Stø AS Certificate Services TSPS

Version 1.2 Last updated 23. September 2025.

bankID bankaxept

Contents

Document history

Version	Date	Changes	Approved by
1.2	24.09.2025	Reflecting name change to Stø	ID Advisory Board
1.1.2	11.12.2024	Editorial changes in section 4.3.a)	Approval not needed
1.1.1	28.10.2024	Minor changes in section 3.2.b) Changed numbering in sections 6.6 and 6.7	ID Policy Board
1.1	24.09.2024	Incorporating comments from Stage 1 audit, including a specification of which eIDs are accepted + some editorials	As above
1.0	03.05.2024	First approved version	ID Policy Board
0.9	28.04.2024	Temporary version	
0.8	10.04.2024	Initial complete version	

1 Introduction

Stø AS is a Norwegian Trust Service Provider (TSP). Since May 4th, 2025 Stø AS has been the name of the company formerly known as BankID BankAxept AS. BankID BankAxept AS was established July 19th, 2022 and has a long and in-depth experience in designing, developing and operating Trust Services compliant with the eIDAS regulation (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC).

The name BankID BankAxept AS is still used in this version of the TSPS. Future versions will incorporate the name change.

1.1 Overview

This document describes the policy and practices BankID BankAxept AS has established for issuance of Certificates for e-Signatures and Qualified Time-stamping services.

Figure 1 provides a logical overview of BankID BankAxept AS PKI infrastructure established to provide Certificate Services, consisting of a BankID BankAxept AS Root CA and a set of subordinate Issuing CAs:

- The e-Sign CA, and
- The TSA CA.

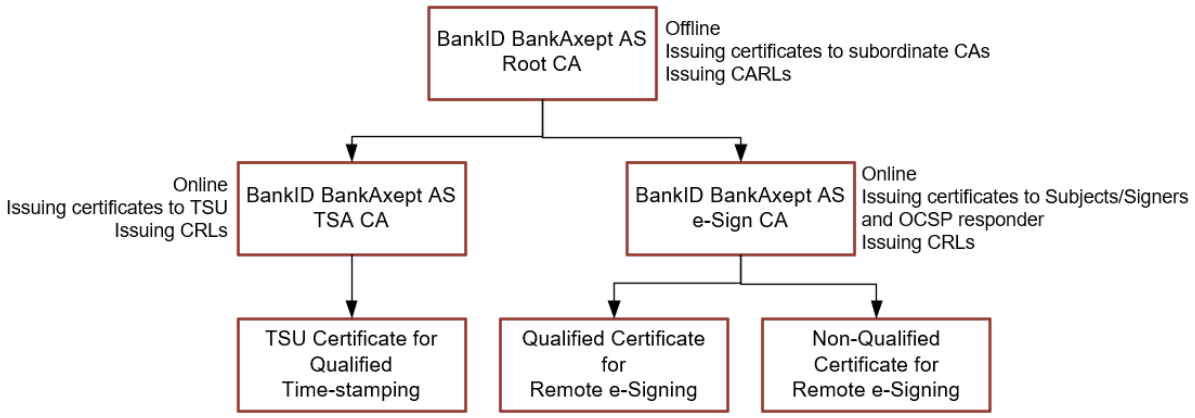

Figure 1: Logical overview BankID BankAxept AS PKI infrastructure

The BankID BankAxept AS PKI infrastructure consists of:

- BankID BankAxept AS Root CA which is:
  - Offline – residing in a High Security Zone.
  - Issuing certificates to subordinate CAs;
    - BankID BankAxept AS e-Sign CA and BankID BankAxept AS TSA CA.
  - Issuing Certificate Authority Revocation Lists (CARLs).
- BankID BankAxept AS e-Sign CA which is:
  - Online – residing in High Security zone in line with practices set forth in [22]
  - Issuing:
    - Qualified and non-Qualified e-Signing certificates to Subjects/Signers for Remote e-Signing as described in [23]
    - OCSP certificates to BankID BankAxept AS internal OCSP responder.
    - Certificate Revocation Lists (CRLs)
- BankID BankAxept TSA CA which is:
  - Online – residing in High Security zone in line with practices set forth in [22]
  - Issuing Certificates to Time-stamping Units providing Qualified Timestamping as described in [24]
  - Issuing Certificate Revocation Lists (CRLs)

Note: When issuing certificates based on a notified eID on level substantial, BankID BankAxept AS will issue a non-qualified certificate suitable for advanced electronic signature.

1.2 Document name and identification

Document Name; Stø AS Certificate Services Practice Statement

No OID is allocated for this document.

1.2.1 Conventions

The structure (headings and subheadings) in this TSPS is organized in accordance with recommendations in [18].

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules [19].

1.3 PKI participants and responsibilities/obligations

1.3.1 Trust Service Provider

BankID BankAxept AS is the Trust Service Provider providing Certificate Services described in this document.

1.3.2 Registration authorities

BankID BankAxept AS is the Registration authority for BankID BankAxept AS Root CA and BankID BankAxept AS TSA CA. The RA function is undertaken by dedicated personnel in Trusted roles appointed in line with requirements in [22].

BankID BankAxept AS is the Registration authority (RA) for BankID BankAxept AS e-Sign CA issuing Certificates to Subjects/Signers. The e-Signature Service is issuing a CSR based on Subject/Signer data received from the NIdP to whom the Authentication process is delegated as described in chapters 3.2 and 3.3.

1.3.3 Subscribers/subjects

Subjects of Certificates issued by BankID BankAxept AS Root CA are the subordinate CAs; BankID BankAxept AS e-Sign CA and BankID BankAxept TSA CA.

Subjects of certificates issued by BankID BankAxept AS e-Sign CA are natural persons (Signers) using the BankID BankAxept AS e-Signing Service as described in [23].

Subjects of certificates issued by BankID BankAxept AS TSA CA are Time-stamping Units as described in [24]

1.3.4 Relying Parties

Relying Parties includes any entity (natural and legal persons, systems, devices) accepting and relying on e-signatures, signed OCSP responses and signed timestamps provided by BankID BankAxept AS e-Signature Service [23] and BankID BankAxept Timestamping Service [24].

1.3.5 Other participants

This includes auditors, supervisory bodies, Sub-contractors, and other stakeholders.

1.4 Policy administration

Policy administration is according to chapter 1.5 of Stø AS Trust Services TSPS [22].

1.4.1 Organization administering the document

See [22].

1.4.2 Contact person

See [22].

1.4.3 Person determining TSPS suitability for the policy

See [22].

1.4.4 TSPS approval procedures

See [22].

1.5 Definitions of terms, symbols, abbreviations and notation

1.5.1 Terms

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.
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 CA's private key.
Certificate Authority	Authority trusted by one or more users to create and assign public-key certificates.
Certificate Authority Revocation List	Signed list indicating a set of CA-certificates that are no longer considered valid by the Certificate issuer.
Certificate Authority System	The system signing certificates and CRLs with its private key.
Certificate Policy	Named set of rules that indicates the applicability of a certificate to a particular community.
Certificate Revocation List	Signed list indicating a set of certificates that are no longer considered valid by the Certificate issuer.
Distinguished Name	A set of attributes that uniquely identifies an entity.
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, see [i.14].
Electronic identification	Process of using person identification data in electronic form uniquely representing natural person.
Electronic identification means	Material and/or immaterial unit containing person identification data and which is used for authentication for an online service.
Identity Provider	Entity that makes available identity information.
Notified Identity Provider	Identity Provider notified under eIDAS [i.14] issuing eIDs and providing Subjects with eID means.
Object Identifier	A sequence of integers which uniquely identifies an object, as described in [i.3]. Objects in this context, means i.e. a defined information structure or a specification.
OpenID Connect	An identity authentication protocol that is an extension of open authorization (OAuth) 2.0 providing support for inclusion of profile information (attributes) related to the end user.
Public Key Infrastructure	Infrastructure able to support the management of public keys able to support authentication, encryption, integrity or non-repudiation services.
Qualified	When the term is used in conjunction with one or more Trust Service(s) it reflects that the particular Service(s) are meeting the requirements for qualified Trust services set forth in [i.1].

Qualified Signature Creation Device	Computer hardware and software used for creating an electronic signature evaluated and certified according to ISO/IEC 15408 [1] to a protection profile suitable for fulfilling the requirements laid out under Annex II of [i.1].
Registration Authority	An entity that commits to correctly confirming the identity of a future Subject.
Relying Party	Entity (natural and legal person, systems, devices) accepting signatures and signed timestamps based on Certificates issued by BankID BankAxept AS Certificate Services
Repository	A central location in which data is stored and managed.
Short-term Certificate	Certificate with a validity period of 15 minutes or less.
Signer	Natural person being the creator of a digital signature, identified in a Certificate as controlling the private key associated with the public key given in the Certificate (See Subject), acknowledging and adhering to any Subscriber obligations set forth in Terms and Conditions.
Sub-contractor	An entity (organization, legal or individual person) contracted to carry out tasks as part of a Trust Service Provider's Services.
Subject	Entity (natural or legal person, system, device) identified in a Certificate as controlling the private key associated with the public key given in the Certificate.
Subscriber	Depending on context, this term may refer to the Subject of Certificates issued by a BankID BankAxept AS CA or the entity that is contracted with BankID BankAxept AS for use of the Qualified Timestamping Service.
Trust Service Provider	A natural or a legal person who provides one or more Services as defined in [i.1].

1.5.2 Abbreviations

CA	Certificate Authority
CARL	Certificate Authority Revocation List
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
EC	Elliptic Curve
eID	Electronic identification
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
LoA	Level of Assurance
NIdP	Notified Identity Provider
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OIDC	OpenID Connect
PDS	PKI Disclosure Statement
PKI	Public Key Infrastructure
QSCD	Qualified Signature Creation Device
RA	Registration Authority
RFC	Request for Comment
RTO	Return To Operation
TCP/IP	Transmission Control Protocol / Internet Protocol
TSA	Time-stamping Authority
TSP	Trust Service Provider
TSPS	Trust Service Practice Statement
TSU	Time-stamping Unit
TWS	Trustworthy system

1.6 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

1.6.1 Normative references

The following referenced documents are necessary for the application of the present document.

