

BankID TSPS Personal or Employee v1.0

BankID TSP documents

Table of Contents

1 Introduction	12
1.1 Overview.....	12
1.2 Document name and identification.....	14
1.3 PKI participants and responsibilities/obligations	14
1.3.1 Trust Service Provider	14
The TSP's Information security policy practices	15
1.3.2 Registration authorities.....	16
1.3.3 Subscribers/subjects	16
1.3.4 Relying parties	16
1.3.5 Other participants	16
1.4 Certificate usage	17
1.4.1 Appropriate certificate uses.....	17
1.4.2 Prohibited certificate uses	17
1.5 Policy administration	17
1.5.1 Organization administering the document.....	18
1.5.2 Contact person.....	18
1.5.3 Person determining TSPS suitability for the policy	18
1.5.4 TSPS approval procedures.....	19
1.6 Definitions and acronyms	19
1.6.1 Definitions	19
1.6.2 Acronyms.....	20
2 Publication and repository recommendations.....	22
2.1 Repositories	22
2.2 Publication of certification information.....	22
2.3 Time or frequency of publication.....	23
2.4 Access controls on repositories	23
3 Identification and authentication.....	24
3.1 Naming.....	24
3.1.1 Types of names.....	24
3.1.2 Need for names to be meaningful	25
3.1.3 Anonymity or pseudonymity of subscribers.....	25

3.1.4	Rules for interpreting various name forms	26
3.1.5	Uniqueness of names	26
3.1.6	Recognition, authentication, and role of trademarks	26
3.2	Initial identity validation	26
3.2.1	Method to prove possession of private key.....	26
3.2.2	Authentication of organisation identity	26
3.2.3	Authentication of individual identity.....	28
3.2.4	Non-verified subscriber information	30
3.2.5	Validation of authority.....	30
3.2.6	Criteria for interoperation	31
3.3	Identification and authentication for re-key requests	32
3.3.1	Identification and authentication for routine re-key.....	32
3.3.2	Identification and authentication for re-key after revocation	32
3.4	Identification and authentication for revocation request.....	33
4	Certificate life-cycle operational requirements	35
4.1	Certificate Application.....	35
4.1.1	Who can submit a certificate application.....	35
4.1.2	Enrolment process and responsibilities	35
4.2	Certificate application processing.....	36
4.2.1	Performing identification and authentication functions	36
4.2.2	Approval or rejection of certificate applications	39
4.2.3	Time to process certificate applications	39
4.3	Certificate issuance	40
4.3.1	CA actions during certificate issuance.....	40
4.3.2	Notification to subscriber by the CA of issuance of certificate.....	40
4.4	Certificate acceptance.....	41
4.4.1	Conduct constituting certificate acceptance.....	41
4.4.2	Publication of the certificate by the CA	42
4.4.3	Notification of certificate issuance by the CA to other entities.....	42
4.5	Key pair and certificate usage.....	42
4.5.1	Subscriber private key and certificate usage	42
4.5.2	Relying party public key and certificate usage	42
4.6	Certificate renewal	42
4.6.1	Circumstance for certificate renewal	43

4.6.2	Who may request renewal.....	44
4.6.3	Processing certificate renewal requests.....	44
4.6.4	Notification of new certificate issuance to subscriber	44
4.6.5	Conduct constituting acceptance of a renewal certificate.....	44
4.6.6	Publication of the renewal certificate by the CA.....	44
4.6.7	Notification of certificate issuance by the CA to other entities	44
4.7	Certificate re-key.....	45
4.7.1	Circumstance for certificate re-key	45
4.7.2	Who may request certification of a new public key	45
4.7.3	Processing certificate re-keying requests	45
4.7.4	Notification of new certificate issuance to subscriber	45
4.7.5	Conduct constituting acceptance of a re-keyed certificate	45
4.7.6	Publication of the re-keyed certificate by the CA.....	45
4.7.7	Notification of certificate issuance by the CA to other Entities.....	45
4.8	Certificate modification.....	45
4.8.1	Circumstance for certificate modification	45
4.8.2	Who may request certificate modification	46
4.8.3	Processing certificate modification requests.....	46
4.8.4	Notification of new certificate issuance to subscriber	46
4.8.5	Conduct constituting acceptance of modified certificate.....	46
4.8.6	Publication of the modified certificate by the CA	47
4.8.7	Notification of certificate issuance by the CA to other entities.....	47
4.9	Certificate revocation and suspension	47
4.9.1	Circumstances for revocation	47
4.9.2	Who can request revocation	48
4.9.3	Procedure for revocation request.....	49
4.9.4	Revocation request grace period.....	50
4.9.5	Time within which CA must process the revocation request	50
4.9.6	Revocation checking requirement for relying parties	51
4.9.7	CRL issuance frequency.....	51
4.9.8	Maximum latency for CRLs.....	51
4.9.9	On-line revocation/status checking availability	51
4.9.10	On-line revocation checking requirements.....	51
4.9.11	Other forms of revocation advertisements available	52
4.9.12	Special requirements re key compromise.....	52

4.9.13	Circumstances for suspension	52
4.9.14	Who can request suspension	52
4.9.15	Procedure for suspension request.....	53
4.9.16	Limits on suspension period	54
4.10	Certificate status services	54
4.10.1	Operational characteristics.....	54
4.10.2	Service availability.....	54
4.10.3	Optional features	54
4.11	End of subscription.....	55
4.12	Key escrow and recovery policy and practices	55
4.12.1	Key escrow and recovery	55
4.12.2	Session key encapsulation and recovery policy and practices.....	55
5	Facility, management, and operational controls	56
5.1	Physical controls.....	56
5.1.1	Site location and construction.....	57
5.1.2	Physical access	57
5.1.3	Power and air conditioning.....	58
5.1.4	Water exposures	59
5.1.5	Fire prevention and protection.....	59
5.1.6	Media storage.....	59
5.1.7	Waste disposal	60
5.1.8	Off-site backup.....	60
5.2	Procedural controls	61
5.2.1	Trusted roles	61
5.2.2	Number of persons required per task.....	62
5.2.3	Identification and authentication for each role.....	63
5.2.4	Roles requiring separation of duties.....	64
5.3	Personnel controls.....	65
5.3.1	Qualifications, experience, and clearance requirements.....	65
5.3.2	Background check procedures	66
5.3.3	Training requirements.....	66
5.3.4	Retraining frequency and requirements	67
5.3.5	Job rotation frequency and sequence.....	68
5.3.6	Sanctions for unauthorized actions.....	68

5.3.7	Independent contractor requirements	69
5.3.8	Documentation supplied to personnel.....	69
5.4	Audit logging procedures	70
5.4.1	Types of events recorded	71
5.4.2	Frequency of processing log	72
5.4.3	Retention period for audit log.....	73
5.4.4	Protection of audit log.....	74
5.4.5	Audit log backup procedures	74
5.4.6	Audit collection system (internal vs. external).....	75
5.4.7	Notification to event-causing subject.....	75
5.4.8	Vulnerability assessments.....	75
5.5	Records archival	76
5.5.1	Types of records archived	76
5.5.2	Retention period for archive	77
5.5.3	Protection of archive	78
5.5.4	Archive backup procedures.....	78
5.5.5	Requirements for time-stamping of records.....	78
5.5.6	Archive collection system (internal or external)	78
5.5.7	Procedures to obtain and verify archive information.....	79
5.6	Key changeover.....	79
5.7	Compromise and disaster recovery	80
5.7.1	Incident and compromise handling procedures.....	80
5.7.2	Computing resources, software, and/or data are corrupted	81
5.7.3	Entity private key compromise procedures	82
5.7.4	Business continuity capabilities after a disaster	83
5.8	CA or RA termination	85
6	Technical security controls	88
6.1	Key pair generation and installation	88
6.1.1	Key pair generation	88
6.1.2	Private key delivery to subscriber.....	90
6.1.3	Public key delivery to certificate issuer	90
6.1.4	CA public key delivery to relying parties	90
6.1.5	Key sizes	91
6.1.6	Public key parameters generation and quality checking.....	91

6.1.7	Key usage purposes (as per X.509 v3 key usage field)	91
6.2	Private Key Protection and Cryptographic Module Engineering Controls	91
6.2.1	Cryptographic module standards and controls	91
6.2.2	Private key (n out of m) multi-person control	92
6.2.3	Private key escrow	93
6.2.4	Private key backup	93
6.2.5	Private key archival	94
6.2.6	Private key transfer into or from a cryptographic module	94
6.2.7	Private key storage on cryptographic module	95
6.2.8	Method of activating private key	95
6.2.9	Method of deactivating private key	96
6.2.10	Method of destroying private key	96
6.2.11	Cryptographic Module Rating	96
6.3	Other aspects of key pair management	96
6.3.1	Public key archival	96
6.3.2	Certificate operational periods and key pair usage periods	96
6.4	Activation data	97
6.4.1	Activation data generation and installation	97
6.4.2	Activation data protection	98
6.4.3	Other aspects of activation data	98
6.5	Computer security controls	99
6.5.1	Specific computer security technical requirements	99
6.5.2	Computer security rating	101
6.6	Life cycle technical controls	101
6.6.1	System development controls	102
6.6.2	Security management controls	103
6.6.3	Life cycle security controls	103
6.7	Network security controls	103
6.8	Time-stamping	105
7	Certificate, CRL, and OCSP profiles	106
7.1	Certificate profile	106
7.1.1	Version number(s)	106
7.1.2	Certificate extensions	106
7.1.3	Algorithm object identifiers	106

7.1.4	Name forms.....	106
7.1.5	Name constraints.....	106
7.1.6	Certificate policy object identifier	107
7.1.7	Usage of Policy Constraints extension	107
7.1.8	Policy qualifiers syntax and semantics.....	107
7.1.9	Processing semantics for the critical Certificate Policies extension.....	107
7.2	CRL profile	107
7.2.1	Version number(s).....	107
7.2.2	CRL and CRL entry extensions.....	107
7.3	OCSP profile	107
7.3.1	Version number(s).....	107
7.3.2	OCSP extensions	107
8	Compliance audit and other assessments	109
8.1	Frequency or circumstances of assessment	109
8.2	Identity/qualifications of assessor.....	109
8.3	Assessor’s relationship to assessed entity	109
8.4	Topics covered by assessment.....	109
8.5	Actions taken as a result of deficiency.....	110
8.6	Communication of results	110
9	Other business and legal matters	111
9.1	Fees.....	111
9.1.1	Certificate issuance or renewal fees	111
9.1.2	Certificate access fees	111
9.1.3	Revocation or status information access fees	111
9.1.4	Fees for other services.....	111
9.1.5	Refund policy	111
9.2	Financial responsibility	111
9.2.1	Insurance coverage.....	111
9.2.2	Other assets	111
9.2.3	Insurance or warranty coverage for end-entities.....	112
9.3	Confidentiality of business information	112
9.3.1	Scope of confidential information.....	112
9.3.2	Information not within the scope of confidential information	112

9.3.3	Responsibility to protect confidential information	113
9.4	Privacy of personal information	113
9.4.1	Privacy plan.....	113
9.4.2	Information treated as private.....	113
9.4.3	Information not deemed private	114
9.4.4	Responsibility to protect private information	114
9.4.5	Notice and consent to use private information	114
9.4.6	Disclosure pursuant to judicial or administrative process.....	114
9.4.7	Other information disclosure circumstances.....	114
9.5	Intellectual property rights	114
9.6	Representations and warranties.....	115
9.6.1	CA representations and warranties	115
9.6.2	RA representations and warranties	115
9.6.3	Subscriber representations and warranties.....	116
9.6.4	Relying party representations and warranties.....	117
9.6.5	Representations and warranties of other participants	117
9.7	Disclaimers of warranties	117
9.8	Limitations of liability.....	118
9.9	Indemnities	119
9.10	Term and termination	119
9.10.1	Term	119
9.10.2	Termination	119
9.10.3	Effect of termination and survival	119
9.11	Individual notices and communications with participants.....	119
9.12	Amendments.....	119
9.12.1	Procedure for amendment.....	119
9.12.2	Notification mechanism and period.....	120
9.12.3	Circumstances under which OID must be changed	120
9.13	Dispute resolution provisions	120
9.14	Governing law	120
9.15	Compliance with applicable law	120
9.16	Miscellaneous provisions	120
9.16.1	Entire agreement	121
9.16.2	Assignment.....	121

9.16.3	Severability	121
9.16.4	Enforcement (attorneys' fees and waiver of rights).....	121
9.16.5	Force Majeure.....	121
9.17	Other provisions	121
9.17.1	Termination of the BankID scheme	122
9.17.2	Risk management.....	123
10	References.....	126

1 Introduction

Document history

Version	Date	Changes	Approved by
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 describes the Trust Service Provider Practice Statement (TSPS) for BankID Certificates for natural persons (Personal BankID or Employee BankID). 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 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 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 pertains to Netcentric BankID where private keys are stored in a secure bank system that protects the keys so that only the rightful owner can use them.

A Bank that offers Personal BankID to its customers 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 bank that offers Employee BankID to the employees of a subscriber, shall enter into an agreement with the subscriber that requests Employee BankID certificates. The agreement shall be in the language the bank usually uses in communication with the subscriber and explain the rights and duties of the subject. In addition, there shall be a signed statement from the persons who fulfil the roles as subjects.

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

When the Certification Authority System creates a certificate, the issuer of BankID certifies the link between the public key and the subject's identity. In the case of Employee BankIDs, it is also necessary to certify that the subject is employed by or acts on behalf of the subscriber. 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.

This TSPS assumes that Nets Norge Infrastruktur AS (Nets) is the service provider for BankID issuers. Several parts of this document depend on, and refer to, whole documents or specific parts of documents [3] and [4] which describe internal procedures in Nets. 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.

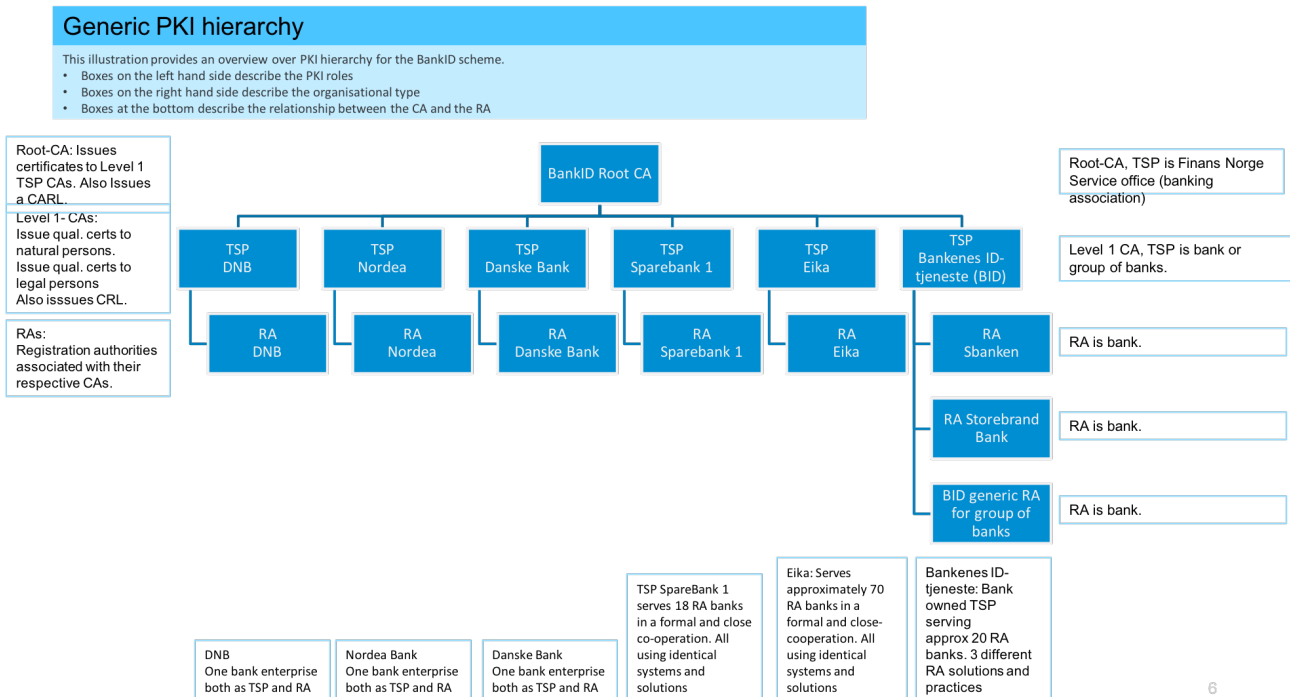
This TSPS is a standard document covering all Level 1 issuers of BankID who use Nets as service provider for common operational infrastructure. Some points in the TSPS documentation refer to the practices of the issuer of BankID and will be supplemented by documents prepared by the issuer. Annex A in this document contains requirements for how individual practices shall be documented.

