risk assessment and accepted the residual risk.

Issuer specific

For Bankenes ID-tjeneste: Bankenes ID-tjeneste as Joint Issuer and its RAs, which are banks, perform an annual risk analysis for the risks associated with issuing BankID certificates taking into account both business and technical risks. The analysis performed by the RAs are confirmed to Bankenes ID-tjeneste and risks and possible actions reported are taken into consideration by the RA. The risk assessment performed by the operator of the Common Operational Infrastructure is taken as input to the TSP risk assessment. RAs are identified in APPENDIX 1.

For DNB: Mobile Personal BankID is part of the applications connected to the TSP's security applications and are on the TSPs list of the most critical routines. Annually risk assessments are conducted.

For Eika: Eika Gruppen performs regularly risk analysis for the risks associated with issuing BankID certificates. The risk assessment takes into account both business and technical risks. The risk assessments performed by the operator of the Common Operational Infrastructure and other parties

are taken as input to the TSP risk assessment. Detailed procedures and templates for the TSP risk assessment is maintained in the Eika Gruppen's Quality system.

Eika Gruppen's risk procedure is evaluated and revised on a yearly basis.

The BankID risk assessment is presented to Eika Gruppen's Executive Management, who will accept the residual risk or request additional measures to be taken.

10 References

[1] BankID Rules, Finance Norway Service Office, last changed by Bits AS on 15th March 2018

[2] Security Requirements for Cryptographic Modules, NIST, US Dept. of Commerce, FIPS 140-1,1994 and FIPS 140-2, 2002.

[3] "BankID Internal Security Procedures", version 0.5, 13 June 2016.

[4] Document no longer referenced

[5] Document no longer referenced

[6] ISO/IEC 27001:2013 and ISO/IEC 27002:2013 - Information technology -- Security techniques -- Information Security Management Systems -- Requirements -- Controls.

[7] Document no longer referenced

[8] Document no longer referenced

[9] Key Words for Use in RFCs to Indicate Requirement Levels, S.Bradner, RFC2119, March 1997

[10] Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S.Chokhani, W.Ford, RFC2527, March 1999

[11] X.509 Internet Public Key infrastructure Online Certificate Status Protocol – OCSP, M.Myers, R.Ankney, A.Malpani, S.Galperin, C.Adams, RFC2560, June 1999

[12] Document no longer referenced

[13] BankID Certificate Profiles, Bits AS. (previously "External Certificates"). See Section 2 for document URL.

[14] The Personal Data Act, 15 June 2018, https://lovdata.no/dokument/NL/lov/2018-06-15-38/

[15] Act on Electronic Trust Services, which implements the EU Regulation on electronic Identification, Authentication and trust Services for electronic transactions in the internal market ((EU) No 910/2014), “Lov om elektroniske tillitstjenester”, https://lovdata.no/dokument/NL/lov/2018-06-15-44

[16] Norwegian BankID Root CP/CPS v2.3 August 2016

[17] Document no longer referenced

[18] Document no longer referenced

[19] Act of 1 June 2018 No. 23 relating to measures to combat money laundering and the financing of terrorism etc., with associated regulations, https://lovdata.no/dokument/NL/lov/2018-06-01-23

[20] Terms and Conditions for Personal BankID and Employee BankID – PDS, Bits / Finance Norway Service Office, 2019.

[21] Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks, ITU-T X.509, 11/2008

[22] Sikkerhetsråd for aktivering og bruk av BrukerstedsBankID, v1.7 (Security advice for activation and use of Merchant BankID, v1.7).

[23] Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[24] ETSI EN 319 401 v2.2.1: Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers, June 2017.

[25] ETSI EN 319 411-1 v1.2.2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements, June 2017.

[26] ETSI EN 319 411-2 v2.2.2: Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates, June 2017.

[27] RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[28] Act of 25 June 1999 on financial contracts and financial assignments [Financial Contracts Act]