[1] ISO/IEC 15408 (parts 1 to 3): "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security".

[2] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".
[3] ISO/IEC 19790:2012: "Information technology - Security techniques - Security requirements for cryptographic modules".
[4] CA/Browser Forum (V1.6.7): "Guidelines for The Issuance and Management of Extended Validation Certificates".
[5] CA/Browser Forum (V1.7.1): "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".
[6] ISO/IEC 9594-8/Recommendation ITU-T X.509: "Information technology - Open Systems Interconnection - Part 8: The Directory: Public-key and attribute certificate frameworks".
[7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
[8] ETSI EN 319 401 (V2.3.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[9] ETSI EN 319 412-2 (V2.2.1): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons".
[10] ETSI EN 319 412-3 (V1.2.1): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".
[11] IETF RFC 6960: "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP".
[12] FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules".
[13] ETSI EN 319 412-1 (V1.4.4): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".
[14] ETSI TS 119 461: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects".
[15] ETSI EN 319 411-1 (V1.3.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers issuing certificates; Part 1: General requirements".
[16] ETSI EN 319 411-2 (V2.4.1): “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”
[17] ETSI EN 319 412-5 (V2.3.1): "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".
[18] RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
[19] ETSI Drafting Rules (EDRs), accessed 29.02.2024: https://portal.etsi.org/Services/editHelp/How-to-start/ETSI-Drafting-Rules
[20] ETSI TS 119 431-1 (v1.2.1): Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev
[21] Lov 15.juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven)
[22] Stø AS Trust Services Practice Statement
[23] Stø AS e-Signature Service Practice Statement
[24] Stø AS Qualified Timestamping Services Practice Statement

1.6.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] ETSI EN 319 403: "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers".
[i.3] ISO/IEC 9834-1 (ITU-T X.660): “Procedures for the operation of object identifier registration authorities, Part 1: General procedures and top arcs of the international object identifier tree”
[i.4] ISO 19005 (parts 1 to 3): "Document management - electronic document file format for long-term preservation".
[i.5] ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2".
[i.6] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".
[i.7] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".
[i.8] ISO/IEC 7498-2/Recommendation ITU-T X.800: "Data communications network - Open systems interconnection - Security, structure and applications: Security architecture for open systems interconnection for CCITT applications".
[i.9] TS 419 261: "Security requirements for trustworthy systems managing certificates and time stamps", (produced by CEN).
[i.10] ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
[i.11] IETF RFC 5246: "The Transport Layer Security Protocol Version 1.2".
[i.12] ETSI TS 119 612: "Electronic Signatures and Infrastructures (ESI); Trusted Lists".
[i.13] ETSI TS 101 533-1: "Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management".
[i.14] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.
[i.15] ETSI EN 319 421: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps".
[i.16] TS 419 221-2: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).
[i.17] TS 419 221-3: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for Cryptographic module for CSP key generation services", (produced by CEN).
[i.18] TS 419 221-4: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).
[i.19] EN 419 221-5: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).
[i.20] ETSI TR 119 411-4: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 4: Checklist supporting audit of TSP against ETSI EN 319 411-1 or ETSI EN 319 411-2".
[i.21] ETSI TS 119 511:"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques".

1.7 Notations

Text that is outside text boxes is the applicable policy requirements. Each requirement is identified with the following syntax:

In brackets: <6 digits>/<3 letters>-<clause number>

- The 6 digits reflect the standard stating the requirement.
- The 3 letters refer to type of requirement.
- The clause number reflects the clause number in the referred standard.

Text contained inside orange colored text boxes details the practices employed by BankID BankAxept AS to meet the applicable policy requirements.

This document is organized according to the chapter division in IETF RFC 3647 [18]. Empty sub-chapters are excluded from the document to improve readability.

2 Publication and repository recommendations

a) **(319 411-1/DIS-6.1-01A)**: The TSP shall make certificates available to subscribers and subjects.

The short-term certificate will be present as part of the signature generated.

b) **(319 411-1/DIS-6.1-01B)**: The TSP may make certificates available to relying parties only if subject's consent has been obtained.

BankID BankAxept AS Root CA Certificate and subordinate CA Certificates are made publicly available to all Relying parties on BankID BankAxept AS web site.

Signer's certificates are short-term certificates which are only valid for a small number of signing operations. Accept of terms & conditions is a pre-requisite for use of the certificate.

Certificates are implicitly made available to Relying Parties by the Subject/Signer presenting the digitally signed document to a Relying Party. Subjects/Signers Certificates and TSU Certificates are appended to the digital signature.

BankID BankAxept AS will not make Subject/Signers Certificates available to Relying Parties unless signer approval has been obtained.

c) **(319 411-1/DIS-6.1-01C)** [CONDITIONAL]: If the subject is a device or system, the consent for DIS -6-1-01B shall be obtained from the natural or legal person responsible for operating the device or system, instead of the subject.

Not applicable.

BankID BankAxept AS Certificate Service are not issuing Certificates to devices or systems that cannot be owned or controlled by BankID BankAxept AS, see chapter 3.2 letter l).

d) **(319 411-1/DIS-6.1-02A)**: The complete and accurate certificate shall be available for use by the subscriber or subject or, if needed, TSP managing the private key on behalf of the user.

Subject Certificates are available to TSP managing the private key as described in [23].

e) **(319 411-1/DIS-6.1-04)**: The TSP shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 6.9.4).

Terms and conditions are made publicly available to all Relying Parties on the BankID BankAxept AS web site.

f) **(319 411-1/DIS-6.1-05)**: The applicable terms and conditions shall be readily identifiable for a given certificate.

Terms and conditions for Subjects/Signer Certificates are made publicly available on the BankID BankAxept AS web site as described in [22] chapter 3.2.

g) **(319 411-1/DIS-6.1-07A)** [NCP]: The information identified in DIS-6.1-01A, DIS-6.1-01B and DIS-6.1-04 above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavors to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

See [22] chapter 3.1 letter e)

BankID BankAxept AS applies best endeavors to ensure RTO within 60 minutes following an incident.

h) **(319 411-1/DIS-6.1-08)**: The information identified in DIS-6.1-04 above should be publicly and internationally available.

The BankID BankAxept AS web site is publicly available both nationally and internationally.

3 Identification and authentication

3.1 Naming

NOTE: Requirements for naming in certificates are as specified in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7] and the appropriate part of ETSI EN 319 412 [2], [9] and [10]. See clause 6.6.1 of the present document.

The NIdP contracted with and authorized by BankID BankAxept AS providing delegated Authentication services, see [23] chapter 1.3 figure 2 is responsible for fulfilling the requirements for naming in certificates as part of the process of issuing eID means.

3.2 Initial identity validation

a) **(319 411-1/REG-6.2.2-01)**: The TSP shall verify the identity of the subscriber and subject, and shall check that certificate requests are accurate, authorized and complete according to the collected evidence or attestation of identity.

BankID BankAxept AS verifies the attested data received from a trusted Notified Identity Provider (NIdP).

During this process it is checked that the identity record is authorized and complete, whilst the accuracy of the data is ensured by only accepting Identity Providers Notified under eIDAS 910/2014 Article 9 [i.1].

For certificate profile [QCP-n-qscd] the NIdP is required to be notified on level of assurance high

For certificate profile [NCP+] the NIdP is required to be notified on level of assurance substantial or higher.

An updated list of which NIdPs are accepted, can be found on BankID BankAxept AS' webpages.

BankID BankAxept wil keep a list of notified eIDs and NIdPs that are accepted and supported for issuance of certificates according to these certificate profiles.

The Norwegian eID BankID, declared and notified in Europe on level High, is currently the only eID accepted. Certificates issued from these eIDs will be according to certificate profile [QCP-n-qscd].

BankID BankAxept AS will inform subjects and relying parties when there are changes to the list of notified eIDs.

b) **(319 411-2/REG-6.2.2-02)** [QCP-n] and [QCP-n-qscd]: The identity of the natural person and, if applicable, any specific attributes of the person, shall be verified:
   a) by the physical presence of the natural person; or
   b) using methods which provide equivalent assurance in terms of reliability to the physical presence and for which the TSP can prove the equivalence.

A method according to alternative b) is used. Identity is verified by. Identity of the natural person is verified by use of a notified eID on European level of assurance High.

See also 3.2 a) above.

c) **(319 411-1/REG-6.2.2-02A)**: The TSP shall collect and validate either direct evidence or an attestation from an appropriate and authorized source, of the identity (e.g. name) and if applicable, any specific attributes of subjects to whom a certificate is issued.

BankID BankAxept AS will always base the issuance of certificates to natural persons on attested information from a Notified Identity Provider (NIdP) of level of assurance high or substantial.

The following attested information is collected from the NIdP:

- Unique identifier declared by the Notified Identity Provider.
- Full name.
- Date of birth
- National Identification Number (if available).

Additionally, BankID BankAxept AS will collect and validate sufficient information to get in contact with the subject either from the NIdP or from authenticated subjects directly.

d) **(319 411-1/REG-6.2.2-02B)**: Verification of the subject's identity shall be at time of registration by appropriate means.

Verification of the subject’s identity is always verified using a Notified Identity Provider at the time of registration.

e) **(319 411-1/REG-6.2.2-05)** [NCP] [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), evidence of the subject's identity (e.g. name) shall be checked against this natural person either directly by physical presence of the person (the subject shall be witnessed in person unless a duly mandated subscriber represents the subject), or shall have been checked indirectly using means which provides equivalent assurance to physical presence.

See letters a) to c) above.

f) **(319 411-1/REG-6.2.2-06)** [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), evidence shall be provided of:
   a) full name (including surname and given names consistent with the national identification practices);
   b) date and place 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.

See letters a) to c) above. The natural person will always be uniquely identified by the Notified Identity Provider's unique identifier.

g) **(319 411-1/REG-6.2.2-07)** [CONDITIONAL]: If the subject is a natural person (i.e. physical person as opposed to legal person), the place of birth should be given in accordance with national or other applicable conventions for registering births.