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 Vipps AS, see table in Chapter 1.2. This document pertains to Bank-stored BankID where private keys are stored in a secure bank system on the service provider’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 subscribers, and for Employee BankID the subject’s subscriber. 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 Nets as service provider on behalf of Root-CA.



The structure (headings and subheadings) in this TSPS is organised in accordance with recommendations in [10].

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

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.

This document describes the Certificate Policy for BankID Certificates issued as qualified certificates to natural persons, either as Personal BankID or Employee BankID. See section 7.1.6 for Object Identifiers for this policy. The Object Identifier for this document version is 2.16.578.1.16.1.12.1.1.1.0 for Personal BankID and 2.16.578.1.16.1.13.1.1.1.0 for Employee BankID, 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 underlying procedures are sufficient, even if these are carried out by third party. This means the 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.

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

For Danske Bank: Within this TSP, it is Group IT Security & Risk at Danske Bank which is the internal management body responsible for implementing the practices within the organisation.

For DNB: Within this TSP, it is DNB New Business 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 BankID belonging to the owner of a personal certificate. 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 and defined as either a Personal BankID or a Employee BankID

For Personal BankID, the Subject and Subscriber are always the same entity. For Employee BankID, the Subjects and Subscribers are separate entities.

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.

The following clarification applies for Employee BankID: the subscriber, not the individual, enters into an agreement with the bank acting as RA about issuance of Employee BankID. The subscriber must confirm in writing to the bank acting as RA that every person who is to be issued with Employee BankID have an employment or contractual relationship with the subscriber.

For Bankenes ID-tjeneste: This TSP does not issue EmployeeBankID.

For Danske Bank: This TSP does not issue EmployeeBankID.

For DNB: This TSP does not issue EmployeeBankID.

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 service provider of the CA-system and the central storage entity 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

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.

1.4.1 Appropriate certificate uses

Certificates issued in accordance with this TSPS can only be used between natural persons who are subjects, and merchants, to perform the following security services:

- Authentication;
- Digital signing.

Certificates issued under this TSPS can only be used on relying parties services or websites for purposes such as logging on services and in web applications on the merchant sites.

The subject shall use BankID together with the appropriate software, hardware or security equipment specified by the bank. The bank may add new requirements for software, hardware or security equipment where this is necessary for security reasons or due to necessary BankID upgrades. If BankID is enabled in a computer environment that does not meet the BankID security requirements, this may leave it open to misuse. Banks will provide requirements and advice re: appropriate user environments.

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 user documentation.

Certificates issued in accordance with this certificate policy cannot be used as basis for issuing other certificates or credentials.

1.4.2 Prohibited certificate uses

Everything which is not explicitly allowed, is prohibited.

1.5 Policy administration

Vipps AS is responsible for maintaining this policy. The TSP, bank acting as RA, service providers and Bits AS can initiate TSPS changes. Subjects or users can propose changes through a bank or by contacting Vipps AS directly. 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;
- Nets Norge Infrastruktur AS (in their capacity as service provider for root-CA).

Bits AS are 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

Vipps AS is responsible for developing and managing BankID TSPS. Bits AS administrates Vipps AS' standards and policies on behalf of Vipps AS, and is responsible for maintaining this document. Cf. "BankID Rules" §4.1 [1].

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

This Common TSPS is registered with Vipps AS and approved by Bits AS. Vipps AS is responsible for the administration and maintenance of this document. The specific sections where it is identified that the TSP individual practices; describing the TSP and bank acting as RA practices are marked. For these sections a separate appendix for this purpose is written by the TSP.

Any questions regarding this document may be addressed to:

Vipps AS
Munkedamsveien 45
N-0250 Oslo
Norway
Telephone: +47 480 33 777
Web site: <http://www.bankid.no>
Contact: Tommi Pohjaniemi (Compliance manager)

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 in cooperation with its service provider. 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 in cooperation with its technical serviceprovider. Any TSPS created within the scope of a BankID policy must be approved by Bits AS. The document must be approved when it is first produced and subsequently if any major amendments are made.

Each TSPS undergoes a yearly review and is included in the internal audit schedule. Compliance with RFC 3647 [27] and ETSI 319 411-2 [26] will be assessed, and any inconsistency remedied.

Before publishing new TSPS, Bits AS 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.

BankID COI: BankID's Common Operational Infrastructure

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.

Certification Authority Revocation List: Revocation list containing a list of CA-certificates issued to certification authorities that are no longer considered valid by the certificate issuer.

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 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 (cf. Chapter 1.3.1).

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

Locally Stored BankID: BankID where the private key is stored locally on the subject's computer. Required software is downloaded at first use and permanently installed on the computer.

Netcentric 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.

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.

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 Netcentric 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. A person who is a subject, can also fulfil the role of relying party. (Comment: In agreements between subscribers and banks the subject may also be referred to as the "user".)

Validation Service: Ref. Certificate validation service.

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
OCSP Online Certificate Status Protocol
OID Object Identifier
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

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/>

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/globalassets/dokumenter/apne-sider/regler-om-bankid/regler-om-bankid-per-070217.pdf>
- BankID root certificate: <https://www.bankid.no/en/rootca>
- BankID Certificate Profiles: https://www.bankid.no/en/bankid_certificate_profiles.pdf
- PDS Personal:
 - **For Bankenes ID-tjeneste:** https://www.bankid.no/en/bid_pds_personal
 - **For Danske Bank:** https://www.bankid.no/en/danskebank_pds_personal
 - **For DNB:** https://www.bankid.no/en/dnb_pds_personal
 - **For Eika:** https://www.bankid.no/en/eika_pds_personal
 - **For Nordea:** https://www.bankid.no/en/nordea_pds_personal
 - **For SpareBank 1:** https://www.bankid.no/en/sparebank1_pds_personal
- TSPS Personal (this document): https://www.bankid.no/en/tsps_personal

2.1 Repositories

The TSP makes information about revocations available to BankID Certificate Validation Services service providers, see chapter 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 chapter 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 by the approval body described in section 1.5.

2.4 Access controls on repositories

The Certificate database is protected according to security controls found in this chapters 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 PERSONAL BankID:

Personal BankIDs are 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)	Optional	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.

SUBJECT NAME EMPLOYEE BankID

Employee BankIDs are certificates tied to a person's identity and an employment or engagement relationship.

Attribute	Importance	Content Requirement
Country (C)	Mandatory	Shall have the value “NO”.
Organisation (O)	Mandatory	<Enterprise name> <,> <enterprise organisation no.>
Serial Number (SN)	Mandatory	Alphanumeric value that ensures that the name is unique (see section 3.1.2).
Organisational Unit (OU)	Optional	Alphanumeric value that describes the employee’s relationship to the enterprise. Can be department, employee no. etc

Attribute	Importance	Content Requirement
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

All individuals are assigned a unique National ID number or D number from the national authorities. A person who has applied to become a BankID subject is verified by the RA against the information in the National Registry, 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.

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 Personal BankIDs or Employee BankIDs. 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.

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

All private keys for certificates issued in accordance with this TSPS are generated and stored in a separate, secure storage entity in a secure system on the service provider's premises. Keys are protected to ensure only the relevant subject has access.

A subject can only prove ownership of a private key when he or she can show that they have access to the secrets that are necessary to use the key. This is described in chapter 6.1.2.

3.2.2 Authentication of organisation identity

It is possible to issue a Employee BankID to a person who has access to the account belonging to another legal entity (e.g. an enterprise). Employee BankIDs are issued to natural persons. The RA verifies the identity of the person to whom the BankID is to be issued in accordance with the requirements described in this chapter. The Subscriber must confirm that the relevant person has an employment or contractual relationship with the

Subscriber. It is a prerequisite Employee BankID is only used for official tasks or assignments on behalf of the Subscriber.

Before an Employee BankID is issued, the certificate applicant shall document their ID and confirm that the submitted information is correct. Such identification and identity validation shall be made based on physical presence at the bank or its representative, unless the person's identity has already been validated through an existing customer/account relationship with the bank. Checks shall be made in accordance with the provisions in the Money Laundering Act [19] and the Electronic Signature Act [15]. The enterprise shall provide documentation confirming the person's employment or contractual relationship with the Subscriber.

The bank may request further information or documentation, and may also conduct further investigation into the accuracy of the information provided, authorisations etc.

Certificate applicants who already have a customer relationship with the bank can provide proof of ID electronically. This assumes that the bank has already performed a full control of the person's identity and that the person in question can access the Registration Authority through a service (e.g. online banking) that uses an approved authentication method.

For Bankenes ID-tjeneste: BID does not issue Employee BankID.

For Danske Bank: Danske Bank does not issue Employee BankID.

For DNB: DNB as a TSP does not issue Employee BankID.

For Eika: Eika Gruppen issues Employee BankID.

When Eika Gruppen shall issue an Employee BankID to employees in a company or organisation, the organisation has to be represented by a person with power to commit the organisation or with an explicit authorisation to sign an agreement regarding EmployeeBankID on behalf of the organisation. This person must give the bank his necessary personal information and identification papers. His or hers authorisation to sign the agreement must be documented by giving the bank a Norwegian Certificate of Registration for the company or organisation or other equivalent documentation. The bank will keep a certified copy of all authorisation and identification documents.

It is the legal person (e.g. company or organisation) which enters into the contract for EmployeeBankID with the bank, that informs the bank about which employees that will get EmployeeBankID. These employees must then register and identify themselves to the bank in the same way as any regular personal customer.

The organisation has its own signed agreement with the bank that is RA. And the individual that is going to get EmployeeBankID, will be presented to and have to accept a separate agreement before he activates EmployeeBankID for the first time.

Eika Gruppen uses customer agreements based on standard templates fra Finance Norway.

If a certificate is revoked, the customer has to apply for/order a new BankID.

For Nordea: The following information about the organisation / certificate subscriber shall be presented to the Nordea customer representative before the registration process:

Full name and legal status of the Subscriber as defined in the company register (Brønnøysundregistrene). The Subscribers' Organization Number as defined in the company register (Brønnøysundregistrene). A document that identifies that the person who by the organization has the given signature right for the organization or per procurator. The Nordea customer representative will perform checks in accordance with the provisions in the Money Laundering Act Money Laundering Act.

Nordea employees are already identified and authenticated by Nordea that has all employees' documents (personnel record) after their hiring. Without prejudice to the requirements of law, the identification and authentication process Nordea employees' takes place by direct personal knowledge and could be a little different than the process for externals holders.

Further, if all other circumstances being equal, the following rules are valid for employees and the external persons.

Data and documentation provided are handled through automated procedures strictly for the purposes described above and with the use of security measures to ensure the confidentiality of personal data and to prevent illegal access to data pursuant to eIDAS and Legislative Decree n.196/2003.

For SpareBank 1: No additions.

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. The Bank has a duty, governed by laws and regulations on money laundering, to record the credentials of its customers [19]. 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.

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.

Personal customers who already have a customer relationship with the bank, and who have previously been identified 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 access the Registration Authority through a service (e.g. online banking) that uses an approved authentication method.

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 certificates for new customers based on BankIDs issued by another bank.

The Bank shall process 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 chapter, and may not register themselves

For Bankenes ID-tjeneste: RAs only issues certificates to subjects having been physically present and authenticated by the credentials specified, and do not issue certificates for new subjects based on BankIDs issued by another bank.

Subject information is retrieved from the Customer Ledger which is regularly washed against the National Population Register.

For Danske Bank: Danske Bank ensures that physical presence required, either in a branch or Posten. The customer name is verified against the National Population Register and controlled with information in the passport. The customer register is washed against the National Population Register regular.

For DNB: Certificate applicant name and national ID number are retrieved from the bank's central customer register during the process for ordering Personal BankID. They are then shown to the certificate applicant for approval as one of the steps in the application process.

The customer register is washed against the National Population Register weekly. The data transferred from the National Population Register consists of the national ID number, full name, residential address and postal address.

All individuals are unambiguously linked to a [Norwegian] national ID number or "D-number" (temporary national ID no.). The TSP only issues Personal BankIDs to persons who are unequivocally linked to a national ID number. The TSP does not issue Personal BankIDs to certificate applicants who only have a D-number. Activation data are sent to the certificate applicants address in the National Population Register or to an alternative address specified by the certificate applicant, if applicable. Notification that activation data has been dispatched by post is sent by SMS or e-mail.

The TSP only issues Personal BankID to certificate applicants who order it themselves through the Internet banking service. This means that the certificate applicant must have entered into an Internet banking agreement with the bank, and must be logged onto the Internet banking service. This calls for two-factor identification for the certificate applicant to initiate and complete the ordering process. The TSP only issues Personal BankID to certificate applicants who have a valid Norwegian national identity number and over the age of 15.

Certificate applicants between the ages of 15 and 18 must have permission from their legal guardian(s) to order a Personal BankID. In such event, the certificate application must be initiated by the guardian through the Internet banking service. Upon receipt of an approved order from a guardian, the Personal BankID will be issued in the standard manner for persons over the age of 15.

The RA and certificate issuer determine the subject's full DN and ensure that the name is unique. All subjects are assigned a unique identifier in accordance with the BankID rules.

For Eika: Eika Gruppen issues Personal BankID and Employee BankID.

When Personal BankID or Employee BankID is issued, the name of the subject in the certificate is then drawn from the name that is registered in the central customer register of the bank. The names in the bank's central customer register is checked toward the customer's name in the Norwegian National Registry on a regular basis.

The full name of the customer is always used by the bank.

All new customers in branch banks wanting online banking and BankID, must as a rule meet in person at a bank branch when initiating a banking relationship. In special cases, individual banks may have to use Posten Norge's PUM service. If so, the recipient must meet in person at the post office or corresponding postal service at a store/outlet to collect the shipment by displaying valid identification and sign the PUM receipt.

All new customers in online banks wanting BankID, will for their part be identified through Posten Norge's PUM service.

The bank's routines for checking identification involve certain given requirements for identification in connection with initiating new customer relations.

Valid identification is:

- Valid Norwegian passport (Main rule)
- Valid Norwegian immigrant's passport (Main rule)
- Foreign passport (In special cases where the bank is certain about the person's identity.)

Eika Gruppen does not issue certificates for new customers based on BankIDs issued by another bank.

The banks which are RAs for BankIDs issued by Eika Gruppen, will always register the subscriber's and the subjects' physical address in their customer systems.

Eika Gruppen issues contracts on paper or electronically depending of the individual bank and whether the customer uses a bank branch or an online solution.

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

For Nordea: For the time being, the subject has to be 15 years or older in order to receive BankID from Nordea. (BankID can be issued to persons over 13 years old, but Nordea internal policies state 15 years. This might be subject to change). Additional requirement in order to be granted a BankID Certificate, the subject must be identified with valid passport.

For SpareBank 1: The RA system has two methods for ordering certificates; self-serviced and manually by bank employees. The customer must take an active part in each type of issuing process.

For issuing bank-stored BankID to customers under 18 years, legal guardian must also sign.

Personal data is regularly synchronised with the Norwegian register of residents (Det Sentrale Folkeregister (DSF)).

3.2.4 Non-verified subscriber information

Not applicable.

3.2.5 Validation of authority

Upon entering into an Employee BankID agreement, the enterprise shall be represented by the signatory or a person who has been expressly authorised by the signatory to enter into an Employee BankID agreement on behalf of the enterprise. A sole proprietorship shall be represented by the proprietor of the sole proprietorship or a person authorised by the proprietor to enter into an Employee BankID agreement on behalf of the sole proprietor.

The representative shall submit personal data and appropriate ID documents and confirm that the information is correct. His or her right to enter into the agreement shall be documented by presentation of a Norwegian Certificate of Registration from the Norwegian Register of Business Enterprises, or similar.

The Bank is obliged to keep a securely stored copy of the submitted ID documents. The Bank has a duty, governed by laws and regulations on money laundering, to record the credentials of its customers [19].

Subscribers employed in the TSP organisation must follow the same validation of authority as stated in this chapter, and may not register them selves.

For Bankenes ID-tjeneste: BID does not issue Employee BankID.

For Danske Bank: Danske Bank does not issue Employee BankID.

For DNB: DNB does not issue Employee BankID

For Eika: When Eika Gruppen shall issue an Employee BankID to a company or organisation, the organisation has to be represented by a person with power to commit the organisation or with an explicit authorisation to sign an agreement regarding Employee BankID on behalf of the organisation. This person must give the bank his necessary personal information and identification papers. His or hers authorisation to sign the agreement must be documented by giving the bank a Norwegian Certificate of Registration for the company or organisation or other equivalent documentation. The bank will keep a certified copy of all authorisation and identification documents, and the copy will be retrievable.

It is the legal person (e.g. company or organisation) which enters into the contract for Employee BankID with the bank, that informs the bank about which employees that will get Employee BankID. These employees must then register and identify themselves to the bank in the same way as any regular personal customer.

For Employee BankID the organisation is identified by a unique organisation number, while there is also a field for identifying the employee by his employee number or another association to the organisation.

For Nordea: Full name and legal status of the subscriber as defined in the company register (Brønnøysundregistrene). The Subscribers' Organization Number as defined in the company register (Brønnøysundregistrene). A document that identifies that the person who by the organization has the given signature right for the organization or per procurator.

For SpareBank 1: No additions.

3.2.6 Criteria for interoperation

The certificate applicant has to agree to and actively participate in the issuance process. This does not prevent the bank acting as RA from initiating the issuance process provided the certificate applicant is actively involved.

The bank acting as RA shall process registration data and other customer data in accordance with the Personal Data Act [14].

For Person BankID, the customer shall be informed through the text in the agreement that content from the Person BankID will be included in message exchanges with merchants. The customer's National ID number is not part of the contents of Personal BankID, and will never be disclosed by the issuing bank to merchants who do not already legally hold the customer's National ID number.

For Employee BankID, the subject shall be notified that content from the Employee BankID will be included in message exchanges with merchants. The subject's National ID number is not part of the contents of his or her Employee BankID.

For Bankenes ID-tjeneste: The certificate applicant has to 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. All BID RAs use a contract form for Personal BankID between a subject and a bank developed and recommended by Finance Norway. Such agreements are logged and retained for a minimum of 10 years.

For Danske Bank: The certificate applicant has to agree to, and actively participate in, the issuance process by accepting an agreement and using the Activation Data and Possession Element issued by the Danske Bank. The subject need to activate and order BankID at self-service online system hosted by Danske Bank. Danske Bank do make available the Terms & Conditions to the customers in the eBanking.

For DNB: No additions.

For Eika: The order process for BankID in the banks affiliated with Eika Gruppen always requires that the customer participate actively in the process.

Branch banks: The customer must visit a bank branch and enter into a customer relationship.

Online banks: The customer is presented with the BankID-agreement during the registration process. There he is asked to confirm that he has read the agreement and accepted the terms.

BankID will not be issued unless the agreements is accepted by the customer.

Eika Gruppen's BankID solution logs all new agreements to issue BankID. Such log data are stored for a minimum of 10 years

All the banks acting as RA under Eika Gruppen's CA process registration data and other customer data in accordance with the Personal Data Act. This is a requirement from Norwegian banking authorities in general and does not follow from the BankID regulation alone.

Eika Gruppen uses customer agreements based on standard templates from Finance Norway.

For Nordea: No additions.

For SpareBank 1: No additions.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Routine re-key is performed as regular renewal initiated from the RA in a 90 day window before the certificate expires. The RA therefore keeps track of all expiration days for all BankID's issued according to this TSPS. The RA marks the BankID for renewal in the CA-system, and the BankID will be automatically renewed with re-keying the next time the end user is invoking key usage with the credentials as described in chapter 6.1.2.

For Bankenes ID-tjeneste: RAs perform re-keys as described using current subject information from the RAs customer ledger. In the event of a subject changing name, a re-key is performed. Subjects receives a notification in advance of the certificate expiring.

For Danske Bank: Danske Bank as a RA check, if any certified names or attributes have changed and if so, the changed registration information is verified, recorded, agreed to by the subscriber as per section 3.2.

For DNB: The TSP sends a reminder by SMS or by letter 90 days prior to certificate expiring. The reminder includes information about how to renew certificate.

For Eika: Personal BankID certificates to be renewed are marked in the central storage unit in BankID COI. This happens by Eika Gruppen's BankID system sending a message to BankID COI.

When renewing, the customer can keep the same activation data (static BankID password and OTP unit). If there are changes to the information in a certificate, e.g. name, Eika will submit a renewal notification to BankID COI.

Eika Gruppen will not change a certificate due to changed names or other essential attributes, unless this new registration information is verified, either according to dialogue with and verification from the customers or verification from the Norwegian National Registry.

If a certificate is revoked, the customer has to apply for/order a new BankID, whereas customer information then will be retrieved from the bank's central customer register.

For Nordea: No additions.

For SpareBank 1: No additions.

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: Danske Bank as RA check if the previous certificate has been revoked and if so, the registration information shall be verified, recorded, agreed to by the subscriber as per section 3.2.

For DNB: The TSP does not automatically issue a new certificate to replace one that has been revoked. Certificants can order new certificates themselves in the Internet banking service. In the event of misuse or suspicion thereof, the subject will be “black-listed” and will not be able to order a new BankID.

For Eika: After revocation, the customer must submit a certificate request following the same process as at the initial registration. In such cases of re-issuance secure identification according to the guidelines of the bank is required.

The ordinary procedures for requesting a BankID must for all significant parts be followed. Any customer information will be retrieved from the bank's central customer register.

For Nordea: Normal procedure is to contact the bank's customer service in order to get a new certificate. However, in certain scenarios, customers with a revoked certificate may be asked to undergo the initial registration process (described in Section 3.2) to obtain a new certificate.

For SpareBank 1: No additions.

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, 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.

For Bankenes ID-tjeneste: All RAs have a 24/7 suspension service handling suspensions outside business hours. Reopening and revocation are only performed by the RAs.

Requests for revocation and reports of events relating to revocation requires either physical presence, messaging through the Internet banking service or similar service using a recognized authentication mechanism, or a verification through control questions using the RAs telephone support service.

For Danske Bank: Certificate owner can submit revocation request through Danske Bank self-service systems where authorisation is verified via the relevant BankID based authentication (2 Factor).

The certificate owner could also call Danske Bank customer support to submit revocation request where authorisation is verified via the set of Secret Question answers.

Danske Bank will initiate despatch of a snail mail to the subject informing about the revocation request.

For DNB: The TSP has a 24/365 invalidation/blocking service. 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.

The TSP must notify the service provider (NNI) as soon as there are grounds for revoking a certificate. The contents of the notification message are validated, and the sender is thereafter validated in the certification authority system. Once the message has been validated, the certificate is revoked in the certification authority system and a signed message is immediately sent to the certificate validation service stating that the status of the certificate has been changed. In addition to the real-time message which includes the revocation details for the individual certificate, a signed Certificate Revocation List (CRL) is sent from the certification authority system to the certificate validation service once an hour.

When the bank or RA has sent instructions to the service provider to revoke a Personal BankID, the bank or RA must verify that the status of the relevant Personal BankID has been changed in the certification authority system. This is done by means of continuous status checking from the Registration Authority's side of the certificate authority system (i.e. from the registration application). The bank shall subsequently inform the subject that his/her Personal BankID has been revoked.

The subject may request revocation of his/her BankID by going in person to a bank branch office or over the telephone. The bank has special standard procedures for handling such requests. If the certificate holder goes to a branch office, he/she must show valid proof of identity. If the subject contacts the TSP by telephone, he/she must go through an enhanced customer identity checking process in Customer Service to verify the correctness of the subject's authenticity. In general terms, this entails answering a number of more complex questions related to different sets of underlying data. Keeping a log is one of the requirements stipulated in the standard procedure.

The bank always sends the subject written confirmation of revocation. The channels that are used to confirm revocation are: eDialog ('electronic dialogue') in the Internet banking service, regular mail, SMS and email. The bank logs and stores all requests for revocation. A message is always sent in eDialog. The customer adviser must also select an additional channel for notification.

All requests for revocation are logged and stored by the bank

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 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.

If a customer asks for suspension of his BankID, the bank will do this after only asking for the customer's national ID number.

For Nordea: Customer service of Nordea shall authenticate all revocation requests.

A subject/customer can contact Nordea customer service in order to revoke or suspend a BankID certificate, by person in a local branch by presenting appropriate ID (valid passport), by signed request or by telephone to customer service.

If contacting customer service by telephone the customer/subject has to prove correct answer to a number of security questions.

For SpareBank 1: The subject has to answer a number of security questions if the request for revocation is done by phone.

4 Certificate life-cycle operational requirements

The BankID CA-system and central servers and storage equipment is 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.

Persons shall be identified at the RA as described in Chapter 3.2.

The central storage entity operated by the service provider 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 service provider.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: In Danske Bank Applicants must be 15 years or older to apply for a BankID, and have a customer relationship with a Danske Bank Norway.

For DNB: Certificate applicants must have a valid bank account and a possession item issued by the TSP.

For Eika: Persons with a customer relationship with a bank in Eika Gruppen acting as RA can submit a certificate application. Applicants must be 13 years or older to apply for a BankID.

Persons applying for BankID is identified at the RA as described in Chapter 3.2.

For Nordea: Even though BankID policy states that applicants must be 13 years old in order to apply, Nordea internal rules states that the age limit is currently 15 years old. This might be subject to change.

For SpareBank 1: No additions.

4.1.2 Enrolment process and responsibilities

Subscribers and parties relying on the PersonBankID 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 TSPs customer system.

A 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.

Before an Employee BankID can be used, the RA will verify that the enterprise has ensured that the subject has signed a statement explaining rights and obligations, has access to instructions for use and has installed a personal security environment if required.

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

For Bankenes ID-tjeneste: Subject information is retrieved from the Customer Ledger and will be presented to the subject for verification during the issuance process.

No further additions for Personal BankID. BID does not issue Employee BankID.

For Danske Bank: Terms and conditions are made available to the customers within online banking (eBanking). Danske Bank stores an electronic copy of the signed agreement in the customer folder.

For DNB: The RA has the necessary personal data, including the national ID number in its central customer register. When filling out an application for a Personal BankID in the Internet banking service, the certificate applicant will be shown the personal data such as his/her name and national ID number, as well as the terms and conditions for BankID. The application cannot be completed until the certificate applicant confirms that the personal data are correct and that he/she has read and agrees to the contractual terms and conditions.

Users have to accept terms and conditions when BankID are issued. BankID terms and conditions are available to all BankID subjects on the TSPs website after ordering BankID.

For Eika: Personal customers will be presented with the BankID agreement between themselves and the bank in the course of the registration process. They have the opportunity to print out the agreement during the registration process. During the registration process the customer will also be presented for any necessary security instructions.

It is the legal person (e.g. company or organisation) which enters into the contract for Employee BankID with the bank, that informs the bank about which employees that will get Employee BankID. These employees must then register and identify themselves to the bank in the same way as any regular personal customer. A person having Employee BankID, must also sign an appendix to the organisation's own BankID agreement with the bank. These agreements and the appendix inform the customers of their obligations.

For Nordea: All subjects are required to present a valid passport. The requirement is currently that the id verification has to be done in person in either a local branch or in a post office.

The customer will need to sign the [3] Bank/Customer agreement. After that, the subject/customer will receive a one-time PIN to the authentication token that is enforced to be changed. After the customer has changed the pin the customer gets enrolled as a BankID certificate holder.

For SpareBank 1: No additions.

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.

The certificate applicant will perform a registration sequence and will receive or select an initial password submitted with the certification request. If the password is not selected by the Subject, the password must be changed before initial use.

The certificate issuer shall provide a unique ID to ensure that the combination of "IssuerDN" and "subjectDN" is unique within the BankID domain.

The registration authority (RA) shall provide information to the service provider about which possession element in the two-factor authentication shall be used for the relevant BankID. The RA shall allocate and personalise a possession element for the certificate applicant. Solutions and routines for this shall be established by the RA and approved by Bits AS.

Communication between the RA and the service provider is protected against unwanted disclosure and manipulation as described in Chapter 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 on which the RA is entitled to issue certificates.

The service provider notifies the RA that the certificate application is completed.

Following the certificate issuance, the customer who has become a subject must have authentication mechanisms for two-factor authentication. One or both of these may have been issued previously.

For Bankenes ID-tjeneste: The subject will be provided with a possession element for generation of one time codes. The RA informs the subject of issuance of the certificate and that a Initial Activation code has been distributed.

For Danske Bank: No additions.

For DNB: Personal BankIDs are issued on the basis of an ordering process in the Internet banking service in which the certificate applicant has actively participated. In one part of this application process, the certificate applicant is asked to confirm that the personal data registered by the bank– the name and national ID number - are correct. After confirming the displayed personal data, the certificate applicant must open the BankID terms and conditions and confirm that he/she accepts the contractual terms and conditions. The subject will then be given a temporary password, which can be sent by SMS if the subject's mobile telephone number is already registered in the bank's systems. The certificate applicant will then be logged off the Internet banking service, and needs to use the temporary password to log back onto the service.

The certificate applicant then needs to change the temporary password to a self-chosen, static BankID password. The subject will use this password, together with the already assigned possession item, as an authentication mechanism when he/she uses the BankID. The subject will be notified when the agreement has been accepted and the BankID has been issued. The notification will be sent to the subjects mailbox in the Internet banking service, and through another channel (e-mail, SMS or by post).

The possession item is used as an authentication element in BankID and as a one-time code in a proprietary banking solution together with a personal code.

The BankID password must consist of at least 8 characters (numbers, letters, and special characters) and can be changed by the subject in the BankID client. Used as the "know-element" in BankID.

Personal code are a proprietary bank solution. 4-digit code used to log onto the Internet and mobile banking services together with the one-time password from the possession item. The subject can change the personal code through the Internet banking service.

The TSP mostly distributes private/confidential items by post and SMS. If the password and the possession item are both sent to the subject at the same time, the password generator will be sent by registered mail. If the personal code is sent by SMS, the password generator will be sent by regular mail. Password generators that are distributed through normal production are packed and sent by the bank's sub-contractors, and automatic personalization is triggered by the orders.

The orders of possession items can be automatic orders resulting from either the establishment of a new customer relationship or purchases of new products that entail Internet banking. Other normal reshipments due to battery failure, loss of a password generator and the like are handled by the solution for normal production. Distribution in

connection with normal production is based on the principle of physical separation between the subject, processor/customer service representative in the bank and the password generator. This principle has been observed for previous mass shipments carried out, for instance, in connection with the retirement of non-approved solutions like paper-based code cards. To ensure separation, the bank's personnel are not permitted access to the sub-contractor's place of business and sub-contractors do not have access to the personalization solution.

As a rule, personal codes are sent by SMS but they may also be sent by post. The personal code is a personal 4-digit code used together with the possession item in the Internet banking service and Kontofon/Telegiro. There are a few additional distribution solutions: Possession items: The Account Administration section has a small supply of password generators that can be sent directly through the Post Office if the subject is in urgent need of a password generator and the normal distribution through the Post Office is not fast enough. Emergency password generators: All of the branch offices have a small supply of possession items. These supplies are replenished by Account Administration when necessary. There are only 2 individuals in each office who are authorized to personalize these password generators.