Not applicable, the place of birth is not required as distinguishing factor and is therefore not collected.

h) **(319 411-1/REG-6.2.2-18)**: The TSP shall record all the information necessary to verify the subject's identity and if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity.

Records sufficient to verify the subject's identity are archived.

See also [22] chapter 4.10 letter c).

i) **(319 411-1/REG-6.2.2-21)**: The subscriber shall provide a physical address, or other attributes, which describe how the subscriber shall be contacted.

As part of registration BankID BankAxept will collect sufficient information to contact the subscriber. For subscribers in Norway, this will be their national identification number which is sufficient to send electronic or physical letter post, using state-backed channels.

If sufficient information cannot be provided directly by the Identity Provider, BankID BankAxept AS will request additional contact information from the subscriber upon registration.

j) **(319 411-1/REG-6.2.2-22)**: The TSP shall provide evidence of how they meet applicable data protection legislation within their registration process.

BankID BankAxept AS operates in accordance with Norwegian Privacy Law [21]. Details on data processing is described in the terms and conditions.

BankID BankAxept AS has incorporated into its policies design principles and guidelines aimed at fostering "Privacy by Design", and has a group of data protection officers that regularly inspect products and services for compliance with the aforementioned polices.

k) **(319 411-1/REG-6.2.2-23)**: The TSP's verification policy shall only require the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the certificate.

BankID BankAxept AS has adopted the principle of "data minimization" ensuring that only required evidence of Subjects/Signers identity is captured required for issuing e-Signing Certificates to Subjects/Signers.

See also letter c) above.

l) **(319 411-1/REG-6.2.2-24A)**: To avoid any conflicts of interests, the subscriber and TSP organization entity shall be separate entities. The only exceptions are:

- A third party organization running all or part of the RA tasks in order to subscribe to certificates for subjects identified in association with it.
- Certificates that a TSP issues for itself (as a legal person) or natural persons belonging to it (as a subject).

BankID BankAxept AS operates according to this requirement.

BankID BankAxept AS will not be a subscriber to the Certificate Service, except when issuing certificates to natural persons employed by BankID BankAxept AS in their capacity as private persons.

m) **(319 411-1/REG-6.2.2-25)**: Certificates that a TSP issues for itself or persons belonging to it (as a subject) shall be requested, validated and handled according to the TSP's defined processes for the selected type of certificates.

BankID BankAxept AS has defined processes and routines for issuance, handling and life-cycle management of Certificates issued to BankID BankAxept AS systems, devices and personnel from the following CAs:

- Self-signed BankID BankAxept AS Root CA Certificates
- BankID BankAxept AS Subordinate CA Certificates
- BankID BankAxept AS TSU Certificates
- BankID BankAxept AS OCSP Responder Certificates

3.3 Identification and authentication for re-key requests

Not applicable. All BankID BankAxept AS certificates are short-lived certificates. Re-key is therefore not supported.

3.4 Identification and authentication for revocation request

a) **(319 411-1/REV-6.2.4-01)**: The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

a) Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.

b) How they can be submitted.

c) Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

d) Whether and for what reasons certificates can be suspended or revoked.

e) The mechanism used for distributing revocation status information.

f) The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties.

g) The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties.

Certificates issued by BankID BankAxept AS e-Sign CA to Subjects, are Short-term Certificates and the Private Signing Key is deleted immediately after use. Revocation services are not available for these Certificates.

Personnel in Trusted roles may perform revocation of CA, TSA and TSU certificates in accordance with established procedures and routines following the Security Officer's decision.

As an emergency precaution, revocation of any of BankID BankAxept AS CAs will be communicated to Subscribers, Subjects and Relying parties by removing the CA's CRL/CARL from BankID BankAxept AS web site. Such removal will be performed without any undue delay following a revocation.

b) **(319 411-1/REV-6.2.4-03A)**: The maximum delay between receipt of a certificate revocation or suspension request and the actual change of the certificate status information being available to all relying parties shall be at most 24 hours.

See letter a) above. Any change of Certificate status information will be made available to Relying Parties within 24 hours, see letter d) below.

c) **(319 411-1/REV-6.2.4-03B)** [CONDITIONAL]: If the revocation cannot be confirmed within 24 hours then the status need not be changed..

No stipulation, see letter a) above

d) **(319 411-1/REV-6.2.4-03C)** [CONDITIONAL]: If a TSP supports both CRL and on-line certificate status service to provide revocation status and delays in updating the status information for all the methods exist or are possible, the maximum delay of 24 hours shall apply to both methods.

BankID BankAxept AS Root-CAs issue CARLs. CARLs are publicly available on BankID BankAxept AS web site. OCSP is not supported.

BankID BankAxept AS TSA issue CRLs. CRLs are publicly available on BankID BankAxept AS web site.

Certificates issued by the e-Sign CA cannot be revoked. As such, both the CRL and OCSP will be in sync.

The maximum delay of 24 hours applies to publishing of CRLs.

e) **(319 411-1/REV-6.2.4-05A)** [CONDITIONAL]: If the revocation request requires revocation at a future date (e.g. subject's planned cessation from his/her duties at a certain date), then the scheduled date may be considered as the time at which receipt of the request has occurred.

Not applicable

f) **(319 411-1/REV-6.2.4-06A)**: A TSP may give faster process times than the time required in REV-6.2.4-03A for certain revocation reasons.

Not applicable

g) **(319 411-1/REV-6.2.4-07)**: The time used for the provision of revocation services shall be synchronized with UTC at least once every 24 hours.

Issuance of CRLs/CARLs and OCSP are synchronized with UTC at least once every 24 hours.

h) **(319 411-1/REV-6.2.4-08)**: Requests for revocation and reports of events relating to revocation shall be processed on receipt.

See letter a) above.

i) **(319 411-1/REV-6.2.4-09)**: Requests for revocation and reports of events relating to revocation shall be authenticated, checked to be from an authorized source.
NOTE 2: Such reports and requests will be confirmed as required under the TSP's practices.

See letter a) above

4 Certificate life-cycle operational requirements

4.1 Certificate Application

a) **(319 411-1/REG-6.3.1-01)** [CONDITIONAL]: If the subject's key pair is not generated by the CA, the certificate request process shall provide reasonable assurance that the subject has possession or control of the private key associated with the public key presented for certification.

The Subject's key pair is generated by the BankID BankAxept AS e-Signing Service as described in [23] chapter 3.1.

The certificate request process ensures Subject's control of the Private Signing Key by verifying the signed CSR submitted by the e-Signing Service. For information related to the CSR, see [23] chapter 3.3.

4.2 Certificate application processing

a) **(319 411-1/REG-6.3.2-01)**: Application for certificates shall be from a trusted and authorized source such as a registration service or a duly authenticated subscriber previously registered.

Certificates issued to Subjects/Signers by the BankID BankAxept AS e-Sign CA are securely and unambiguously linked to the Subject/Signer registration and identification process described in chapter 3.2 above, and in [23] chapters 3.3 and 4.1.

BankID BankAxept AS e-Sign CA only issues Certificates to Subjects based on authenticated and signed CSRs received from BankID BankAxept AS e-Signing Service, see [23] chapter 3.2.

b) **(319 411-1/REG-6.3.2-02)** [CONDITIONAL]: When external registration service providers are used registration data shall be exchanged securely and only with recognized registration service providers, whose identity is authenticated.

Not applicable

4.3 Certificate issuance

a) **(319 411-1/GEN-6.3.3-01)**: The CA shall issue certificates securely to maintain their authenticity.

BankID BankAxept AS CAs are trustworthy systems. CAs maintain Certificate authenticity by digitally signing the Certificates using their CA Private Key which resides in evaluated and certified HSM [1].

b) **(319 411-1/GEN-6.3.3-02)**: The CA shall take measures against forgery of certificates.

Forgery of Certificates is prevented by the processes established controlling access to the Private CA Signing Keys and software, choice of appropriate cryptographic CA signature algorithm, as well as controls protecting the integrity of data (Certificates) to be signed.

c) **(319 411-1/GEN-6.3.3-02A)** [NCP]: The CA should introduce randomness in certificate's serial number.

Randomness in Certificate's serial number is ensured by the CA software.

d) **(319 411-1/GEN-6.3.3-03)** [CONDITONAL]: In cases where the CA generates the subjects' key pair, the CA shall guarantee confidentiality during the process of generating such data.

BankID BankAxept AS generates the subject's key pair as part of the issuance process. The subject's private key is generated inside a Qualified Signature Creation Device, only used for one signature session and is promptly deleted afterwards. This guarantees the confidentiality of this key.

e) **(319 411-1/GEN-6.3.3-04)**: The procedure of issuing the certificate shall be securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject-generated public key.

Each certificate issuance process is uniquely linked to a single authentication process by a Notified Identity Provider (NIdp). The sessions are bound together by a single use challenge value (nonce) which is propagated through the whole authentication process and verified during provisioning of the certificate.

f) **(319 411-1/GEN-6.3.3-05)**: The TSP should not issue certificates whose lifetime exceeds that of the CA's signing certificate.

None of BankID BankAxept AS CAs issues Certificates whose lifetime exceeds the lifetime of the CA's signing Certificate.

g) **(319 411-1/GEN-6.3.3-07)** [CONDITIONAL]: If the CA generated the subject's key pair, the procedure of issuing the certificate shall be securely linked to the generation of the key pair by the CA.

The CA ensures that the generated key pair is securely linked to the issued certificate. Technically this is ensured by validation of a certificate signing request generated in the Qualified Signature Creation Device.

h) **(319 411-1/SDP-6.3.3-09A)** [NCP+][CONDITIONAL]: If the TSP generated the subject's key pair, the secure cryptographic device containing the subject's private key shall be securely delivered to the registered subject or, in the case of a third party TSP managing the key on behalf of the subject, to that third party TSP.

Not applicable. BankID BankAxept is managing the subject's private key on behalf of the subject. Therefore the subject's private key is never delivered to the subject.

i) **(319 411-1/GEN-6.3.3-10)**: Re-assignment of distinguish name [CHOICE]:
- [All policies except DVCP]: Over the life time of the CA a subject distinguished name which has been used in a certificate shall never be re-assigned to another subject.

BankID BankAxept AS e-Sign CA are issuing Certificates to Subjects/Signers based on the CSR received from BankID BankAxept AS e-Signing Service. As described in [23] chapter 3.2 letter e) the Subjects/Signers person identification data combined with the eID means used constitutes the Subjects/Signers DN in the CSR thus ensuring that a Subjects/Signers DN will not be re-assigned to another Subject/Signer.

j) **(319 411-1/GEN-6.3.3-11)** [CONDITIONAL]: If a certificate is issued to a natural person identified in association with the legal person, then the subject attributes identifying the organization in the certificate should represent the legal person or sub-entity of that legal person and the subject identifier in the certificate shall be the natural person.

Not applicable

k) **(319 411-1/GEN-6.3.3-12)**: The CP identifier shall be [CHOICE]:

• [NCP]:
- as specified in clause 5.3 item a); and/or
- an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.
• [NCP+]:
- as specified in clause 5.3 item b); and/or
- an OID, allocated by the TSP, other relevant stakeholder or further standardization for a certificate policy enhancing the policy requirements defined in the present document.

The CP identifier for the policy reflected in this TSPS document is either [QCP-n-qscd] or [NCP+] depending on the level of assurance used during the issuance process.

For the Certificates issued to Subjects authenticating with a Notified Identity Provider (NIdP) notified as level of assurance high the CP identifier shall be [QCP-n-qscd].

For the Certificates issued to Subjects authenticating with a Notified Identity Provider (NIdP) notified as level of assurance substantial the CP identifier shall be [NCP+].

4.4 Certificate acceptance

a) **(319 411-1/OVR-6.3.4-01)**: The terms and conditions shall indicate what is deemed to constitute acceptance of the certificate. See clause 6.9.4.

The terms and conditions clearly indicate that authenticating the request to sign constitutes the Subject's acceptance of the Certificate issued by BankID BankAxept AS.

b) **(319 411-1/REG-6.3.4-02)**: Before entering into a contractual relationship with a subscriber, the TSP shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 6.9.4.

BankID BankAxept AS e-Signing Service informs the Subject/Signer by presenting the authenticated Subject/Signer with the terms and conditions before enrolling to the service and generating a CSR.

c) **(319 411-2/OVR-6.3.4-02)** [CONDITIONAL]: If the subscriber agreement is in electronic form, it should be signed with an Advanced Electronic Signature or an Advanced Electronic Seal as specified by Regulation (EU) No 910/2014 [i.14].

Following authentication of Subject/Signer as described in chapter 3.2, the Subject/Signer acknowledges agreement to the terms and conditions presented by means of a traceable action, e.g. ticking a box. All activities, presentation of terms and conditions and acknowledge of acceptance, is logged but not signed.

This evidence is retained for 7 years.

d) **(319 411-1/REG-6.3.4-03)** [CONDITIONAL]: If the subject is a person (i.e. not a device), and not the same as the subscriber, the subject shall be informed of his/her obligations.

Not applicable

e) **(319 411-1/OVR-6.3.4-04)**: The TSP shall communicate the terms and conditions through a durable (i.e. with integrity over time) means of communication, and in a human readable form before the agreement.

See letter f) below.

f) **(319 411-1/OVR-6.3.4-05)**: The terms and conditions may be transmitted electronically.

Terms and Conditions is available on BankID BankAxept AS web site and Subject/Signer is always presented with link to them to read and understand before accepting them.

Terms and conditions are possible to download, both in current and previous versions.

g) **(319 411-1/OVR-6.3.4-06)**: The terms and conditions may use the model PKI disclosure statement given in annex A.

BankID BankAxept AS terms and conditions is formatted in accordance with BankID BankAxept AS internal rules for public documents. The model in annex A of ETSI EN 319 411-1 [15] will be used.

h) **(319 411-1/REG-6.3.4-07)**: The TSP shall record the agreement with the subscriber and if the subscriber and subject are two separate entities and the subject is a natural or legal person, with the subject.

See letter c) above.

i) **(319 411-1/REG-6.3.4-08)**: The agreement in requirement REG-6.3.4-07 shall involve explicit acceptance of the terms and conditions by a wilful act which can be later supported by evidence.

See letter c) above.

j) **(319 411-1/REG-6.3.4-12)** [CONDITIONAL]: If the subject and subscriber are the same entity or the subject is a device, the agreement shall be in one or two parts.

The terms and conditions constituting the agreement are in only one part.

k) **(319 411-1/REG-6.3.4-13)** [CONDITIONAL]: If the subject and subscriber are the same entity or the subject is a device, the agreement shall include the part 1 (see REG-6.3.4-10) and part 2 (see REG-6.3.4-11) items listed above.

See letter j) above

l) **(319 411-1/REG-6.3.4-16)** : The agreement may be in electronic form.

The terms and conditions constituting the agreement are in electronic form, available as described in chapter 2 letter e) above.

m) **(319 411-1/REG-6.3.4-17)**: The records identified above shall be retained for the period of time as indicated to the subscriber (as part of the terms and conditions).

All logged activities constituting agreement as described in letter c) above are retained for 7 years as described in [22] chapter 4.10.

4.5 Key pair and certificate usage

a) **(319 411-1/OVR-6.3.5-01)**: The subscriber's obligations (see clause 6.3.4) shall include:
   a) an obligation to provide the TSP with accurate and complete information in accordance with the requirements of the present document, particularly with regards to registration;

Not Applicable. During registration Subjects are identified and authenticated by Notified eID Providers as described in chapter 3.2 and in [23] chapters 3.2 and 4.1. No further information is required from the subject.

b) an obligation for the key pair to be only used in accordance with any limitations notified to the subscriber and the subject if the subject is a natural or legal person;

Not applicable. BankID BankAxept AS governs all access to the Subject's Private Key and will ensure that it is only used as intended.

c) prohibition of unauthorized use of the subject's private key;

Not applicable. See letter b) above.

f) [NCP+] an obligation to only use the subject's private key(s) for cryptographic functions within the secure cryptographic device;

Subject's Private signing Key is only used inside the same QSCD/SCDev where it was generated.

h) an obligation to notify the TSP without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate:

i) the subject's private key has been lost, stolen, potentially compromised;
ii) control over the subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons;
iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject;

Certificates issued to Subjects by BankID BankAxept AS e-Sign CA are Short-term and the Private signing Key is deleted immediately after use. Subjects have an obligation to notify if they find errors in certificate contents. This is covered in Terms & Conditions.

i) an obligation, following compromise of the subject's private key, to immediately and permanently discontinue the use of this key, except for key decipherment; and

Not applicable. The Subject's Private Key is only available for one signing session and then immediately destroyed.

j) an obligation, in the case of being informed that the subject's certificate has been revoked, or that the issuing CA has been compromised, to ensure that the private key is no longer used by the subject.

Certificates issued to Subjects by BankID BankAxept AS e-Sign CA are Short-term and no revocation service is available. The private key cannot be used by the Subject after a CA compromise.

b) **319 411-2/SDP-6.3.5-02)** [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: If the TSP manages the QSCD for the subject, the private key shall not be used for signing except within a QSCD.

Subjects Private signing Keys are only available for signing operations within a QSCD as described in [23] chapter 4.

c) **(319 411-1/OVR-6.3.5-03)**: The notice to relying parties (see clause 6.9.4) shall recommend the Relying Party to:

a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the Relying Party (see clause 6.9.4);
b) 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 supplied as required in clause 6.9.4; and
c) take any other precautions prescribed in agreements or elsewhere.

The terms and conditions with the above recommendations, are made available to Relying Parties on BankID BankAxept AS web site, see [22] chapter 3.1 letter e)

d) **(319 411-2/SDP-6.3.5-03)** [QCP-n-qscd] [CONDITIONAL]: If the TSP manages the QSCD for the subject, the subject's private key shall be used under the subject's sole control.

See [23] chapter 4

e) **(319 411-1/OVR-6.3.5-04)** [NCP][CONDITIONAL]: If the TSP manages the private key on behalf of the subject and the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9], the TSP shall ensure that the subject has sole control (or if the subject is a legal person, "control") over its private key.

See [23] chapter 4

f) **(319 411-1/OVR-6.3.5-05)** [NCP][CONDITIONAL]: If a third party TSP manages the private key on behalf of the subject and the certificate key usage is of type A, B, or F as specified in clause 4.3.2 of ETSI EN 319 412-2 [9], the TSP shall confirm that the TSP managing the key ensures that the subject has sole control (or if the subject is a legal person, "control") over its private key.

Not applicable – BankID BankAxept AS is not a third party TSP

g) **(319 411-2/SDP-6.3.5-05)** [QCP-n-qscd] [CONDITIONAL]: If the TSP manages the QSCD for the subject, the subject's key pair should be used only for electronic signatures.

See [23] chapter 4

h) **(319 411-1/OVR-6.3.5-06)**: Conformance to ETSI TS 119 431-1 [**Error! Reference source not found.**, should be used to demonstrate that the TSP managing the key on behalf of the subject meets the requirements for ensuring (sole) control as required in OVR-6.3.5-04 or OVR-6.3.5-05.

See [23] chapters 4.1 and 4.2

i) **(319 411-2/OVR-6.3.5-07)** [QCP-n-qscd] and [QCP-l-qscd]: The subscriber's obligations (see clause 6.3.4) (or respectively the obligations on the TSP managing the key on behalf of the subject) shall require that digital signatures are only created by a QSCD device.

See [23] chapters 3 and 4

j) **(319 411-2/SDP-6.3.5-08)** [QCP-n] and [QCP-n-qscd]: The subscriber's obligations (see clause 6.3.4) (or respectively the obligations on the TSP managing the key on behalf of the subject) shall require that the subject's private key is maintained (or respectively is used) under the subject's sole control.

See [23] chapter 4

k) **(319 411-2/SDP-6.3.5-10)** [QCP-n] and [QCP-n-qscd]: The subscriber's obligations (see clause 6.3.4) or the obligations on the TSP managing the key on behalf of the subject should recommend that the subject's key pair is used only for electronic signatures.