These possession items are normally sent 50 at a time to the branch offices by first class mail. The possession items are thereafter handled in the same manner as other office supplies. They are intended for use in especially critical situations, for instance when the subject has an acute need for a replacement possession item. The possession item are personalized when they are handed over to the subject. Password and personal code: The bank has two types of distribution for personal codes and "unlocking" passwords for BankID. BankID password: solution whereby the one-time BankID code is sent to the subject by SMS. Personal code: The subject calls the customer service for an reset. Both these solutions are backed by an enhanced customer identity checking process in Customer Service to verify the subject's identity and establish/authenticate that he/she is the correct subject.

In general terms, this entails answering a number of more complex questions related to different sets of underlying data. Keeping a log is one of the requirements stipulated in the standard procedure. All events related to security instruments (possession items, password, personal code etc.) are logged in the administration system.

For Eika: The order process for BankID in the banks affiliated with Eika Gruppen requires that the customer participate actively in the process.

Branch banks: First, the customer must visit a bank branch and enter into a customer relationship. This entails the customer presenting identification, stating required personal information, and signing required agreements in the bank.

Online banks: For online banks and other special cases where the customer can't come to a bank branch, Eika Gruppen uses Posten Norge's PUM service to identify the customer in a secure way. If so, the recipient must meet in person at the post office or corresponding postal service at a store/outlet to collect the shipment by displaying valid identification and sign the PUM receipt. All new customers in online banks wanting BankID, will be identified through Posten Norge's PUM service. First, the customer must visit the bank's web site and enter into a customer relationship. This entails the customer stating required personal information on the web pages. The customer will then receive a PUM shipment with, among other things, the required agreements with the bank.

When the customer has entered into a customer relationship, the bank will make sure that a One Time Password (OTP) mechanism is distributed to the new customer in a secure way. The OTP is constructed according to Bits AS' rules. Together with the OTP unit, the customer also receives other necessary information.

The certificate applicant also receives a static, personal BankID password from Eika, and this password together with an OTP is used in the activation process further on. The customer will also have to change this password to a password of his own choosing at first time login in the bank's internet bank. This personal password has to be constructed according to current BankID password rules to be accepted by the system.

Communication between the RA and the service provider is protected against unwanted disclosure and manipulation as described in Chapter 6.

Eika's service provider notifies the RA that the certificate application is completed.

Following the certificate issuance, the customer who has become a subject, will now have authentication mechanisms for two-factor authentication.

For Nordea: A Nordea representative validates the received documentation and enters the subjects data in the registration application. Any rejection of the application is communicated by the RA (Nordea) to the applicant. Request validation is performed by the Nordea employee that receives the request and is managed in the same application used to register the application. After the approval, the Nordea forwards issue request to the CA infrastructure to proceed with the certification issuance.

For SpareBank 1: The Registration Authority generates an initial password for the BankID that has to be changed by the customer.

4.2.2 Approval or rejection of certificate applications

For Bankenes ID-tjeneste: A certificate applicant is deemed to have accepted BankID and the certificate when his/her portion of the registration process has been completed. When the certificate applicant accepts his/her BankID, he/she is given the status “BankID subject” (certificate holder).

For Danske Bank: No additions.

For DNB: A certificate applicant is deemed to have accepted BankID and the certificate when his/her portion of the registration process has been completed. When the certificate applicant accepts his/her BankID, he/she is given the status “BankID subject” (certificate holder).

For Eika: See sub-chapters 4.9.3 - Procedure for revocation request – and 4.9.5 – Time within which CA must process the revocation request.

For Nordea: Approval is done if the subject qualify according to BankID and Nordea policies. If a subjects application is rejected, the subject will be informed by the employee.

For SpareBank 1: The registration authority will only accept the certificate application if the Applicant

- is a customer of the bank
- has been successfully identified
- has provided the required data
- has approved the agreement

If there requirements are not met, the application will be rejected.

4.2.3 Time to process certificate applications

Issuing of PersonBankID is based on a queing system in the CA-system. After the certification request is forwarded from the RA to the CA, the certificate is normally issued in near real time, 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 generates the key pairs for authentication and signing respectively and formats the PKCS#10 certification requests to the CA instance where the bank acting as RA is associated with. The CA instance provides a queing 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

Key generation and certification are performed in the TSP CA-system on the service provider's premises. Before keys can be generated, the CA-system service provider authenticates the RA and validates the order message. There is no need for further interaction with the certificate applicant, and there is no need for distribution and installation of software on the applicant's devices to accomplish this.

The CA-system creates key pairs on behalf of the certificate applicant. The certification authority system uses approved key generation software based on, amongst other things, random number generation, inside a FIPS 140 [2] Level 4 approved hardware security module (HSM). The personal customer's private keys are transmitted from the HSM in a highly encrypted state for storage in a secure database in the central storage entity. The public keys are sent to the certification authority system in a certification request. (PKCS#10 format [8]).

The certification authority system produces EmployeeBankID and PersonBankID certificates based on information received from the RA and from the certification request from the key generation system associated with the central storage entity.

All communication between the central storage entity and the certification authority 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 to central storage entity;
4. 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.

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 makes the information available to the RA, which then notifies the subject of the issuance of a new BankID certificate.

The bank is responsible for issuing two-factor authentication mechanisms to persons who are approved to be certificate holders.

For Bankenes ID-tjeneste: The subject will receive a notification that the BankID Initial Activation code have been distributed. The Initial Activation code is an automatically generated password available to no other which will have to be changed on first use of the Personal BankID, and is sent in one channel (SMS or e-mail). A notification of the password distribution is sent in the other channel. Contact information used in the distribution and notification are fetched from the Customer Ledger.

For Danske Bank: No additions.

For DNB: The issuer informs the RA/Bank RA that a certificate has been issued. The RA shall, in turn, inform the certificate holder.

For Eika: When the customer has received both the activation mechanisms and completed the login to the online bank for the first time after having changed the first-time BankID password, it will be implicitly clear for the customer that Personal BankID has been generated. The customer can now go to Vipps AS' web page – www.bankid.no – and test Personal BankID there. The user can also use tools to see the certificate contents here.

As described in sub-chapter 4.2.1 – Performing identification and authentication functions – the bank will issue the appropriate two-factor mechanisms to the BankID customers.

For Nordea: Issuance of BankID at the branch office is enabled instantly.

For SpareBank 1: No additions.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The issuer shall inform the RA bank that the certificate has been generated. The RA bank in turn is responsible for informing the subject. The bank may choose to let the issuer of BankID notify the subject directly.

The RA Bank shall request, in the provided contractual material [20], that the subject tests the use of the issued BankID on the BankID's tools page.

The certificate applicant has indirectly accepted BankID and certificates when:

- An agreement has been entered into, electronically or in writing. If the agreement is in electronic form, it should be signed with an Advanced Electronic Signature or Advanced Electronic Seal.
- The certificate has been generated, and the personal customer has begun using it.

The person thereafter has the status of BankID subject.

For Bankenes ID-tjeneste: When the subject have changed the Initial Activation code to Activation Data of his own choice and uses a One-Time Code from the Possession Element, those actions constitutes acceptance of the certificate and the subject will have access to keys in the central storage.

For Danske Bank: No additions.

For DNB: This is done by sending the certificate applicant a message after the order has been placed, stating that the subject needs to activate the Personal BankID by using it to log onto the Internet banking service. At the end of the application process, the subject is informed that the BankID certificate has been issued and will be ready for use when the BankID status in the Internet banking service shows that the customer's bank ID has been activated.

For Eika: See sub-chapter 4.3.2 – Notification to subscriber by the CA of issuance of certificate.

The order process for BankID in the banks affiliated with Eika Gruppen requires that the customer participate actively in the process. The certificate applicant accepts the BankID agreement explicitly, and he or she has also indirectly accepted BankID and certificates when:

- The certificate has been generated, and the personal customer has begun using it.

The person thereafter has the status of BankID subject.

For Nordea: No additions.

For SpareBank 1: No additions.

4.4.2 Publication of the certificate by the CA

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

The complete and accurate certificate is also available to the subject in the BankID client used for normal operation.

4.4.3 Notification of certificate issuance by the CA to other entities

Not applicable.

4.5 Key pair and certificate usage

BankID has different key pairs for authentication and signing.

4.5.1 Subscriber private key and certificate usage

For authentication certificates; NonRepudiation(1)/DigitalSignature(0)/KeyAgreement(4) is used.

For signing certificates; Non-repudiation(1) is used.

4.5.2 Relying party public key and certificate usage

For authentication certificates; NonRepudiation(1)/DigitalSignature(0)/KeyAgreement(4) is used.

For signing certificates; Non-repudiation(1) is used.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

Routine renewals require a certificate re-key.

The RA and TSP shall keep track of expiration dates for Personal BankIDs and Employee BankIDs. When there are less than a specified number of days left until the BankID expires, the issuer of BankID shall ask the service provider to flag these for renewal in the central storage entity.

The renewal will be instigated when the subject next uses the flagged BankID. This shall take place during the dialogue with the subject. The actual renewal will not noticeably delay the use of the keys, and will ordinarily not be noticed by the subject.

Upon renewal, the subject can continue using the same activation data (password and authentication device).

In case of manual renewal (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).

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.

For Bankenes ID-tjeneste: Certificates are set for renewal up to 63 days before expiry, or when a change in customer data (typically a name change) requires it. Renewal is performed upon the next use of the certificate. Notification of pending renewal is sent to the subject.

For Danske Bank: Danske Bank has a notification system, which would inform the service provider to flag any certificate up for renewal in 90 days.

For DNB: The TSP sends a reminder by SMS or by letter 90 days prior to certificate expiring. The reminder includes information about how to renew certificate.

For Eika: Personal BankID certificates to be renewed are marked in the central storage unit in BankID COI. This happens by Eika Gruppen's BankID system sending a message to BankID COI, flagging all BankID to be renewed. In this process Eika also checks the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject are still valid. Routine renewals also involve key changeover.

The renewal will be instigated when the subject next uses the flagged BankID. When renewing, the customer can keep the same activation data as before (static BankID password and OTP unit). If there are changes to the information in a certificate, e.g. name, Eika will submit a renewal notification to BankID COI.

If the subject does not renew the certificate before the expiration date, BankID will be revoked. To be issued with a new BankID after a revocation like this, the same procedures as for renewal after revocation must be followed.

For Nordea: Nordea RA systems routinely checks with the order and distribution system at the central storage entity, which certificates are about to expire the following 90 days.

For SpareBank 1: The RA system does a periodic search for active BankID's and flag the ones that expire in the next period according to the description above. The certificate holder is notified close 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.

For other renewal purposes requested by the end user or the RA the reissue function for renewal is used, i.e. for certificate content modification or password change.

4.6.3 Processing certificate renewal requests

The renewal process at the CA-system consist of these elements:

- Generation of new key pair
- Certification of new public key
- Revocation of certificate with old keypair

4.6.4 Notification of new certificate issuance to subscriber

After renewal is requested from the RA to the CA, the renewal process will be processed by the CA in real-time the next time the end user invokes usage of the private key. The end user is informed about the renewal in the dialogue.

4.6.5 Conduct constituting acceptance of a renewal certificate

The end user may abort the renewal process in the BankID dialogue. If not aborted this constitutes acceptance of a renewal of the certificate.

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.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Ordinary re-key is performed as part of the renewal or reissue process.

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 Personal BankID or an Employee BankID with new information from the RA. For Employee BankIDs, changes can also be made if there are changes in a Subject's relationship with the Subscriber (department, etc.).

For this, the RA reissue function is used. The reissue function will generate a new certificate with changed content and a new key pair.

The banks have access to the National Registry 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, end user or the enterprise (for EmployeeBankID) may request certificate modification.

4.8.3 Processing certificate modification requests

The renewal process at the CA-system consist of these elements:

- Collection of updated certificate details from the RA
- Creation of certification request
- Generation of new key pair
- Certification of new public key
- Revocation of certificate with old keypair

4.8.4 Notification of new certificate issuance to subscriber

For Bankenes ID-tjeneste: This is done by sending the certificate applicant a message after the order has been placed, stating that the certificate applicant needs to activate BankID by using it to log onto the Internet banking service. At the end of the ordering process, the subject is informed that the BankID certificate has been issued and will be ready for use when the BankID status in the Internet banking service shows that the customer's bank ID has been activated.

For Danske Bank: No additions.

For DNB: This is done by sending the certificate applicant a message after the order has been placed, stating that the certificate applicant needs to activate BankID by using it to log onto the Internet banking service. At the end of the ordering process, the subject is informed that the BankID certificate has been issued and will be ready for use when the BankID status in the Internet banking service shows that the customer's bank ID has been activated.

For Eika: No additions.

For Nordea: The customer must notify Nordea of any changes to the information provided at the time of registration: personal data, residence, telephone numbers, email address, etc. where changes impacts on certificate contents, a new certificate will be issued according the re-key procedure.

For SpareBank 1: When a certificate is issued, the subscriber is notified by either e-mail or SMS.

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 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 customers (subjects and enterprises) access to a service where they may request that their BankID is invalidated. This service is 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.

Requests for invalidation is made to the bank acting as RA where the subject ordered the 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.

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. This shall contain all invalidated (revoked and suspended) certificates. Expired certificates can be removed from subsequent lists.

The TSP generates an updated revocation list at least once per hour and immediately make 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.

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

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.

4.9.1 Circumstances for revocation

Certificates are 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 or stolen activation data;

- Known misuse of a certificate;
- The subject has changed their name;
- The subject is no longer entitled to have a certificate;
- PersonBankID: The subject terminates their customer relationship with the bank;
- EmployeeBankID: the subject is no longer entitled to have a certificate (e.g. their employment relationship has ended or their authorisation has changed);

EmployeeBankID: The subscriber terminates their customer relationship with the bank.

4.9.2 Who can request revocation

The following can request revocation:

- Subject;
- The enterprise the subject is employed by or acts on behalf of (in the case of EmployeeBankID);
- The bank that has entered into an agreement with the customer (with the subject or enterprise about EmployeeBankID);
- Registration Authority;
- Issuer of BankID.

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

For Bankenes ID-tjeneste: 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.

Another operator or body may request revocation. Another operator or body may be the police, Nordic Financial CERT, BID, Bits AS, Nets, Finance Norway or another RA.

For Danske Bank: No additions.

For 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.

For Eika: Certificates from Eika Gruppen must 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 or stolen activation data;
- Known misuse of a certificate;
- The subject has changed their name;
- The subject is no longer entitled to have a certificate;
- Person BankID: The subject terminates their customer relationship with the bank;
- Employee BankID: The subject is no longer entitled to have a certificate (e.g. their employment relationship has ended, or their authorisation has changed);
- Employee BankID: The subscriber terminates their customer relationship with the bank.

For Nordea: No additions.

For SpareBank 1: No additions.

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.

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.

For Bankenes ID-tjeneste: Requests for revocation of a Personal BankID may be sent or justified in the following ways:

- The subject may send the request by letter, fax or a scanned, signed document sent by e-mail. The signature will be verified against signatures already in the RAs possession.
- The subject may request revocation by personal attendance at the RA's premises.
- The subject may terminate his relationship as customer in which case the certificate will be revoked automatically by the RA.
- Another operator or body may request revocation. Another operator or body may be the police, Nordic Financial CERT, BID, Bits AS, Nets, Finance Norway or another RA.

Reasons for the request for revocation are registered/archived. Signed requests are sent to the Certificate Authority system and the Certificate Validation System and the RA application is updated with the certificates "revoked" status. The RA-application logs and archives all events for 10 years.

For Danske Bank: Certificate owner can submit revocation request through Danske Bank self service systems where authorisation is verified via the relevant BankID based authentication (2 Factor).

The certificate owner could also call Danske Bank customer support to submit revocation request where authorisation is verified via the set of Secret Question answers. Another operator or body may request suspension. Another operator or body may be the police, Nordic Financial CERT, Bits AS, Nets, Finance Norway or another RA.