Subjects/Signers Key pair is only available for signing operations as described in [23]

l) **(319 411-2/OVR-6.3.5-12)**: The notice to relying parties shall inform them that, as part of the conditions for a certificate to be relied upon as an EU Qualified Certificate, the trust anchor for the validation of the certificate shall be as identified in a service digital identifier of an appropriate EU trusted list entry for a QTSP (see ETSI TS 119 612 [i.12]).

The terms and conditions include a link to the BankID BankAxept AS eSign CA and TSA CA entries in the EU trusted list.

4.6 Certificate renewal

Certificate renewal is not available for Certificates issued by BankID BankAxept AS e-Sign CA to Subjects/Signers.

4.7 Certificate re-key

Certificate re-key is not provided for Certificates issued by BankID BankAxept AS e-Sign CA to Subjects/Signers.

4.8 Certificate modification

Not applicable for Certificates issued to Subjects/Signers. BankID BankAxept AS certificates for Signers are Short-term.

4.9 Certificate revocation and suspension

a) **(319 411-1/CSS-6.3.9-02) – (319 411-1/CSS-6.3.9-04):**

Not applicable for Certificates issued to Subjects/Signers. BankID BankAxept AS certificates for Signers are Short-term.

b) **(319 411-1/CSS-6.3.9-05)** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates are used, including any variants, *either the CRL or the variant* shall be published at least every 24 hours.

Full CRLs, supporting validation services requiring CRL to be present, concerning Subjects' Certificates are published every 24 hours on BankID BankAxept AS web site, see [22] chapter 3.1 letter e).

c) **(319 411-1/CSS-6.3.9-06)** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, every CRL shall state a time for next scheduled CRL issue, unless it is the last CRL issued for those certificates in the scope of the CRL, in which case the nextUpdate field in the CRL defined in IETF RFC 5280 [7], should be set to "99991231235959Z".

Both CARLs and CRLs issued by BankID BankAxept AS CAs state the time for next scheduled issuance.

The nextUpdate field in the last CARL and CRL to be issued by the respective CAs will be set to "99991231235959Z".

d) **(319 411-1/CSS-6.3.9-07)** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, a new CRL may be published before the stated time of the next CRL issue.

CRLs for end users will always be empty.

e) **(319 411-1/CSS-6.3.9-08)** [CONDITIONAL]: If Certificate Revocation Lists (CRLs) concerning end users certificates including any variants (e.g. Delta CRLs) are used, the CRL shall be signed by the CA or an entity designated by the TSP.

CRLs issued by BankID BankAxept AS e-Sign CA are signed by BankID BankAxept AS e-Sign CA.

f) **(319 411-1/CSS-6.3.9-12)** [CONDITIONAL]: If CARL is used, a new CARL shall be generated at least once a year with a nextUpdate of at most 1 year after the issuing date.

BankID BankAxept AS Root CA issue a new CARL at least once a year and within the date included in the nextUpdate field of the CARL.

g) **(319 411-1/CSS-6.3.9-13)** [CONDITIONAL]: If CARL is used, a new CARL shall be generated once a CA certificate has been revoked.

BankID BankAxept AS Root CA will issue a new CARL immediately after revoking any subordinate CA Certificate.

h) **(319 411-1/CSS-6.3.9-14)**: In the case of any cross-certificates issued by the CA to other TSPs, the CARL should be issued at least every 31 days.

Not applicable

i) **(319 411-1/REV-6.3.9-15)**: A TSP need not have a revocation management service to address requirements REV-6.2.4-01, REV-6.2.4-03A, REV-6.2.4-03BA, REV-6.2.4-05A to REV-6.2.4-09, REV-6.3.9-01, REV-6.3.9-02 and SDP-6.5.1-21 for short-term certificates, as these requirements are not necessarily applicable to short-term certificates.

BankID BankAxept AS does not provide any revocation management service for Certificates issued by BankID BankAxept AS e-Sign CA to Subjects/Signers since the CA is only issuing non-revocable Short-term Certificates.

j) **(319 411-1/REV-6.3.9-15A)** [CONDITIONAL]: For short-term certificates which can be revoked the TSP shall fulfil requirements REV-6.2.4-01, REV-6.2.4-03A, REV-6.2.4-03BA, REV-6.2.4-05A to REV-6.2.4-09, REV-6.3.9-01, REV-6.3.9-02 and SDP-6.5.1-21.

Not applicable. BankID BankAxept AS does not offer revocation of short-term Certificates.

k) **(319 411-1/REV-6.3.9-16)**: A TSP issuing short-term certificates shall explicitly describe in the CPS which certificates cannot be revoked through a revocation management service and which certificates cannot be revoked even by the TSP on its own initiative.

The Short-term end-user certificates issued by the BankID BankAxept AS eSign CA cannot be revoked, even by the TSP. This is also described in the CPS.

4.10 Certificate status services

a) **(319 411-1/CSS-6.3.10-01)**: The TSP shall provide services for checking the status of the certificates.

BankID BankAxept AS provides Certificate status checking services:

- BankID BankAxept AS Root CA are issuing CARLs, and
- Both BankID BankAxept AS TSA CA and BankID BankAxept AS e-Sign CA are issuing CRLs.
- BankID BankAxept AS e-Sign CA are supporting OCSP providing status information to BankID BankAxept AS signature service to be included in the document signature.

Both CARLs and CRLs will be communicated to Subscribers, Subjects and Relying parties and made available on BankID BankAxept AS web site.

b) **(319 411-1/CSS-6.3.10-02)**: Revocation status information shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the CPS.

Revocation status information is available on BankID BankAxept AS web site 24/7 as described in [22] chapter 3.1 letter e).

BankID BankAxept AS will apply best endeavours to ensure that maximum time the information is unavailable is 60 minutes.

c) **(319 411-1/CSS-6.3.10-03)**: The integrity and authenticity of the status information shall be protected.

The integrity of the status information provided in the CARLs and CRLs are ensured by them being digitally signed by the respective CA issuing the CARL/CRL.

d) **(319 411-1/CSS-6.3.10-04)**: Revocation status information shall include information on the status of certificates at least until the certificate expires.

Information in CARLs and CRLs includes Certificate revocation status information on all non-expired Certificates.

e) **(319 411-1/CSS-6.3.10-05)**: OCSP or CRL shall be supported.

All BankID BankAxept AS CAs support CARLs or CRLs.
BankID BankAxept AS e-Sign CA also support OCSP available to BankID BankAxept AS signature service only.

f) **(319 411-1/CSS-6.3.10-06)**: OCSP should be supported.

See letter e) above

g) **(319 411-1/CSS-6.3.10-08)** [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, any updates to revocation status shall be available for all methods.

Both CRL and OCSP issued by BankID BankAxept AS e-Sign CA are updated supporting validation services requiring CRL and/or OCSP to be present also for non-revocable Short-term Certificates. The CRL will always be empty and the OCSP will always return “Good” within the Certificate lifetime.

h) **(319 411-1/CSS-6.3.10-09)** [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status, the information provided by all services shall be consistent over time taking into account different delays in updating the status information for all the methods.

See letter g) above.

Revocation status information provided is consistent over time.

i) **(319 411-1/CSS-6.3.10-9A)** [CONDITIONAL]: If a TSP supports multiple methods (CRL and on-line certificate status service) to provide revocation status and delays in updating the status information for all the methods exist or are possible, the TSP shall document in its CPS the origin of such delays and how to interpret the results in case of differences.

See letter d) above

j) **(319 411-1/CSS-6.3.10-10)**: The revocation status information shall be publicly and internationally available.

CARLs and CRLs issued by BankID BankAxept CAs are publicly and internationally available on BankID BankAxept AS web site as described in [22] chapter 3.1 letter e)

k) **(319 411-2/CSS-6.3.10-02)**: Revocation status information shall be made available beyond the validity period of the certificate with at least one of the methods used during the period of validity of the certificate (i.e. CRL or OCSP).

Revocation status information will always be possible to find in an updated CRL.

End user certificates cannot be revoked and will never occur in the CRL.

Revoked TSUs or CAs will be present in CRL/CARLs, also after the end of validity.

l) **(319 411-2/CSS-6.3.10-03)** [CONDITIONAL]: If CRLs are provided, the TSP should not remove from the CRL revoked certificates after they have expired.

Revoked Certificates are not removed from CRLs after end of the Certificate's validity period.

m) **(319 411-2/CSS-6.3.10-04)** [CONDITIONAL]: If CRLs are provided and no alternative means (e.g. OCSP) are provided for revocation status information on expired certificates, the TSP shall not remove from the CRL revoked certificates after they have expired.

See letter l) above

n) **(319 411-2/CSS-6.3.10-05)** [CONDITIONAL]: If CRLs are provided and the TSP does not remove from the CRL revoked certificates after they have expired, the CRL shall include the X.509 "ExpiredCertsOnCRL" extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

The "ExpiredCertsOnCRL" extension is included in the CRL profile.

o) **(319 411-2/CSS-6.3.10-06)** [CONDITIONAL]: If CRLs are provided and the TSP removes from the CRL revoked certificates after they have expired, the CRL shall not include the X.509 "ExpiredCertsOnCRL" extension as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6].

Not applicable.

p) **(319 411-2/CSS-6.3.10-07)** [CONDITIONAL]: If CRLs are provided and the TSP decides or is required to terminate a CRL, the TSP should issue and publish at the corresponding CRL Distribution Point a last CRL with a nextUpdate field value as defined in ETSI EN 319 411-1 [15], clause 6.3.9 Requirement CSS-6.3.9-06.

See chapter **Error! Reference source not found.** letter c)

q) **(319 411-2/CSS-6.3.10-08)** [CONDITIONAL]: If CRLs are provided, the TSP should preserve the integrity and the availability of the last CRL at least for the period specified in the CPS as requested in CSS-6.3.10-12.

The integrity of any last CRL issued by a BankID BankAxept AS CA is preserved. Last CRLs will be stored and preserved for a period of 7 years.

r) **(319 411-2/CSS-6.3.10-09)** [CONDITIONAL]: If CRLs are provided, the TSP shall not issue a last CRL until all certificates in the scope of the CRL are either expired or revoked.

BankID BankAxept AS CAs will not issue a last CRL, ref. chapter **Error! Reference source not found.** letter c), until all Certificates in the scope the CRL are either revoked or expired.

s) **(319 411-2/CSS-6.3.10-10)** [CONDITIONAL]: If OCSP is provided, the OCSP responder should use the ArchiveCutOff extension as specified in IETF RFC 6960 [11], with the archiveCutOff date set to the CA's certificate "notBefore" time and date value.

Not supported. OCSP responder is not publicly available.

t) **(319 411-2/CSS-6.3.10-11)** [CONDITIONAL]: If OCSP is provided and the CA's certificate is about to expire, the TSP may compute a last OCSP answer for each and every issued certificate (whether revoked or not), with the "nextUpdate" field set to "99991231235959Z".

Not supported

u) **(319 411-2/CSS-6.3.10-12)**: The TSP shall document precisely in its practices statements and in its terms and conditions how requirements CSS-6.3.10-02 to CSS-6.3.10-11 are met, including:

a) the period over which the revocation status information is made available;
b) how the revocation status information is provided in the case of CA's key compromise;
c) how the revocation status information is provided in the case of TSP termination (see clause 6.4.9).

a) Revocation status information is available for at least 7 years,

b) In the event of CA key compromise, a new CRL will be issued signed by an uncompromised CA key

c) Revocation status information will be kept available for 7 years, through agreement with a service provider

In addition, see letters b) to t) above.

v) **(319 411-2/CSS-6.3.10-13)** [CONDITIONAL]: If the TSP is managing the subject's private key and assures that the certificate is valid at the time of use of the private key, this information should be indicated in its practices statements or certificate policy, and may also be derived from the subject's certificate.

BankID BankAxept AS is managing Subject's/Signer's Private signing Key as described in [23] chapters 3 and 4. This information is readily available both from the PDS, this document and from Subject's/Signer's Certificate by including the validity assured extensions ext-etsi-valassured-ST-certs and QCP-n-qscd, see chapter 7.1 letter c).

4.11 End of subscription

No policy requirement.

4.12 Key escrow and recovery policy and practices

Not applicable. Key escrow and recovery are not supported. The Subjects' private signing keys are only available for a single signing session and then immediately destroyed.

5 Facility, management, and operational controls

5.1 General

a) **(319 411-1/OVR-6.4.1-01)**: The requirements identified in ETSI EN 319 401 [8], clauses 5, 6.3 and 7.3, shall apply.

See [22] chapters 2, 3.3 and 4.3

5.2 Physical controls

See [22] chapter 4.6.1, sub-heading "Certificate Service" for a description on established physical controls

5.3 Procedural controls

See [22] chapters 4.4 and 4.4.1 for a description on established physical controls

5.4 Personnel controls

a) **(319 411-1/OVR-6.4.4-01)**: The requirements identified in ETSI EN 319 401 [8], clause 7.2 shall apply.

See [22] chapter 4.2

b) **(319 411-1/OVR-6.4.4-02)**: In addition to the trusted roles identified in ETSI EN 319 401 [8], (7.2-15), the trusted roles of the registration and revocation officers with responsibilities as defined in TS 419 261 [i.9] should be supported.

Not applicable, revocation is not supported and registration is automated.

5.5 Audit logging procedures

See [22] chapters 4.10 and chapter 4.10.1, sub-heading “Certificate Service” for a description of established audit logging procedures

5.6 Records archival

a) **(319 411-1/OVR-6.4.6-01)**: The TSP shall retain the following for at least seven years after any certificate based on these records ceases to be valid:

a) log of all events relating to the life cycle of keys managed by the CA, including any subject key pairs generated by the CA (see requirement GEN-6.4.5-08);
b) documentation as identified in clause 6.3.4.

See [22] chapter 4.10

b) **(319 411-2/OVR-6.4.5-03)**: The information shall be maintained as necessary to meet legal requirements beyond the termination of the TSP (see clause 6.4.9).

See [22] chapter 4.12

5.7 Key changeover

No policy requirement.

5.8 Compromise and disaster recovery

See [22] chapters 4.11 and 4.11.1, sub-heading “Certificate Service” for a description on compromise and disaster and recovery controls

5.9 CA or RA termination

a) **(319 411-1/OVR-6.4.9-01)**: The requirements identified in ETSI EN 319 401 [8], clause 7.12, shall apply.

See [22] chapter 4.12

b) **(319 411-1/OVR-6.4.9-02)**: Requirement REQ-7.12-06 of ETSI EN 319 401 [8], shall apply to the following information for their respective period of time as indicated to the subscriber and Relying Party (see in particular REG-6.3.4-17 and CSS-6.3.10-02):

a) registration information (see clauses 6.2.2, 6.3.1 and 6.3.4);
b) revocation status information (see clause 6.3.10);
c) event log archives (see clauses 6.4.5 and 6.4.6).

See [22] chapter 4.12 letter f)

c) **(319 411-1/OVR-6.4.9-03)**: Requirement REQ-7.12-10 of ETSI EN 319 401 [8], shall also include the handling of the revocation status for unexpired certificates that have been issued.

End user certificates will be short-term certificates, eliminating the need for handling revocation status after expiry.

See also [22] chapter 4.12 letter j)

d) **(319 411-1/OVR-6.4.9-04)**: When another cross certified TSP stops all operations, including handling revocation (see OVR-6.4.9-03), all cross certificates to that TSP shall be revoked. NOTE: Affected entities to be informed of termination under ETSI EN 319 401 [8], REQ-7.12-10 include crosscertified TSP.

Not applicable

6 Technical security controls

6.1 Key pair generation and installation

a) **(319 411-1/OVR-6.5.1-01)**: The requirements identified in ETSI EN 319 401 [8], clause 7.5, shall apply.

See [22] chapter 4.5

b) (**319 411-1/GEN-6.5.1-02)**: The TSP shall generate CA keys, including keys used by revocation and registration services, securely and the private key shall be secret.

All BankID BankAxept AS CAs keys are generated, stored, and used in HSMs certified in accordance with ISO/IEC 15408 with assurance level EAL 4+ ensuring the secrecy of Private CA keys.

c) **(319 411-1/GEN-6.5.1-03)**: The CA key pair generation and the subsequent certification of the public key, shall be undertaken in a physically secured environment (see clause 6.4.2) by personnel in trusted roles (see clause 6.4.4).

See letter b) above.

All HSMs used by BankID BankAxept AS Trust Services are placed in High security zones as described in [22] chapter 4.6 letter e) and chapter 4.6.1 sub-heading “Certificate Services”. Only personnel in trusted roles have access to High security zones and are authorized to perform CA key generation.

d) **(319 411-1/GEN-6.5.1-04)**: The CA key pair used for signing certificates shall be created under, at least, dual control.

All BankID BankAxept AS CAs keys are generated are generated under, at least, dual control by personnel in trusted roles.

e) **(319 411-1/GEN-6.5.1-05)**: The number of personnel authorized to carry out CA key pair generation shall be kept to a minimum and be consistent with the TSP's practices.

Personnel in trusted roles authorized to perform key pair generation for BankID BankAxept AS CAs are appointed by BankID BankAxept AS management in accordance with the practices described in [22] chapter 4.2. The number of personnel in these roles are in line with resource requirements to maintain the service operations and security requirements.

f) **(319 411-1/GEN-6.5.1-06)**: CA key pair generation should be performed using an algorithm as specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

BankID BankAxept AS CAs key pair generation are performed using EC-DSA algorithm from NIST curve family as specified in [i.10].

g) **(319 411-1/GEN-6.5.1-07)**: The selected key length and algorithm for CA signing key should be one which is specified in ETSI TS 119 312 [i.10] for the CA's signing purposes.

The selected key length and algorithm for all BankID BankAxept AS CAs are secp384r1 NIST P-384 and SHA-384.

h) **(319 411-1/GEN-6.5.1-08)**: Before expiration of its CA certificate which is used for signing subject keys (for example as indicated by expiration of CA certificate), in case of continuing with the service, the CA shall generate a new certificate for signing subject key pairs, and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA certificate.

BankID BankAxept AS have processes in place ensuring that new CA Certificates for signing Certificates are issued prior to expiration, ensuring continuous operations of the BankID BankAxept AS Trust services.

i) **(319 411-1/GEN-6.5.1-09)**: Before expiration of its CA certificate which is used for signing subject keys (for example, as indicated by expiration of CA certificate), in case of continuing

with the service, the new CA certificate shall also be generated and distributed in accordance with the present document.

New CA Certificates are generated and distributed in accordance with the established procedures for the various CA Certificates.

j) **(319 411-1/GEN-6.5.1-10)**: The operations described in GEN-6.5.1-08 and GEN-6.5.1-09 should be performed with a suitable interval between certificate expiry date and the last certificate signed to allow all parties that have relationships with the TSP (subjects, subscribers, relying parties, CAs higher in the CA hierarchy, etc.) to be aware of this key changeover and to implement the required operations to avoid inconveniences and malfunctions. This does not apply to a TSP which will cease its operations before its own certificate-signing certificate expiration date.

BankID BankAxept AS have processes in place applying all necessary actions to avoid disruption to the operations of any entity that may rely on any of BankID BankAxept AS CA certificates.

k) **(319 411-1/GEN-6.5.1-11)**: The TSP shall have a documented procedure for conducting CA key pair generation for certificate signing keys for all CAs, whether root CAs or subordinate CAs, including CAs that issue certificates to end users.

BankID BankAxept AS CA Key ceremonies are conducted in the CA operations facilities in accordance with documented and established procedure by personnel in trusted roles authorized for conducting CA Key ceremonies.

Key ceremonies involving generation of BankID BankAxept AS Root CA Private Keys are under supervision of an independent auditor.

l) **(319 411-1/GEN-6.5.1-12)**: The procedure of GEN-6.5.1-11 shall indicate, at least, the following:

a) roles participating in the ceremony (internal and external from the organization);
b) functions to be performed by every role and in which phases;
c) responsibilities during and after the ceremony; and
d) requirements of evidence to be collected of the ceremony.