For DNB: The TSP has a 24/365 invalidation/blocking service. The TSP must notify the service provider as soon as there are grounds for revoking a certificate. The contents of the notification message are validated, and the sender is thereafter validated in the certification authority system. Once the message has been validated, the certificate is revoked in the certification authority system and a signed message is immediately sent to the certificate validation service stating that the status of the certificate has been changed. In addition to the real-time message which includes the revocation details for the individual certificate, a signed Certificate Revocation List (CRL) is sent from the certification authority system to the certificate validation service once an hour.

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. This is done by means of continuous status checking from the Registration Authority's side of the certificate authority system (i.e. from the registration application). The bank shall subsequently inform the subject that the BankID has been revoked.

The subject may request revocation of his/her BankID by going in person to a bank branch office or over the telephone. The bank has special standard procedures for handling such requests. If the subject goes to a branch office, he/she must show valid proof of identity. If the subject contacts the bank by telephone, he/she must go through an enhanced customer identity checking process in Customer Service to verify his/her identity and

establish/authentic that he/she is the correct certificate holder. In general terms, this entails answering a number of more complex questions related to different sets of underlying data. Keeping a log is one of the requirements stipulated in the standard procedure.

The bank always sends the subject written confirmation of revocation. The channels that are used to confirm revocation are: eDialog ('electronic dialogue') in the Internet banking service, regular mail, SMS and email. The bank logs and stores all requests for revocation. A message is always sent in eDialog. The customer adviser must also select an additional channel for notification. All requests for revocation are logged and stored by the bank.

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.

If a customer asks for suspension of his BankID, the bank will do this after only asking for the customer's national ID number.

If a bank in Eika Gruppen is unable to maintain its obligations to other participants in the BankID partnership, Eika Gruppen uses own routines in combination with routines from Vipps AS and Finance Norway for invalidating all certificates for the bank and its customers.

When the RA bank is informed about a possible compromise of any BankID, the BankID or BankIDs in question will be immediately suspended and later on revoked.

When a BankID certificate is suspended or revoked, Eika Gruppen will send a message about this to the customer to confirm the suspension.

For Nordea: No additions.

For SpareBank 1: The subject may also request for revocation by phone and has to answer a number of security questions if done so.

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 chapter 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 relying parties.

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

Not applicable.

4.9.13 Circumstances for suspension

The CA-system supports time-limited suspension with the same requirements as for revocation.

All conditions sufficient for revocation are also sufficient for suspension. Additionally, notification by phone to bank or CA, or by unsigned request, is accepted. Suspension may be initiated when the subject asks for revocation, but cannot present sufficient evidence of ownership to have BankID revoked.

4.9.14 Who can request suspension

The following can request suspension:

- Subject;
- The enterprise the subject is employed by or acts on behalf of (in the case of EmployeeBankID);
- The bank that has entered into an agreement with the customer (with the subject or enterprise about EmployeeBankID);
- Registration Authority;

- Issuer of BankID;
- Any other person related to the subject

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

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.

The bank 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 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.

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.

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 Danske Bank: Certificate owner can submit suspension request through Danske Bank self service systems where authorisation is verified via the relevant BankID based authentication (2 Factor).

The certificate owner could also call Danske Bank customer support to submit suspension request where authorisation is verified via the set of 5 Secret Question answers.

For DNB: Suspension is rarely used, and then only in special cases where establishing new confidential items or revoking/cancelling the BankID are not viable solutions. All requests for invalidation/suspension are logged by the bank. To open a suspended BankID, the subject must appear in person so the bank can check his/her identification. Sometimes, as an exception, the subject may reactivate the BankID over the telephone subject to enhanced identity checking. In general terms, this entails answering a number of more complex questions related to different sets of underlying data. Keeping a log is one of the requirements stipulated in the standard procedure. If the suspension period for a certificate exceeds 30 days, the certification authority system will revoke the suspended certificate and store the relevant information in a central database. The system supports reopening suspended BankID certificates within the 30-day suspension period.

Keeping a log is one of the requirements stipulated in the standard procedure. The TSP logs and stores all requests for suspension.

For Eika: The certification authority system supports time-limited suspension with the same requirements as for revocation. 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 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 uses a service provider for the suspension.

Eika sends a response to the customer to confirm the suspension.

For Nordea: Nordea assures a suspension service: for urgent requests, due to theft, loss or breach of security, by telephone with a customer service (+47 2320 6001) available around the clock on all business days and holidays; in other cases, the service is available during office hours (8.xx-16.xx).

For urgent suspension requests, the subject, at the request of the operator, must prove his or her identity and give the pass-phrase received with certificates. Where the identity of the person submitting the request is not established, the certificate will be suspended on a precautionary basis.

For SpareBank 1: The subject may also request suspension by phone and has to answer a number of security questions if done so.

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.

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 service provider of the CA and central storage entity 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 EmployeeBankID requested status for
- The associated BBAN account number of the Person- or EmployeeBankID requested status for
- The organisation number from the national number of enterprises of the Employee- or MerchantBankID 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.

4.12 Key escrow and recovery policy and practices

The server based solution is backed up to another site and the only duplicate of the Subscriber's keys are located here. Both original and duplicated keys will be deleted on expiration/revocation of certificate.

4.12.1 Key escrow and recovery

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

Private keys (authentication and signing keys) for PersonBankID and EmployeeBankID are used in a server based solution. The keys are generated in a FIPS 140-2 level 3/4 certified HSM and exported from the HSM as a cryptogram for operational purposes, e.g. load balancing. The encrypted private keys are not usable or readable outside the HSMs with the key material needed to decrypt and use the key.

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 service provider.

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 Service Provider 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).

For Bankenes ID-tjeneste: 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.

Logical access are usually given to two persons jointly. Communication between RA-application and COI are secured and signed. Archival and storage solutions for backups and distribution media that are sufficient to prevent loss, falsification or unauthenticated use of information, and to conform to requirements for archiving, are in place.

For Danske Bank: For the RA system documented and approved procedures are in place that detail physical and logical access controls to data. Access to the Group's internal production and test systems, customer orientated systems, network components and external systems must be obtained via an access control system checking user authenticity. All entrances are furthermore covered by CCTV. Twice a year System Managers receive lists showing all system access users in their area and what authorisations the users have. The System Manager is responsible for confirming that staff have the correct access.

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. The Registration Authority (RA) complies with the rules in the requirement document issued by Bits AS. To ensure such compliance, the banks go through Bits AS's quality control process and are otherwise monitored by means of compliance audits of CPS every three years.

Corporate information security requirements are the TSP's requirements for information security. The requirements are given in accordance with Group guideline for information security, and will be elaborated in standards and/or internal quality control system where applicable. Corporate information security requirements expresses requirements that should be followed across the Group. If requirements concerning

information security are given elsewhere, for instance in regulations or directives, the strictest requirements apply. The information security requirements are based on internationally recognized information security standards.

For Eika: Physical security barriers and controls are established to control access to Eika Gruppen's BankID solution and associated systems.

The security information associated with CA and RA and issued to Eika Gruppen in connection with the key ceremony in BankID COI, is physically protected and securely stored according to the internal routines of Eika Gruppen. Eika is of the opinion that these routines are sufficient to prevent loss, forgery, or unauthorised use of stored information.

For Nordea: No additions.

For SpareBank 1: Physical security barriers and controls are implemented to control access to the registration authority system hardware and software. All physical access to these areas is logged.

5.1.1 Site location and construction

For the CA-system and central servers and storage equipment

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

For the CA-system and central servers and storage equipment

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 Service Provider. 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 data centers. 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 personell only. Both certified personell 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 simoultanisly and enter their personal PIN codes in order to enter the room. Once inside the room both certified personell 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 personell are alerted. Both the KeyWatcher and the security room are monitored 24/7 by cameras. Logs are regulary reviewed by the security officer.

All visitors has to be authorized by personell that are responsible for physical access to the data center, 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 personell 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 personell accompanying them. The visitor is accompanied until checking out and leaving Nets premises.

For Bankenes ID-tjeneste: For the RA-Applications used by the RAs, access to secure zones are governed by strict access controls and procedures for physical and logical Access and is only available for properly authorized personell.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: 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. Access rights and user roles are defined for each zone. 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.

For Nordea: Located outside the PKI premises are the components that interoperate both with Nordea network and with Internet, and the workstations to record users' credentials, and to submit requests to CA. The workstations for the approval of the certificates issue requests do not require a physical security level higher than that of normal workstations.

For SpareBank 1: Only authorized personnel have access to the data center where the registration authority system hardware and software are located. All access to these areas is logged. Operations of the HSM's demands multiple people present.

5.1.3 Power and air conditioning

For the CA-system and central servers and storage equipment

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: No additions.

For Nordea: The data centres of Nordea have redundant systems. The air-conditioning systems regulate temperature and control humidity. 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 centers have air conditioning system, Uninterruptible Power Supply and backup power generator.

5.1.4 Water exposures

For the CA-system and central servers and storage equipment

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

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: No additions.

For Nordea: No additions.

For SpareBank 1: For the RA system: Data centers are protected from water and both datacenters can operate alone in case the other one is unavailable.

5.1.5 Fire prevention and protection

For the CA-system and central servers and storage equipment

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

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: No additions.

For Nordea: The fire prevention and protection system is composed by a smoke detection system and a fire suppression system.

For SpareBank 1: For the RA system: Both data centers have automatic fire alarm and fire extinguishing systems.

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

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 authorized 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

For the CA-system and central servers and storage equipment

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

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

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

For Nordea: No additions.

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

5.1.8 Off-site backup

For the CA-system and central servers and storage equipment

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.

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 Danske Bank: No additions.

For DNB: No additions.

For Eika: Backup systems ensure continued operation in cases of disruption. The security for dualised solutions is the same as the security for regular production solutions.

Backups are stored under the same security regimen 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 centers 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) Security officer: Overall responsible for administering the implementation of security policy and practices which falls within the specific services delivered; 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:

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.

Personell 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 this position is very sensitivity 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

For the CA-system and central servers and storage equipment

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 service provider (both permanent and temporary) shall have job descriptions designed from the view point 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.

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.

BID 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 BID'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 Danske Bank: Danske Bank requirement for the administration of RA keys is as follows:

- Access to crypto facilities, functions, keys, etc. involves two people entering the crypto room together, and two people logging in and operating the crypto equipment together.
- Crypto equipment is located in physically locked premises that require two key officers together.
- Logical access to the crypto function requires two key officers together.
- Key generation always requires two key officers together.
- The administration of keys must be logged.

No single person must be in possession of the original key:

- If keys are to be printed out for split storage, a key holder must be present for each part into which the key is split.
- When media or components that may contain secret keys are to be destroyed, at least two trusted people must be present to ensure that the destruction is done correctly.

Changes to the RA programme must comply with the bank's standard for change control.

For DNB: No additions.

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 and present evidence of identity including “something they know” and “something they have”.

The roles in sub-chapter 5.2.1 – “Trusted Roles” – are staffed and documented in Eika’s BankID routines. Backup roles are also defined for them, in cases of absence.

Eika Gruppen has in its possession CA and RA security elements that have been issued by BankID COI under the key ceremony for CA and RA issuance for the various RA banks (Registration Authorities) associated with Eika. Handling of such CA and RA security elements are regulated and documented through various routines at Eika. The routines require at least two persons being involved in all handling of CA and RA security elements associated with the BankID system itself.

Destruction of CA and RA security elements at Eika are regulated by internal routines, and when these are to be disposed of, at least two trusted persons will be present to ensure that the destruction is in accordance with regulations.

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 Nordea: 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 service provider (both permanent and temporary) shall have job descriptions designed from the view point 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 initialization 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.

For SpareBank 1: The TSP has the following practices:

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

5.2.3 Identification and authentication for each role

For the CA-system and central servers and storage equipment

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 authorized 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 service provider 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.

For Bankenes ID-tjeneste: BID, 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 personell involved.

Trusted roles will be held by personell with required qualifications.

For Danske Bank: There is authorisation control for all of the Danske Bank RA-systems. This is done via the banks authorisation system, which, in interaction with authorisation control mechanisms in the respective systems, ensures that only authorised staff have access to the systems. All authorisations are granted by management and review yearly.

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 such a responsibility, 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 Nordea: No additions.

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

For the CA-system and central servers and storage equipment

The service provider 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

For Bankenes ID-tjeneste: BIDS CA keys are stored in a safe with two person access and only used for key ceremonies at the COI. The RAs keys are stored in securely managed HSMs at the RA Application providers.

BID, RAs and RA-application providers have procedures for granting, maintaining and monitoring access to critical resources. Such controls are also a matter of national regulations for the delivery of financial services.

For Danske Bank: No additions.

For DNB: No additions.

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 Nordea: See section 5.2.1.

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 authorized trusted roles, solid PKI and BankID expertise. All personnel at the service provider are employed for at least 6 months and given proper training before they can access the certification authority systems.

Nets 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 Nets has specific training for new employees or consultants.

For Bankenes ID-tjeneste: Requests for Personal 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 a bank and audited internally, as well as through audits by Finanstilsynet,

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

For Danske Bank: RA IT system: Danske Bank eBusiness Security department is primarily staffed with personnel who have expert knowledge, experience and qualifications from experience and secondarily staffed with personnel who have acquired the knowledge through formal training.

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 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. There are also semi-annual gatherings within both Payment and IT, where current issues are presented to the banks' Payment managers and IT managers respectively.

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

See also sub-chapter 5.2.1 - "Trusted roles".

For Nordea: The same practices applies for the RA.

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

5.3.2 Background check procedures

The service provider will always check job-seeker references. Personnel working with the CA or "archive management and information security systems" will always be subject to a security meeting conducted at the start of the assignment and then annually.

The service provider 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.

For Bankenes ID-tjeneste: RA Officers at the RAs are subject to the same practices, and are given training in advance of access to the RA functions, as well as a yearly refresh of procedures and practices.

For Danske Bank: RA IT System: Danske Bank personnel have a defined job description and appropriate roles assigned in order for them to perform their specific tasks based on a need to know and least privileged principle as well as segregation of duties. All employees are required to perform an annual awareness training. TSP specific functions in form of a security administration, operation and audit including cryptographic key management requires additional training and awareness.

For DNB: Employees must not have other tasks that could conflict with the obligations and responsibilities that follow from their roles relating to the issuance of BankIDs through the relevant Registration Authority. In addition the TSP's guidelines for HR and recruitment applies.

For Eika: Eika Gruppen performs certain background checks of people that apply for employment.

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

For Nordea: The same practices applies for the RA.

For SpareBank 1: For hiring ordinary routines and guidelines at the TSP is used. New employees are background checked.

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 Nets 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.

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 Danske Bank: RA IT System: Danske Bank eBusiness Security department is primarily staffed with personnel who have expert knowledge, experience and qualifications from experience and secondarily staffed with personnel who have acquired the knowledge through formal trainings.

All employees are required to perform an annual awareness training. TSP specific functions in form of a security administration, operation and audit including cryptographic key management requires additional training and awareness.

Information security training is provided to all the employees in the Group. Information security awareness eLearning covering topics such as phishing, social engineering, confidential information, malware, identity theft, cloud services, etc. is mandatory for all the employees. More specific security awareness training for relevant roles like advisors, workstations administrators, etc. is provided to the specific employees. Phishing tests are performed regularly to improve the awareness of the employees. The training material is reviewed regularly to keep it relevant and up to date.

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. There are also semi-annual gatherings within both Payment and IT, where current issues are presented to the banks' Payment managers and IT managers respectively. The employees also receive continuing training and competence maintenance relating to how the need is evaluated from case to case.

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

See also sub-chapter 5.2.1 - "Trusted roles".

For Nordea: The same practices applies for the RA.

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 involve 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 month to establish continuity and updates in the knowledge of the personnel and procedures.

For Bankenes ID-tjeneste: Cf. 5.3.2.

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

All Danske Bank employees are required to perform an annual awareness training. TSP specific functions in form of a security administration, operation and audit including cryptographic key management requires additional training and awareness.

For DNB: Periodic training updates will be carried out to establish continuity and updates in the knowledge of the personnel and procedures.

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. There are also semi-annual gatherings within both Payment and IT, where current issues are presented to the banks' Payment managers and IT managers respectively.

See also sub-chapter 5.2.1 - "Trusted roles".

For Nordea: No additions.

For SpareBank 1: All BankID personnel work with BankID on a daily basis.

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.

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

For Danske Bank: No additions.

For DNB: No additions.

For Eika: 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.

For Nordea: The same practices applies for the RA.

For SpareBank 1: There is no formal job rotation scheme deployed for personnel in trusted roles. 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 service provider 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.

For Bankenes ID-tjeneste: The same practices applies for the RA.

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

Danske Bank personnel have a defined job description and appropriate roles assigned in order for them to perform their specific tasks based on a need to know and least privileged principle as well as segregation of duties.

For DNB: No additions.

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 Nordea: The same practices applies for the RA.

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 Nets security framework and Secure SDLC. In addition there is a separate review of NDA with consultants and employees.

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 Danske Bank: No additions.

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. Contract staff may be subject to the same sanctions as employees in the event of violation of instructions.

For Nordea: The same practices applies for the RA.

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 service provider's premises. Personnel employed by the bank, registration authority, issuer, Vipps AS, Bits AS or the service provider who legitimately need to know, can be granted permission to read these documents in areas approved by Service Provider, provided they sign a non-disclosure agreement.

5.4 Audit logging procedures

For the CA-system and central servers and storage equipment

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 personell can access the information. All access to this information are requested and logged in Nets Change management system.

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 Danske Bank: RA IT System: In Danske Bank, all [orders](#) between the RA and the issuer system are logged in protected DB2 tables. Access to the tables are controlled by the FT system. Only employees with a job-related need have access to the logs.

In addition, following events are monitored:

- Startup and Shutdown are monitored and alerts are generated.
- Availability and Utilization are part of standard operational monitoring

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. OTP validations are also logged. 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.

For Nordea: *No additions.*

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

For the CA-system and central servers and storage equipment

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 service provider for the central servers and storage.

- 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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

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. OTP validations are also logged.

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.

As issuer of BankID Eika Gruppen owns a CA in BankID COI. In connection with the initial key ceremony and later key ceremonies various keys and other security elements were issued to Eika. These keys and security elements have been delivered to Eika Gruppen's key custodian, so accordingly Eika has in its possession various security elements associated with CA – Eika Gruppen's role as TSP issuing BankID. Each of these security elements is stored safely and any changes in their storage or usage is logged.

For Nordea: *No additions.*

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

For the CA-system and central servers and storage equipment

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 CAO by an authorized operator. All archived logs are kept in 2 separate secure room in two separate datacenters 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.

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 Danske Bank: In Danske Bank, the audit logs are created in real time and are automatically monitored for abnormal incidents in real time. Any abnormal incidents are reported via notification/alarm to Danske Bank 24-hour monitoring centre. The centre then contacts the relevant departments/people at Danske Bank.

For DNB: No additions.

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 revisioned in a traceable manner.

For Nordea: For the RA bank systems the following applies:

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

For SpareBank 1: No additions.

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

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.

All audit logs and log information 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.

Logs of status modifications to the certificate are stored for 10 years. Backup are normally also stored for 10 years.

For Nordea: No additions.

For SpareBank 1: No additions.

5.4.4 Protection of audit log

For the CA-system and central servers and storage equipment

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 datacenters inside corresponding secure rooms, and all access to them is monitored and logged.

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

For Danske Bank: No additions.

For DNB: No additions.

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 Nordea: No additions.

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

For the CA-system and central servers and storage equipment

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 center.

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

For Danske Bank: No additions.

For DNB: No additions.

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 Nordea: No additions.

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)

For the CA-system and central servers and storage equipment

The audit collection system is internal.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: See sub-chapter 5.4.5 – Audit log backup procedures.

For Nordea: Nordea uses internal SIEM tool as collection system for the RA-system audit logs.

For SpareBank 1: The RA Audit collection system is internal.

5.4.7 Notification to event-causing subject

For the CA-system and central servers and storage equipment

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 service provider 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 service provider 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 service provider keep record 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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: Vulnerability assessment is part of the annual 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 Nordea: No additions.

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

For the CA-system, central servers and storage equipment

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;
- Issued Certificates;
- Agreements about certificates and protection of keys and activation data;
- Renewals of certificates and associated messages;
- History of key changeovers on certification authority system;
- Invalidation requests (revocation or suspension) with associated messages;

Current TSPS and expired policies and CPSs.

RA are the part with direct customer (subscriber) contact, and responsible to keep the following records:

- The subjects identity, see section 3.2.3
- The subscriber agreement

For Bankenes ID-tjeneste: For the RA-application, see section 5.4.1.

For Danske Bank: Danske Bank stores and archive following records

- An electronic copy of the signed agreement in the customer folder.
- All orders between the RA and the issuer system
- An electronic copy of the signed agreement in the customer folder.
- All incidents between the RA and the issuer system
- All operations in relation to the OTP validator

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.

As issuer of BankID Eika Gruppen owns a CA in BankID COI. In connection with the initial key ceremony and later key ceremonies various keys and other security elements were issued to Eika. These keys and security elements have been delivered to Eika Gruppen's key custodian, so accordingly Eika has in its possession various security elements associated with CA – Eika Gruppen's role as TSP issuing BankID. Each of these security elements is stored safely and any changes in their storage or usage is logged.

For Nordea: No additions.

For SpareBank 1: No additions.

5.5.2 Retention period for archive

Archived 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 Chapter 5.1.6 for at least 10 years. There are 3 copies of the media, 2 kept at the Service providers 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. UniCERT 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 CAO by an authorized operator.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: In Danske Bank, the logs are kept for the present year + 10 years. The logs are stored securely and may be made available for consultation within a reasonable time.

For DNB: No additions.

For Eika: All archives are stored according to legal requirements in the BankID regulations or Norwegian law.

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. Backup are normally also stored for 10 years.

For Nordea: No additions.

For SpareBank 1: No additions.

5.5.3 Protection of archive

For the CA-system and central servers and storage equipment

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

For Bankenes ID-tjeneste: See 5.4.4.

For Danske Bank: No additions.

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 Nordea: No additions.

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: See sub-chapter 5.5.3 – Protection of Archive.

For Eika: See sub-chapter 5.5.3 – Protection of Archive.

For Nordea: No additions.

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

5.5.5 Requirements for time-stamping of records

Not applicable

5.5.6 Archive collection system (internal or external)

For the CA-system and central servers and storage equipment

The records archival system is internal.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: See sub-chapter 5.5.3 – Protection of Archive.

For Nordea: No additions.

For SpareBank 1: The records archival system is internal.

5.5.7 Procedures to obtain and verify archive information

For the CA-system and central servers and storage equipment

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: 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.

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.

Only specific employees at the ICT Operations service providers have access to retrieve backup tapes at a later point.

If the TSP terminates, the logs will be preserved in a readable way for as long as Eika Gruppen's legal requirements are still valid.

For Nordea: No additions.

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 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 service provider keep a track record of all key validities and organise key generation of Root-CA keys and Level 1 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-CAs 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 Netcentric PersonBankID and EmployeeBankID are valid for a maximum of 2 years and must be renewed before they expire.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

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 warning. 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.

If the private key of an issuer has been compromised, the service provider 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 issuer's private key will thereafter be declined by the certificate validation service. Root-CA will also revoke the issuer's certificate:
2. Issuers shall immediately inform all registration authorities, subjects and other issuers of the incident:
3. Key changeover for the issuer shall take place in accordance with the CP/CPS for Root-CA [16]:
4. The registration authority must flag all Personal BankIDs and Employee ankIDs 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.

In case of suspicion that an issuer has been compromised, there are procedures for temporarily withdrawing BankIDs issued by the relevant issuer. If the issuer turns out to have been compromised, the procedure at the top of this section shall be followed.

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.

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.

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.

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.

For BID: No additions.

For Danske Bank: Local IT Managers are part of the incident escalation communication and therefore have possibility and responsibility for reporting and escalating incidents.

The agreed response time for internal technology support for priority 1 cases is within 15 minutes. Priority 2, 3 and 4 cases within 4 hours. However, during working hours this will be likely to be less. In regards to external software suppliers the response time is up to 2 hours.

Security incidents regarding compromise, fraud and abuse of Personal BankIDs is shared to Nordic Financial CERT. link to Nordic Financial Cert <https://www.nfcert.org/>

For Eika: No additions.

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

For the CA-system and central servers and storage equipment

All essential software and information is 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.

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 Danske Bank: No additions.

For DNB: No additions.

For Eika: All systems data necessary to resume CA and RA operation are backed up regularly and stored safely. Backups are stored under the same security regime as the production environment.

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 dualised, so that the backup systems will ensure continued operation in cases of disruption.

The physical security for dualised solutions is the same as the security for regular production solutions.

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 clients within 24 hours the incident occurs.

For Bankenes ID-tjeneste: Key compromises of RA private keys or BID keys will lead to mass revocation and subsequent reissue of certificates. In such cases the RA, BID and Service Providers will:

- Ensure that certificates under the compromised key will be rendered invalid for use
- Prepare for issuance of new certificates
- Report certificates issued under the compromised key for revocation.

After revocation there must be a new issuance of all Person BankID.

For Danske Bank: If a customer credential is compromised for which Danske Bank is the RA, revocation procedures shall be followed.

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

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

For Eika: 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.

Eika Gruppen has developed a continuity and disaster recovery plan for BankID that describes the actions Eika, in the role of CA (Certification Authority), will take in a continuity situation occurring if BankID is compromised. The plan also describes the preparedness Eika has in relation to disasters that can strike their BankID solution. The plan further deals with how Eika Gruppen and user banks will perform measures associated with the individual banks' role as RA (Registration Authority) under Eika's CA.

This plan address any compromise, loss or suspected compromise of a CA's private key as a disaster.

For Nordea: No additions.

For SpareBank 1: No additions.

For the subject

The subjects' private keys are protected by multiple layers of encryption, including an individual encryption key. Due to the nature of the key encryption regime one key pair cannot be compromised as such. Only the credentials, in that case revocation procedures shall be followed. If the encryption technique for all keys are compromised, disaster and recovery procedures shall be followed, including TSP or mass revocation process.

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 banks and banking groups, Finance Norway and Bits AS.

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

For the CA-system and central servers and storage equipment

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

For Bankenes ID-tjeneste: Procedures are in place to restore from backup in case of disaster. In case of compromise, restore is done from trusted backup from before compromise.

For Danske Bank:

- As soon as Danske Bank is made aware, via internal or external channels, about a disaster (e.g. CA certificate may be compromised), an employee from Group Service Centre department creates an incident with the priority 'critical' in Danske Bank's incident management system
- Danske Bank suspends its CA certificate at NETS. When Danske Bank's CA certificate is blocked, no BankID certificates issued by Danske Bank can be used at its own or others' BankID user locations.
- Danske Nettbank will not be running, customers is advice to use the Mobile Banking solution,
- Danske Bank's customers are informed via the proper channels.
- A root cause analysis is initiated.
- The establishment of a new CA certificate is implemented.
- Danske Bank's customers are informed.
- New BankIDs are created for all of the bank's sites
- Danske Nettbank returns to ordinary operation.
- Customers can use the 'BankID administration' service on Danske Bank's website to create a new BankID.

Several of these processes will take place in parallel to achieve the fastest possible reaction time

For DNB:

The TSP's IT Continuity and Disaster Recovery Plan is the overarching tool for managing situations that result in severe reductions of the service level and the delivery of IT services in the TSP. The IT Continuity and Disaster Recovery unit is part of a four-part continuity and disaster recovery management organization in the TSP. The Disaster Management team for IT outages in the banking operations (Bank crisis management) is the strategic management team during crises of a grave and/or enduring nature. The IT Continuity and Disaster Recovery team is the bank's operative disaster management team in the event of a full outage or strong reduction of IT operations. The head of IT serves as the liaison with the affected business and support areas and their continuity management teams. The individual business and support areas have their own continuity organizations and continuity plans that focus on business continuity, i.e. continuing production using available solutions, including backup operation system solutions as well as manual solutions. The Group Emergency Preparedness Management takes precedence over the bank's Disaster Management Team in the event of IT outages in the banking operations.

The emergency preparedness management team largely deals with disasters entailing a risk to life and limb and is responsible for coordinating efforts on the Group level.

Procedures are in place to restore from backup in case of disaster. In case of compromise, restore is done from trusted backup from before compromise. The disaster recovery plan are documented in internal TSP document "Disaster recovery plan for compromised CA-Keys of BankID"

For Eika: 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.

Eika Gruppen has developed a continuity and disaster recovery plan for BankID that describes the actions Eika, in the role of CA (Certification Authority), will take in a continuity situation occurring if BankID is compromised. The plan also describes the preparedness Eika has in relation to disasters that can strike their BankID solution. The plan further deals with how Eika Gruppen and user banks will perform measures associated with the individual banks' role as RA (Registration Authority) under Eika's CA.

When it comes to technical operation with appurtenant catastrophe handling associated with re-establishing software and hardware and restoring data, both Eika and the bank's service providers for IT operations has established continuity plans. Actions in connection with this are also incorporated into the agreement between the parties.

The continuity plan for BankID in Eika Gruppen covers, among other things, the following aspects relating to a disaster situation.

- Criteria for implementation of a continuity plan.
- Roles and distribution of responsibility within Eika Gruppen.

- Order of execution for relevant measures.
- Communication with internal resources, individual banks, and service providers.
- External communication with customers, other banks and bank groups, and trade organisations.
- Establishing corrective measures to the BankID solution.
- A retrospective analysis of the situation with potential improving changes to the disaster recovery plan.

Banks affiliated with Eika Gruppen afflicted by a disaster situation will then publish a declaration about the event to their customers.

If Eika Gruppen or the individual bank's private key is compromised, Eika will then perform relevant necessary tasks to inform the affected parties about the situation and to make sure affected certificates are no longer to be accepted.

For Nordea: No additions.

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.

5.8 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 covers Nets' part of the termination procedures.

For Bankenes ID-tjeneste: Procedures and agreements between BID 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.

BID as Joint Issuer will not be terminated as long as there are banks with active certificates issue by BID. Cf also Termination Plan.

For Danske Bank: For the RA-system: Termination refers to a situation where permanent closure happens to all logical functions related to Danske Bank acting as RA for the issuance of BankIDs

Before Danske Bank terminates its service as a RA, 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 the TSPS document, CP and CPS.

Danske Bank would also ensure that any other banks that use its RA services receive the necessary information to move to another TSP.

The terms above apply when Danske Bank ceases operation in a controlled manner and has time to notify contacts of what is about to happen. The terms do not apply in emergencies.

For DNB: 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 do not apply in emergency situations.

Before Eika Gruppen as issuer of BankID, or a bank issuing BankID under Eika as TSP, terminates its services in a controlled manner, Eika will:

- Inform the owner of the parent CA (BankID root-CA) about the planned termination at least 6 months in advance.
- Inform the subjects, relying parties 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 CP and TSPS.
- Ensure that all Eika Gruppen's private keys, including backup copies, are destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved
- Make arrangements to transfer provision of trust services for its existing customers for a limited period of time to another TSP where relevant and possible.

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 Chapter 4.6.

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

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.

RA key pair generation

The RA key pair used to encrypt the communication between the bank RA servers at the TSP RA service provider and the CA-system service provider is generated by the CA software 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 TSP 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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions

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

As issuer of BankID in the BankID Partnership, Eika Gruppen owns a CA in BankID COI. In connection with this, an initial key ceremony has been performed. Eika's CA was then established in BankID COI, and various keys and other security elements were issued to Eika. These were security elements associated with the group's CA.

In the aftermath, key ceremonies have also been performed associated with Eika Gruppen's CA in BankID COI whenever needed.

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 Nordea: No additions.