BankID BankAxept AS have documented procedures for Key ceremonies covering all elements described above.

m) **(319 411-1/GEN-6.5.1-13)**: The TSP shall produce a report proving that the ceremony, as in GEN-6.5.1-11 above, was carried out in accordance with the stated procedure and that the integrity and confidentiality of the key pair was ensured.

BankID BankAxept AS produces a key ceremony report signed by participants of the ceremony.

n) **(319 411-1/GEN-6.5.1-14)**: This report shall be signed [CHOICE]:

For root CA: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) and a trustworthy person independent of the TSP's management (e.g. Notary, auditor) as witness that the report correctly records the key management ceremony as carried out.
For subordinate CAs: by the trusted role responsible for the security of the TSP's key management ceremony (e.g. security officer) as witness that the report correctly records the key management ceremony as carried out.

See letter m) above.

The Root CA ceremony report is also signed by the independent auditor witnessing the ceremony.

o) **(319 411-1/DIS-6.5.1-16)**: CA signature verification (public) keys shall be available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.

BankID BankAxept AS Root CA Certificate is made available at BankID BankAxept AS web site and the EU Trusted list, see [22] chapter 3.1 letter e).

p) **(319 411-1/SDP-6.5.1-17)** [CONDITIONAL]: If the CA generates the subject's keys, CA-generated subject keys shall be generated using an algorithm recognized as being fit for the uses identified in the CP during the validity time of the certificate.

Subjects Signer keys are generated by BankID BankAxept AS e-Signature service as described in [23] chapter 3.1

q) **(319 411-1/SDP-6.5.1-18)** [CONDITIONAL]: If the CA generates the subject's keys, CA-generated subject keys should be of a key length and for use with a public key algorithm as specified in ETSI TS 119 312 [i.10] for the purposes stated in the CP during the validity time of the certificate.

See [23] chapter 3.1 letter g)

r) **(319 411-1/SDP-6.5.1-19)** [CONDITIONAL]: If the CA generates the subject's keys, CA-generated subject keys shall be generated and stored securely whilst held by the TSP.

See [23] chapter 3.1

s) **(319 411-1/SDP-6.5.1-20)** [CONDITIONAL]: If the CA generates the subject's keys, the subject's private key shall be delivered to the subject's device or to the TSP managing the subject's private key, in a manner such that the secrecy and integrity of the key is not compromised.

See [23] chapters 3.1 and 4

t) **(319 411-1/SDP-6.5.1-21)** [CONDITIONAL]: If the CA generates the subject's keys and if the TSP or any of its designated RAs become aware that a subject's private key has been communicated to an unauthorized person or an organization not affiliated with the subject, then the TSP shall revoke all certificates that include the public key corresponding to the communicated private key.

Not applicable. BankID Bank Axept AS signing keys are Short-term keys, and revocation service is not offered.

u) **(319 411-1/SDP-6.5.1-22)** [CONDITIONAL]: If the CA generates the subject's keys, the CA shall delete all copies of a subject private key after delivery of the private key to the subject, except for conditions as described in clause 6.3.12.

See [23] chapters 3.1 and 4

v) **(319 411-1/SDP-6.5.1-23)** [NCP+] [CONDITIONAL]: If the CA generates the subject's keys, the TSP shall secure the issuance of a secure cryptographic device to the subject.

See [23] chapters 3.1 and 4

w) **(319 411-1/SDP-6.5.1-24)** [CONDITIONAL]: If the CA generates the subject's keys, secure cryptographic device preparation shall be done securely.

See [23] chapters 3.1 and 4

x) **(319 411-1/SDP-6.5.1-25)** [CONDITIONAL]: If the CA generates the subject's keys, secure cryptographic device shall be securely stored and distributed.

See [23] chapters 3.1 and 4

y) **(319 411-2/SDP-6.5.1-02)** [QCP-n-qscd] and [QCP-l-qscd]: Whether the device is prepared by the TSP or not, the TSP shall verify that the device is certified as a QSCD.

See [23] chapter 3.1

z) **(319 411-2/SDP-6.5.1-03)** [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: If the device is managed by a third party TSP on behalf of the subject which is not the TSP issuing the certificate itself, the TSP issuing the certificate shall verify that this third party TSP is meeting the appropriate requirements in terms of qualification.

Not applicable

aa) **(319 411-2/SDP-6.5.1-04)** [QCP-n-qscd] and [QCP-l-qscd]: The certificate request process shall ensure that the public key to be certified is from a key pair generated by a QSCD.

See [23] chapter 3

bb) **(319 411-2/SDP-6.5.1-05)** [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: If the subject's key pair is generated by a TSP and imported into the QSCD used for signature/seal creation, the environmental assumptions and security objectives for the certified device (QSCD used for key generation and QSCD used for signature/seal creation) shall be met by the TSP.

Not applicable

cc) **(319 411-2/SDP-6.5.1-06)** [QCP-n-qscd] and [QCP-l-qscd] [CONDITIONAL]: If the subject's private key is moved between devices potential vulnerabilities to key compromise shall be determined and adequate mechanisms implemented to mitigate any vulnerabilities.

Not applicable. Private keys are never moved.

dd) **(319 411-2/SDP-6.5.1-07A)** [QCP-n-qscd] and [QCP-l-qscd]: The TSP shall take appropriate measures in case of modification of the QSCD status occurring before the end of the validity period of the certificate.

BankID BankAxept AS has processes in place monitoring the certification status of QSCDs used. All Subject/Signers Certificates issued with keys generated and used within QSCD are non-revocable Short-term Certificates and the Private Keys are destroyed immediately after use, see [23] chapters 3 and 4.

In case of change of the units QSCD status, the unit will be taken out of operation and replaced with a new unit fulfilling the required security classification for a QSCD.

ee) **(319 411-2/SDP-6.5.1-07B)** [QCP-n-qscd] and [QCP-l-qscd]: The TSP shall document in its CPS the measures it takes in case of modification of the QSCD status occurring before the end of the validity period of the certificate.

See letter dd) above

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Please refer to [22] chapter 4.5 and 4.5.1 sub-heading “Certificate Services” for a description of Private Key Protection and Cryptographic Module Engineering Controls

6.3 Other aspects of key pair management

a) **(319 411-1/OVR-6.5.3-01)**: The TSP shall use appropriately the CA private signing keys.

CA private keys are used only for Certificate generation and issuing of CRLs.

b) **(319 411-1/OVR-6.5.3-02)**: The TSP shall not use the CA private signing keys beyond the end of their life cycle.

CA private signing keys are not used beyond their lifespan and are destroyed.

c) **(319 411-1/GEN-6.5.3-03)**: CA signing key(s) used for generating certificates as defined in clause 6.3.3, and/or issuing revocation status information, shall not be used for any other purpose.

See letter a) above. CA signing keys are not used for anything else other than Certificate generation and issuing of CRLs

d) **(319 411-1/GEN-6.5.3-04)**: The certificate signing keys shall only be used within physically secure premises.

Certificate signing keys are generated on HSMs, are non-exportable and only used inside HSMs residing in High security zones.

e) **(319 411-1/GEN-6.5.3-05)**: The use of the CA's private key shall be compatible with the hash algorithm, the signature algorithm and signature key length used for generating certificates, in line with current practice as in requirement GEN-6.5.1-07.

See chapter 6.1 letter g)

f) **(319 411-1/GEN-6.5.3-06)**: All copies of the CA private signing keys shall be destroyed at the end of their life cycle.

See letter b) above

g) **(319 411-1/GEN-6.5.3-07)** [CONDITIONAL]: If a self-signed certificate is issued by the CA, the attributes of the certificate shall be compliant with the defined key usage as defined in ISO/IEC 9594-8/ Recommendation ITU-T X.509 [6] and aligned with GEN-6.5.3-05.

BankID BankAxept AS Root CA issue a self-signed Certificate with key usage attributes compliant with the recommendations set forth in ITU-T X.509.

6.4 Activation data

a) **(319 411-1/GEN-6.5.4-01)**: The installation and recovery of the CA's key pairs in a secure cryptographic device shall require simultaneous control of at least two trusted employees.

See chapter 6.1 letter e) and [22] chapter 4.5.1 letter f**Error! Reference source not found.**

b) **(319 411-1/SDP-6.5.4-02)** [CONDITIONAL]: If the TSP issues a secure cryptographic device, secure cryptographic device (e.g. smartcard) deactivation and reactivation shall be done securely.

Not applicable

c) **(319 411-1/SDP-6.5.4-03)** [CONDITIONAL]: If the TSP issues a secure cryptographic device, and where the personalized secure cryptographic device (e.g. smartcard) has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure cryptographic device.

Not applicable

6.5 Computer security controls

a) **(319 411-1/OVR-6.5.5-01)**: The requirements REQ-7.4-01, REQ-7.4-02, REQ-7.4-03 and REQ-7.4-10 in ETSI EN 319 401 [8] shall apply.

See [22] chapter 4.4 letters a), b), c) and h)

b) **(319 411-1/GEN-6.5.5-02)**: Local network components (e.g. routers) shall be kept in a physically and logically secure environment.

See [22] chapter 4.8

c) **(319 411-1/GEN-6.5.5-03)**: Local network components (e.g. routers) configurations shall be periodically checked for compliance with the requirements specified by the TSP.

See [22] chapter 4.8 letter f)

d) **(319 411-1/GEN-6.5.5-04)**: The TSP shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

All accounts capable of directly causing certificate issuance are enforced with multi-factor authentication using smart card and PIN.

e) **(319 411-1/DIS-6.5.5-05)**: Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.

BankID BankAxept AS CAs have in place access control mechanisms ensuring that all certificates and associated information are protected when added, deleted or modified.

f) **(319 411-1/CSS-6.5.5-06)**: Revocation status application shall enforce access control on attempts to modify revocation status information.

See letter e) above

g) **(319 411-1/OVR-6.5.5-07)**: Continuous monitoring and alarm facilities shall be provided to enable the TSP to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.

See [22] chapter 4.9 letters a) and c)

6.6 Life cycle security controls

a) **(319 411-1/OVR-6.5.6-01)**: The requirements identified in ETSI EN 319 401 [8], clause 7.7 shall apply for all service components.