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

Enduser key pair generation

Key pairs for Personal BankID and Employee BankID are generated in a FIPS 140 level 3/4 HSM connected to the central storage entity in accordance with [4].

Subject key pair algorithm is RSA 2048 as documented in the document BankID Certificate Profiles [13].

Bank-stored keys are generated HSM inside secure room on request from CA ARM plugin (ODS plugin) . Public key is then used for issuing of certificate by CA. Public key is triple encrypted with 2 Public Keys from 2 separate components and user provided passphrase and encrypted value is stored in database inside secure room

For Bankenes ID-tjeneste: The RA's keys for secure communication with COI Common Infrastructure are generated by BIDs 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 Danske Bank: No additions.

For DNB:

For Eika: The key pairs are delivered to Eika Gruppen's Key Custodian by personal attendance 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. This is described in [4]. Nordea has internal 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: No additions.

6.1.2 Private key delivery to subscriber

The private keys of a Netcentric PersonBankID or EmployeeBankID are exported as a cryptogram from the HSM where they were generated and stored in an encrypted database on the central storage entity. The subject has to employ two-factor authentication to use the keys.

This ensures the subscriber has sole control of the keys.

There is no delivery of the private key for Netcentric solution, since this is stored in the central database.

6.1.3 Public key delivery to certificate issuer

Public keys are delivered from the from the HSM where they were generated to the CA in a signed certification request. The key generation HSM is an integral part of the CA-system.

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 Chapter 1.3.1). The main rule is that BankID certificate issuers are responsible for making a valid CA level 1-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 is 4096 bits for RSA.

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

The key size for Personal BankID and Employee BankID is 2048 bits for RSA.

6.1.6 Public key parameters generation and quality checking

Key pairs for PersonBankID and EmployeeBankID are generated in a FIPS 140 level 3/4 evaluated HSM.

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

BankID has different key pairs for authentication and signing.

For authentication certificates; NonRepudiation(1)/DigitalSignature(0)/KeyAgreement(4) is used.

For signing certificates; Non-repudiation(1) is used.

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 Bankenes ID-tjeneste: RA system Suppliers store certain elements within a HSM.

For Danske Bank: In relation to RA system in Danske Bank, the access to crypto facilities, functions, keys, etc. involves two people entering the crypto room together, and two people logging in and operating the crypto equipment together.

Crypto equipment is located in physically locked premises that require two key officers together. Logical access to the crypto function requires two key officers together. Key generation always requires two key officers together. The administration of keys are always logged.

For DNB: No additions.

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).

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.

The service provider for BankID COI has dedicated routines for key destruction, and Eika Gruppen has routines for following up the service provider in such cases and verifying that all keys are destroyed and removed. Eika Gruppen has appointed a key custodian who will accompany security officers from the service provider for BankID COI in performing this task.

Customers with Personal BankID and Employee BankID have sole control over their bank-stored private keys, as the customer has sole control over the activation data - the OTP mechanism and the personal static BankID password.

For Nordea: No additions.

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.

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

For Danske Bank: In Danske Bank, the access to crypto facilities, functions, keys, etc. involves two people entering the crypto room together, and two people logging in and operating the crypto equipment together.

Crypto equipment is located in physically locked premises that require two key officers together. Logical access to the crypto function requires two key officers together. Key generation always requires two key officers together. The administration of keys must be logged.

For DNB: No additions

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 Nordea: No additions.

For SpareBank 1: Any access to the system that holds the Registration Authority'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.

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

Private keys for all issuers are backed up for recovery purposes. All certification authority systems shall be recoverable, including all key values stored in the system's HSM. Exports of key materials for recovery purposes shall be performed with a key encryption key, which must be divided into at least two components and never stored in plain text. Knowledge of one component will not provide information about the entire key. Restoring a private key requires all key encryption components to be present and subject to the following rules.

- a) The key encryption key must have at least the strength of two DES keys (112 bit).
- b) It must not be possible to export the components of the key encryption key more than once.

The issuer's key encryption key must be divided into at least two parts, where each key custodian is responsible for one of the key parts.

The centrally stored keys are duplicated (with same encryption) to a Standby site and there will be 2 copies of the endusers keys.

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

For Danske Bank: The TSP stores RA signing keys in several HSMs running active, in geographically dispersed locations. So the HSMs backup each other.

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 sub-chapter 6.2.1 – Cryptographic module standards and controls.

For Nordea: No additions.

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

Private keys are not archived.

Backups of the database in the central storage entity are subject to the same security requirements as for the CA-system.

There is no archive of the bank-stored keys.

6.2.6 Private key transfer into or from a cryptographic module

Private keys for the TSP is backed up for recovery purposes. All certification authority systems are recoverable, including all key values stored in the system's HSM. Exports of key materials for recovery purposes are performed with a key encryption key, which is divided into two components and never stored in plain text. Knowledge of one component will not provide information about the entire key. Restoring a private key requires all key encryption components to be present. The TSP key encryption key is divided into two parts, where each key custodian is responsible for one of the key parts.

The private key of the subject is encrypted with several layers of sequential encryption based on public keys corresponding to private keys generated and held by dedicated HSMs evaluated according to FIPS 140 level 3/4.

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.

Multi-personnel control by means of n-of-m HSM cards is required to load and activate the keys into the HSM. The sensory controller of the HSM can, in a case of an alarm, delete or render useless the key material in the HSM.

For end users as subjects

The subject's private keys are generated and used within an HSM. The keys are stored in a database in a strongly encrypted format outside the HSM in an environment with physical and logical access control, but can then only be read as a cryptogram that only the correct HSM can interpret.

For RA systems

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: See sub-chapter 6.2.1 – Cryptographic module standards and controls.

For Nordea: For RA system the private keys are stored in a HSM and backup in secure physical location.

For SpareBank 1: TSP private keys on the Registration Authority System are generated and kept within a cryptographic module (HSM). If it becomes necessary to restore this, it will arrive as a cryptogram, encrypted using a KEK.

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

To use his or her private key, the subject must perform a strong authentication consisting of two factors, a one-time password (proving that he or she has a possession element) and a static password. Only if the subject's authentication elements are correct for the session, the private key can be decrypted by and used within the dedicated HSM on the central storage entity.

The static password must meet the BankID password rules.

Key pair is only used in accordance to the standard user agreement. Keys can not be accessed without user providing his password. (described in Architecture Description Security 8.2.2. User provided password is part of encryption of private key in storage.

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. Key management for CAs is described in Chapter 4.16 in [4].

The subject has to request a revocation in order to deactivate the keys permanently. A key that has been revoked, suspended or expired can not be activated on central systems.

A private key that has expired is not archived and will therefore not exist once it has expired.

6.2.11 Cryptographic Module Rating

Key generation is made in Hardware Security Modules with FIPS level 140-2 level 3 and FIPS level 140-2 level 4. Private keys never leaves HSMs unencrypted.

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 PersonBankID or EmployeeBankID 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

Subjects must use activation data consisting of two factors to activate their private key: a one time code that proves that the subject has a possession element that can generate unique one time codes, and a static password. Both elements shall be correctly verified before the subject can use the PersonBankID.

Both the possession element and the associated solution included procedures for personalisation, distribution and assignment must be approved by Bits AS. Minor changes shall be notified to Bits AS.

The authentication solution with the possession element shall be uniquely personalised and assigned to the subject in a secure way.

For Bankenes ID-tjeneste: No additions. Cf. also 4.1.2

For Danske Bank: No additions.

For DNB: See 4.2.1

For Eika: Customers with Personal BankID and Employee BankID have sole control over their bank-stored private keys, as the customer has sole control over the activation data - the OTP mechanism and the personal static BankID password. These activation data are assigned and distributed to the customers in a secure way. If it becomes necessary to distribute a new possession element or provide a subject with a new password, the bank and Eika Gruppen will ensure that the subject's identity is correct.

For Nordea: No additions.

For SpareBank 1: TSP has an agreement with a service provider for a possession element system. The system is operated in a secure manner according to the service provider agreement. The solution is approved by Bits AS.

The Registration Authorities have two one-time-code implementations (possession elements):

- Physical one-time-code-generator, which is personalized and distributed to the customer.
- The mobile app, “One-time-code for Mobile” is ordered by the customer in the online bank portal or in the mobile app itself. The order is based on customer information, pre-verified by the customer himself by authentication with BankID or showing valid identification documents in a bank branch office. The software (or the app) is downloaded by the customer from the relevant marketplace to the phone. Personalization codes are sent to the customer in two different channels. The app is protected by a personal PIN-code or the personal security mechanism chosen by the customer for the mobile phone. The PIN-code is set as part of the activation of the app.

TSP also offers the customers to use BankID on Mobile as possession element.

RA-generated password that are sent to the customer as part of the ordering process, is in accordance with Bits AS' requirements. The password must be changed as part of the first authentication. Each time a new password is sent to a customer, the customer is notified in a separate channel. Either email or SMS is used.

6.4.2 Activation data protection

A bank that performs the role of registration authority shall control the procedures for assignment of a possession element to a personal customer. If it becomes necessary to distribute a new possession element or provide a subject with a new password, the bank must ensure that the subject's identity is correct.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: See subchapter 6.4.1 – Activation data generation and installation.

For Nordea: The service provider does not store activation data for subjects. All transfers of activation data to and from systems at the service provider's premises will be secured with strong encryption.

For SpareBank 1: The Registration Authorities have routines to verify the customer's identity for phone inquiries. If the customer's identity cannot be safely verified over phone, the customer must meet personally with valid identification documents.

6.4.3 Other aspects of activation data

The possession element:

The authentication is operated safely by the issuer or a service provider selected by the issuer. All secrets shall be protected. Bits AS is granted the right to approve authentication solutions and will, as part of the approvals process, evaluate both algorithmic security and practical security with regard to the personalisation, assignment and distribution of the possession elements. A Bits AS approved authentication mechanism includes the solution that is distributed to the end user, centrally based software and hardware for verification and processing of one-time codes, as well as the communication between these two.

For Bankenes ID-tjeneste: Customers with Personal BankID have sole control over their bank-stored private keys, as the customer has sole control over the activation data - the OTP mechanism and the personal static BankID password. These activation data are assigned and distributed to the customers in a secure way. If it becomes necessary to distribute a new possession element or provide a subject with a new password, the RAs will ensure that the subject's identity is correct.

For Danske Bank: Danske Bank uses a one-time password (possession element) solution that is approved by Bits AS.

For DNB: See 4.2.1

For Eika: See subchapter 6.4.1 – Activation data generation and installation.

For Nordea: For the time being, the possession element is represented by a physical token (ActivCard) or BankID on mobile as OTP. Nordea will also offer an app solution when approved by Bits AS.

For SpareBank 1: No additions.

The static password:

The static password must contain at least 8 characters. The password is not at any time or place stored in plain text. Checks are made to ensure that the password chosen fulfils the requirements. The password has no expiration

date, but the end user can change the password at any time as long as the new password fulfils the requirements for passwords. The password is used for identification of end users and to protect the personal customer's private keys in the central storage entity.

The RA specifies rules for how a user's password shall be initialised. A password that the bank acting as RA or other third party systems may have processed must be changed at the first opportunity. The relevant information about this shall be part of a bank specific addition to this document.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: The static BankID password is created after the subject has been assigned a temporary, one-time password. The subject needs to change this to a self-chosen, static password the first time he/she uses the BankID. The password must be at least 8 characters long and can be a mixture of numbers, letters and special characters. The subject is free to change the password whenever he/she chooses.

The subject will be sent a temporary one-time password by SMS. The password must be changed the first time the subject uses it, together with the possession item, to log on. The mobile telephone number to which the temporary password is sent must be registered in the bank's systems and cannot have been changed within the last three months.

Notice of a new one-time password will be sent to the subject's mailbox in the Internet banking service, as well as through another channel (e-mail or SMS).

For Eika: No additions.

For Nordea: The static password is sent to the customer as a one-time password that needs to be changed upon first use. It is sent as SMS, email or in a physical letter separated from the possession element.

For SpareBank 1: The static password sent to the customer has to be changed upon first use.

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 Chapter 5.2.1.

The CA system 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 personell 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".

Certificate Status Service

The BankID Certificate status service is protected by the OCSP-protocol as described in chapter 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.

CRL's 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

Centrally stored certificates saves the end-users certificate in a central database with dual access control. The enduser may view it's own certificate through the BankID client, which have read-only access to the certificate database.

For Bankenes ID-tjeneste: BID 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 Danske Bank: Danske Bank sets protection from malicious software to be integral part of workstations and servers builds. This includes anti-virus, firewall and HIPS components, those are centrally managed, updated and protected from service shutdown. Antivirus protection works in on-access mode and in addition scheduled forced scans occur on regular basis. Central reporting gathers all anti-virus alerts, whose are being 24/7 monitored via SIEM integration by Security Operation Centre. In addition to that antivirus deployments (antivirus agents) are constantly monitored by central system monitoring system for the service status and definitions versions. Threat intelligence information is used as part of control review process.

Network-based controls: Internet access control web proxy is used to filter URLs; for messaging services protection E-mail security gateway is used.

Spear phishing is controlled by business procedure for central phishing reporting and takedown services.

A layered system protecting against malware is in place and monitored by Danske Banks Security Operation Center 24/7. This consists of elements in the perimeter, on servers and on workstation. IDS/IPS-systems monitor, log, and send alarms in case of signs on infections e.g. when nodes on the intranet contact known C&C-servers on the internet.

Certain categories and specific sites are blocked including data sharing sites. Web email and Internet chat sites are not blocked as categories.

Danske Bank makes use of private networks, TLS, and VPN connections based on risk assessments. Staff is instructed to encrypt attachments to emails when needed. BitLocker is used for hard disk encryption for laptops.

All systems are subject to security assessments during the development and significant changes. Vulnerability scanning is performed on quarterly basis and penetration testing is performed on a regular basis.

It is part of the normal IT process in Danske Bank not to use this type of media. However, the use of USB is not blocked. Any use of this media is managed via SOP.

For DNB: No additions.

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 Nordea: No additions.

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

Nets Security Framework (NSF) 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

For Bankenes ID-tjeneste: No additions.

For Danske Bank: Danske Bank benchmarks its IT security framework and management system to the ISO 27001:2013 standard. This is done with assurance from external providers, who are specialists in the field, e.g. Verizon and TrustWave

For DNB: No additions.

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 Nordea: No additions.

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 service provider of the CA-system and the central storage entity 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 service provider 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.

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

For Danske Bank: It Governance and Portfolie management are following the proceses described at internal pages of the Bank. Change management procedures are in place that ensures that all changes are documented and approved with the appropriate risk assessment as well as fall back plan. TSP system and information are protected aganst viruses, malicious and unauthorized software.

For DNB: No additions

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.

For Nordea: RA is following Nordea standard practices of IT security and segregation of duties.

For SpareBank 1: No additions.

6.6.2 Security management controls

The service provider of the CA and the central storage entity has implemented a security framework for policy and procedures.

The service provider 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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: Danske Bank systems are operated in compliance with the ITIL standard. There is a media handling policy in place and all media handling procedures should be aligned with it.

For DNB: No additions.

For Eika: All production equipment are placed in a secured environment with multiple layers of physical and logical security.

The server halls are furthermore 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.

For Nordea: No additions.

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.

For Bankenes ID-tjeneste: No additions.

For Danske Bank: No additions.

For DNB: No additions.

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.

For Nordea: No additions.

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 service provider and central storage entity.

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 CA-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 CA-systems are configured to provide the minimum functionality required for the issuing service. All communication ports that are not clearly required are disconnected and software processes using these ports are turned off.

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

The end user must perform two-factor authentication to access the private keys. All network traffic between the end user's equipment and the central storage entity is encrypted and passes through multiple layers of firewalls.

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 system

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

For Danske Bank: In Danske Bank, Firewalls are configured to prevent unauthorized protocols and accesses. Security patches are processed on a monthly basis. Urgent Security patches outside cycle is processed and escalated as a production incident.

The Danske Bank Network are divided in building blocks. The Internal building blocks are interconnected without firewalls whereas all DMZ services are behind firewall protection. All new workload that are build since summer 2017 are based on zero-trust and are protected with several layers of protection. All applications will be migrated to the zero trust environment over the next 2 years.

Restrictive access between the zone is established according to firewall policy. All exceptions are reviewed by Group IT security. Dedicated network for administration of IT systems. Staging environments are TEST, SYST and PROD. Communication between different security zones are only allowed thru trusted encrypted channels and redundancy is ensured by two datacentres.

Processes for patching are in place. Patching is performed due to specific schemes per platform taking severity into consideration prioritising external facing systems.

Environments for development, testing and production are separated. Developers have restricted access to production environment based on authorizations and business needs.

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 service provider 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, as anti-virus software, firewalls etc.

The host computers used in Eika Gruppen's BankID solution are not directly accessible through open networks. The BankID solution is also protected by firewalls. Communication between CA and RA is also protected.

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

For Nordea: No additions.

For SpareBank 1: RA system is placed in a network zone separated from other internal networks, guarded by firewall with statefull 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 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 chapter 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
 - a. 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.
 - b. 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.
 - c. BankID Personal BankID and Employee BankID certificates consists of 2 certificates and 2 keys, and used for electronic ID (authentication) and signing electronic documents in merchants sites.
The keys and certificates are stored in a central system for BankID called the COI (Common Operational Infrastructure) operated by a trusted third party.

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.

PersonBankIDs based on a netcentric solution, shall use the following identifier:

Object Identifier (OID): {joint-iso-itu-t(2) country(16) norway(578) organisasjon(1) bankenes-standardiseringskontor(16) policy(1) qualifiedCertificates(12) netcentric(1) 1}

EmployeeBankIDs based on a netcentric solution, shall use the following identifier:

Object Identifier (OID): {joint-iso-itu-t(2) country(16) norway(578) organisation(1) bankenes-standardiseringskontor(16) policy(1) qualifiedEmployeeCertificates(13) netcentric(1) 1}

7.1.7 Usage of Policy Constraints extension

The Personal BankID is issued to a natural person which must be a customer in Norwegian Bank.

The Employee BankID is issued to a natural person employed in a company that is a customer of a Norwegian Bank.

7.1.8 Policy qualifiers syntax and semantics

All PersonBankID and EmployeeBankID 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.

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 PersonBankID and EmployeeBankID 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 service provider of the CA-systems and the central storage entity are subject to periodic compliance audits. Compliance audits shall be 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 service provider 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 documents. 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 TSP, bank acting as RA and any service provider involved in operating BankID Services on behalf of these entities actually operate, shall be reported to the management team of the TSP and Bits AS. The parties will jointly define corrective measures and set a deadline for implementation. Bits AS shall assess whether TSP's shall be informed immediately of matters relating to the joint issuer or service provider used by the bank.

In the event of a discrepancy between requirements laid down in the relevant certificate policy and practical implementation, the TSP 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 PersonBankID or EmployeeBankID is issued by a TSP according to this TSPS and 'Regler om BankID', and that the end user has used the BankID according to the end user agreement, the TSP is liable for up to NOK100.000,- 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 Electronic Signature Act [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 serviceprovider involved in the operation of BankID are amongst other things responsible for keeping the following types of information confidential:

- Issuer's and Registration Authority's private keys;
- Passwords, PINs and other activation data, provided the information is held by the bank/issuer;
- All private keys belonging to subjects if at any stage they have been processed by the issuer or its service provider;
- 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, d.o.b. 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 serviceprovider involved in the operation of BankID 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].

For Bankenes ID-tjeneste: Subject information is managed by the RAs according to Norwegian laws and regulation, see 9.3. BID does not manage subject information.

For Danske Bank: Danske Bank adhere to and comply with GDPR and its principles.

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 Eika: No additions.

For Nordea: No additions.

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 serviceprovider involved in the operation of BankID 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 PersonBankID or EmployeeBankID 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 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 Chapter 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 Chapter 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 Electronic Signature Act [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:

- 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;
- Enable key generation in the central key store;
- 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 TSPS.

In the case of PersonBankID the RA shall in addition:

- Check and verify the identity of certificate applicants as described in Chapter 3;
- Guide and assist the certificate applicant during the registration process;

In the case of EmployeeBankID the RA shall in addition:

- Check and verify the identity of enterprises applying for issuance of Employee Certificates as described in Chapter 3;
- Check and verify the identity of certificate applicants who require EmployeeBankID;
- Guide and assist the enterprise and the persons during the registration process.

9.6.3 Subscriber representations and warranties

PersonBankID

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 BankID Certified Software and in accordance with the intended use;
- Protect passwords, PINs and other activation data, and ensure they are 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;
- Warn the bank of any suspicion that passwords, PINS or other activation data may have become known to others;
- Immediately stop using a BankID if the private key or activation data may have become known to others.

EmployeeBankID

Key obligations for Subscribers who enter into an agreement on EmployeeBankID, shall also be documented in the agreement between the bank and the Subscriber [20].

The Subscriber shall:

- Follow the procedures provided when applying for an employee certificate;
- Provide correct and complete information about the enterprise and relevant individuals when applying for a certificate;
- Confirm that persons who are included in the application for employee certificates are either employed by, or have a contractual relationship with the enterprise;
- Read and understand the terms and conditions for issuing and using BankID, and confirm acceptance of terms to the bank;
- Read and understand all user documentation and ensure that this is distributed to the persons who are allocated an EmployeeBankID;
- Assist individuals during the registration process and set up of their user environment, as necessary;
- Protect passwords, PINs and other activation stored by the enterprise, and ensure these are kept secret;
- Inform the bank of any matters of importance to the contractual relationship, including changes to information supplied at the time of issuance and changes to the employment relationship;
- Explain to holders of EmployeeBankID that they have a duty to report to the bank any suspicion that private key or activation data has become known to others.

Key obligations for subjects shall also be documented in the user statement signed by the subject. [20]. A suggestion for the content of this statement is attached to the model agreement for bank/customer.

The Subject shall:

- Follow the procedures provided when applying for a EmployeeBankID;
- Provide correct and complete information when applying for EmployeeBankID;
- Sign the user statement and comply with the terms and conditions of this declaration;
- Only use keys and certificates in connection with BankID Certified Software and in accordance with the intended use;

- Protect passwords, PINs and other activation data, and ensure they are kept secret;
- Report to the bank (or its service provider) if a private key is suspected to have become known to others;
- Warn the bank of any suspicion that passwords, PINS or other activation data may have become known to others;
- Immediately stop using a BankID if the private key or activation data may 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).

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 storage entities for netcentric BankID 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;

In the case of centralised data storage the service provider for the storage entity shall:

- Generate key materials for end users (personal customers and subjects with EmployeeBankID);
- Make the necessary software available to subjects to allow them to use their keys;
- Protect all private keys to ensure only the rightful owner can access these;
- Use certificates and keys only for the intended use and in the intended usage environment;
- Make stored certificates accessible to subjects;
- Make additional information about subjects available to replying parties with the required authorisation;
- Log and archive historical data concerning key usage.

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 PersonBankID and EmployeeBankID, is governed by agreements, both when the customer is a subject and a relying party.

In the case of EmployeeBankID, the liability relationship between the TSP and the enterprise is governed by agreements, both when the enterprise enters into an agreement on EmployeeBankID 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 (Finansavtaleloven), 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 PersonBankID

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.

Subject liability EmployeeBankID

The enterprise's liability is governed by agreement [4] between the bank and the enterprise on the issuance of EmployeeBankID. If the subscriber uses BankID, software or documentation in violation of the agreement, including unauthorised modification or manipulation of BankID or software by the subscriber or individual employees, the bank may hold the subscriber liable for any losses the bank suffers in consequence.

The subscriber will also, in accordance with common legal practice, be held responsible for dispositions made by anyone who has been able to use the EmployeeBankID due to an intentional or negligent act or omission by the subscriber.

9.9 Indemnities

The TSP's financial liability is limited to NOK100.000 per transaction [20]. 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 Chapter 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 Electronic Signature Act [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).

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 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 chapter 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.

The termination of BankID scheme is regulated in the BankID Rules article 21: If a BankID is terminated, each participant is required to retain information about BankID agreements they have entered into and to be able to confirm the validity of such BankIDs for at least 10 years after the last time that BankID could have been used by the subject. Termination of BankID involved terminating all participating TSPs and procedures resulting from this. Any information, certificates, software or hardware not covered by individual TSP's termination plans, shall be destroyed or withdrawn from use in a secure and trustworthy manner in line with details here and in section 5.8.

For Bankenes ID-tjeneste: BID as Joint Issuer will not be terminated as long as there are banks with active certificates issued by BID. BID's owners have established agreements and procedures that ensures that the last bank using BID as Joint Issuer under agreement (Bruksrettsavtale) and with active certificates will be the sole owner of the company and can terminate BID as Issuer only after revocation of the Bank's certificates issued by BID.

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 (agreement between the RA and BID) and active Certificates. Termination of a Bruksrettsavtale implicates that all certificates issued by the RA shall be revoked.

For Danske Bank: No additions.

For DNB: No additions.

For Eika: The termination plan of Eika Gruppen states that Eika will:

- Inform the owner of the parent CA (BankID root-CA) about the planned termination at least 6 months in advance.
- Inform the subjects, relying parties 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 CP and TSPS.
- Ensure that all Eika Gruppen's private keys, including backup copies, are destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved

- Make arrangements to transfer provision of trust services for its existing customers for a limited period of time to another TSP where relevant and possible.

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. The banking industry has furthermore prepared procedures that shall be followed if a participating bank or registration authority goes into administration.

Eika Gruppen will further back up all log data in its possession and enable storage for at least 10 years in an archive that is readable.

All of Eika Gruppen's private keys will be destroyed.

According to the Norwegian BankID Rules a TSP of BankID shall have an arrangement to cover the costs to fulfil these minimum requirements regarding continued fulfillment of certain obligations toward customers and relying parties in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy. Eika Gruppen has such guarantee arrangements.

For Nordea: No additions.

For SpareBank 1: No additions.

9.17.2 Risk management

The TSP has a 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 determines 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 service provider of the CA-system and the central storage entity.
- 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 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.

Nets makes an annual risk assessment of BankID. This handles risk for IT part of the solution. The risks are documented in a risk analysis document. The implementation of the risk treatment procedures are based on the Nets security framework Security Policy.

For Bankenes ID-tjeneste: BID 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 BID and risks and possible actions reported are taken into consideration by the RA. The risk assessment performed by the operator (Nets) of the Common Operational Infrastructure is taken as input to the TSP risk assessment. RAs are identified in APPENDIX 1.

For Danske Bank: Danske Bank follow the guidance and risk evaluations process from Vipps AS and Bits AS. Danske Bank does a risk assessment whenever major changes happen in the system and with every major change, a Security Assessment is done.

Danske Bank has continuous overview of the fraud issues, in case of unusual patterns, the bank re-evaluate and change the systems and risk assessment. In addition, Danske Bank and FinansCert Norway collaborates for monitoring the daily threats against BankID.

Security requirements and operational procedure definition task is performed primary by the Danske Bank Business representatives in Norway and secondarily by the eBusiness Security department, the later make the needed changes in the IT systems.

Approval of the Risk Assessment is followed as a part of the security assessment process of Danske Bank system and Group Security department of the bank accepts the residual risk

Group Operational Risk defines the overall policies and framework for Operational Risk Management and IT Risk is governed by the operational risk policy and framework as well. Group IT Security and Risk has more detailed risk management processes in place. The general risk assessment covers the whole platform including physical and logical security aspects as well as cyber risks. On a local plan, risks are identified for individual solutions in relation to the custody business and actions plans are in place to address any risk identified. This is then fed through to the local Operations risk register and consolidated with all units risks.

Risk Management committees

The Enterprise Risk Management (ERM) framework specifies a number of Risk Committees, which are responsible for the oversight and control of risks, group wide. These include, for instance, the Board Risk Committee, the All-Risk committee, various specific oversight committees (e.g. Operational Risk Committee), and several others.

In addition, Country, Subsidiary, Business and Function Units are allowed to establish local risk committees. Local risk committees must ensure that risks within the given entity are managed effectively and in accordance with risk frameworks and constraints set by the Group. The country, subsidiary business or function manager is chairman of the local risk committee. Established local risk committees functionally report to Group risk committees.

Operational Risk Policies and Procedures

Local risk policies follow the Group Operational Risk Policies and Procedures.

Group Operational Risk is responsible for developing operational Risk Policy. The Board of Directors approves the policy and specifies high-level principles and standards of operational risk management for the Danske Bank Group. In addition, the Operational Risk Framework endorsed by the Executive Board describes how the Executive Board implements and embeds Operational Risk Policy across the Group. Furthermore, the Bank has a Fraud Policy, Outsourcing Policy and Corporate Governance Policy.

Operational risk control and assessment tool

Operational risk control and assessment is implemented via the Operational Risk Management Process. This process is established for both operational risks and operational risk events management to ensure that risks are identified, assessed and managed effectively across the Group, so the Group remains within risk appetite.

Operational Risk Standards and tools, including risk taxonomies and matrices, are applied to give comparable indicators and ensure management of operational risks. Dedicated information systems are in place for capturing identified risks and operational risk events. Tools such as the Business Risk Management document and Fraud Risk Register are used by the business to document, mitigate and reduce risks. An IT Risk assessment is carried out for projects internally in the bank as well as when suppliers are used.

Who are the providers of the coverage

Roles and responsibilities related to risk management are defined in accordance with a three lines of defence principle:

The business units and the operations and service organisations represent the first line of defence. This entails individual units who own and manage their own activities and risk, either at business level or at function level. The heads of the business units, operations areas and service areas are responsible for all business-related risks

The second line of defence is represented by the group-wide functions that monitor whether the business units and the operations and service organisations adhere to the general policies and mandates. These are independent control functions who specify the policies and standards under which the first line must operate.

The third line of defence is Group Internal Audit (GIA) Defence and is headed by the Chief Internal Audit Officer. Local auditing functions are functionally part of Group Internal Audit. Group Internal Audit provides an independent and objective assurance to test the design and operating effectiveness of the internal control environment in the First Line and Second Line.

Independent risk management area

The local risk management area is functionally part of Group Risk Management. Group Risk Management (unit) is an independent risk management area and acts as the second line of defence. The Group Chief Risk Officer, who is also an Executive Board member, heads this unit. Likewise, local Operational Risk functionally is part of Group Operational Risk.

Reviews by external auditors

An external audit firm is responsible for the statutory financial audit of the Danske Bank Group. The audit is conducted in accordance with the International Standards on Auditing and additional requirements under the Danish audit regulation. Currently, Deloitte Statsautoriseret Revisionspartnerselskab is the appointed external audit firm.

For DNB: 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.

For Nordea: No additions.

For SpareBank 1: No additions.

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] PKCS#10 v1.7: Certification Request Syntax Standard, Public Key Cryptography Standard #10, RSA Data Security Inc., May 2000
- [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] NS-ENISO9001:2008 Quality Management Systems - Requirements
- [13] BankID Certificate Profiles, Bits AS. (previously "External Certificates"). See Section 2 for document URL.
- [14] Act of 14 April 2000 No. 31 relating to the processing of personal data, with subsequent amendments
- [15] Act of 15 April 2001 No. 81 relating to electronic signatures, last amended 17 June 2005
- [16] Norwegian BankID Root CP/CPS v2.3 August 2016
- [17] Policy Requirements for Certification Authorities Issuing Qualified Certificates, v.1.4.3 (2007-05)
- [18] Document no longer referenced
- [19] Act of 3 June 2009 No. 11 relating to measures to combat money laundering and the financing of terrorism etc., with associated regulations.
- [20] Agreement between bank and subject about BankID, based on the model agreements "Avtalevilkår for PersonBankID" (Terms for PersonBankID) and "Avtalevilkår for AnsattBankID" (Terms for EmployeeBankID) developed by the Finance Norway Service Office.
- [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 MerchantBankID, 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]