See [22] chapter 4.7

b) **(319 411-1/OVR-6.5.6-02)** [NCP]: Capacity demands shall be monitored and projections of future capacity requirements shall be made to ensure that adequate processing power and storage are available

BankID BankAccept AS has processes and routines in place for monitoring capacity demands and project future capacity requirements to ensure adequate processing power and storage are available

6.7 Network security controls

a) **(319 411-1/OVR-6.5.7-01)**: The requirements identified in ETSI EN 319 401 [8], clause 7.8 shall apply.

See [22] chapter 4.8

b) **(319 411-1/OVR-6.5.7-02)**: The TSP shall maintain and protect all CA systems in at least a secure zone and shall implement and configure a security procedure that protects systems and communications between systems inside secure zones and high security zones.

BankID BankAxept AS CA systems are located in security zones as described in [22] chapter 4.6.1. Communications between security zones are secured as described in [22] chapter 4.8 letter k)

c) **(319 411-1/OVR-6.5.7-03)**: The TSP shall configure all CA systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's operations.

All CA systems are configured taking into account all of the listed aspects as well as other security relevant elements.

d) **(319 411-1/OVR-6.5.7-04)**: The TSP shall grant access to secure zones and high security zones to only trusted roles.

See [22] chapter 4.6 letter b)

e) **(319 411-1/OVR-6.5.7-05)**: The Root CA system shall be in a high security zone.

BankID BankAxept AS Root CA is off-line in a dedicated High security zone.

6.8 Time-stamping

NOTE: Not in the scope of the present document.

7 Certificate, CRL, and OCSP profiles

Reminder: The Certificates issued by BankID BankAxept AS are issued under one of two certificate profiles, depending only on the level of assurance of the Subject registration as provided by the Notified Identity Provider.

When the Subject is registered at level of assurance high, the Certificate issued is [QCP-n-qscd].

When the Subject is registered at level of assurance substantial, the Certificate issued is [NCP+].

7.1 Certificate profile

a) **(319 411-1/GEN-6.6.1-01)**: The certificates shall meet the requirements specified in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

Both certificate profiles meet their respective requirements in IETF RFC 5280 [7].

b) **(319 411-1/GEN-6.6.1-02)**: The certificate shall be issued according to the relevant certificate profile [CHOICE]:
[LCP, NCP and NCP+] for issuance of certificates to natural persons (excluding for web site certificates): ETSI EN 319 412-2 [9].
[LCP, NCP and NCP+] for issuance of certificates to legal persons (excluding for web site certificates): ETSI EN 319 412-3 [10].
[OVCP], [IVCP], [DVCP], [EVCP], and [LCP], [NCP] and [NCP+] for issuance of certificates for web sites or devices: ETSI EN 319 412-4 [2].

When the Subject is registered at level of assurance substantial, the Certificate issued is [NCP+].
When the Subject is registered at level of assurance high, the Certificate issued is [QCP-n-qscd]. The corresponding standard OID is included in the Certificate.

c) **(319 411-1/GEN-6.6.1-03)**: A TSP issuing short-term certificate should use the validity assured extension ext-etsi-valassured-ST-certs defined in ETSI EN 319 412-1 [13] within the short-term certificates which cannot be revoked.

Both certificate profiles are issues as Short-term non-revocable Certificates and use the validity assured extension *ext-etsi-valassured-ST-certs*.

d) **(319 411-1/GEN-6.6.1-04)**: The TSP issuing short-term certificates shall not use the validity assured extension ext-etsi-valassured-ST-certs defined in ETSI EN 319 412-1 [13] in short-term certificates which can be revoked.

BankID BankAxept AS e-Sign CA does not issue revocable Short-term Certificates.

e) **(319 411-1/GEN-6.6.1-05)**: The TSP shall not use the validity assured extension ext-etsi-valassured-ST-certs defined in ETSI EN 319 412-1 [13] in certificates which are not short-term certificates.

BankID BankAxept AS CAs does not use the validity assured extension ext-etsi-valassured-ST-certs for Certificates that are not short-term Certificates.

f) **(319 411-2/GEN-6.6.1-02)**: The certificate shall include all appropriate qcStatements as defined in ETSI EN 319 412-5 [17].

Only for profile [QCP-n-qscd]: The appropriate qcStatements are included in Qualified Certificates issued under profile.

g) **(319 411-2/GEN-6.6.1-03)** [QCP-n-qscd] and [QCP-l-qscd]: The certificate shall include the qcStatement for QSCD (esi4-qcStatement-4) defined in ETSI EN 319 412-5 [17].

Only for profile [QCP-n-qscd]: The qcStatement QCP-n-qscd is included in the Qualified Certificate issued to natural persons.

h) **(319 411-2/GEN-6.6.1-04)**: The qcStatement for QSCD (esi4-qcStatement-4) shall not be included in certificates that are not issued according to [QCP-n-qscd] or [QCP-l-qscd] requirements.

The qcStatement for QSCD shall not be included in certificates not issued according to [QCP-n-qscd] or [QCP-l-qscd] requirements.

This qcStatement is not included in Certificates issued as [NCP+].

i) **(319 411-2/GEN-6.6.1-05)**: The certificate shall include at least one of the following policy identifier [CHOICE]:

[QCP-n]:
- the policy identifier defined in clause 5.3 item a); and/or
- an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QCP-l]:
- the policy identifier defined in clause 5.3 item b); and/or
- an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QCP-n-qscd]:
- the policy identifier defined in clause 5.3 item c); and/or

- an OID, allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QCP-l-qscd]:
- the policy identifier defined in clause 5.3 item d); and/or
- an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QEVCP-w]:
- an OID as specified in EVCG [4], clause 9.3.2; and at least one of the following policy identifiers:
 as defined in clause 5.3 item e); and/or
 an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QNCP-w]:
- an OID as specified in BRG [5], clause 1.2 or 7.1.6.1; and at least one of the following policy identifiers:
 as defined in clause 5.3 item f); and/or
 an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

• [QNCP-w-gen]:
- the policy identifier defined in clause 5.3 item g); and/or
- an OID allocated by the TSP (or any relevant stakeholder) to the certificate policy applied to issue the certificate.

When the Subject is registered at level of assurance high, the Certificate issued is [QCP-n-qscd]. The corresponding standard OID is included in the Certificate.

7.2 CRL profile

a) **(319 411-1/OVR-6.6.2-01)**: The CRL shall be as defined in ISO/IEC 9594-8/Recommendation ITU-T X.509 [6] or IETF RFC 5280 [7].

CRLs issued by BankID BankAxept AS CAs meets the requirements defined in IETF RFC 5280 [7]

7.3 OCSP profile

a) **(319 411-1/OVR-6.6.3-01)**: The OCSP shall be as defined in IETF RFC 6960 [11].

OCSP responses meet the requirements defined in IETF RFC 6960.

b) **(319 411-1/OVR-6.6.3-02)**: If the OCSP responder receives a request for status of a certificate that has not been issued then the responder shall not respond with a "good" status as per clause 2.2 of IETF RFC 6960 [11].

BankID BankAxept AS OCSP is not publicly available.

In the highly unlikely case that the BankID BankAxept AS e-Signing service requests status for a certificate that has never existed, the OCSP responder will not respond “good”.

c) **(319 411-1/OVR-6.6.3-03)**: The CA should monitor such requests concerning non-issued certificates on the responder as part of its security response procedures to check if this is an indication of an attack.

Unexpected OSCP requests are monitored and checked. See also letter b) above.

8 Compliance audit and other assessments

Please refer to [22], chapter 4.13 for a description on compliance audit.

9 Other business and legal matters

9.1 Fees

No stipulation.

9.2 Financial responsibility

a) **(319 411-1/OVR-6.8.2-01)**: The requirement REQ-7.1.1-04 identified in ETSI EN 319 401 [8], shall apply.

See [22] chapter 4.1.1 letter d)

9.3 Confidentiality of business information

No stipulation.

9.4 Privacy of personal information

a) **(319 411-1/OVR-6.8.4-01)**: The requirement REQ 7.13-05 identified in ETSI EN 319 401 [8], shall apply.

See [22] chapter 4.13 letter e)

b) **(319 411-1/OVR-6.8.4-02)**: The confidentiality and integrity of registration data shall be protected, especially when exchanged with the subscriber/subject or between distributed TSP's system components.

The confidentiality and integrity of registration data is protected using encryption mechanisms.

c) **(319 411-1/OVR-6.8.4-03)**: Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clauses 6.4.5 and 6.4.6).

BankID BankAxept AS has processes and mechanisms in place to securely retaining records fulfilling obligations for protecting both personal and business information in accordance with relevant Norwegian laws.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

a) **(319 411-1/OVR-6.8.6-02)**: The TSP shall provide all its certification services consistent with its CPS.

See [22] chapter 4.13

b) **(319 411-2/OVR-6.8.6-03)**: [QCP-n-qscd] and [QCP-l-qscd]: All obligations specified for NCP+ in ETSI EN 319 411-1 [2] shall apply.

All obligations specified for [NCP+] are applicable to the [QCP-n-qscd] profile as described in this document.

9.7 Disclaimers of warranties

See clause 6.8.6.

See also clause A.2 in ETSI EN 319 411-1 [15] for additional information.

9.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.9.4.

NOTE: See article 13 of the Regulation (EU) No 910/2014 [i.14].

9.9 Indemnities

No stipulation.

9.10 Term and termination

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute resolution provisions

a) **(319 411-1/OVR-6.8.13-01)**: The item h) of requirement REQ-6.2-02 identified in ETSI EN 319 401 [8], and the requirement REQ-7.1.1-06 identified in ETSI EN 319 401 [8], shall apply.
NOTE: See clause A.2 for additional information.

See [22] chapter 3.2 letter b), and chapter 4.1.1 letter f).

The PDS will contain information for customers on how to contact BankID BankAxept AS in case of disputes, and how disputes are settled.

9.14 Governing law

No stipulation

9.15 Compliance with applicable law

a) **(319 411-1/OVR-6.8.15-01)**: The requirements REQ-7.13-01 and REQ-7.13-02 identified in ETSI EN 319 401 [8], shall apply.

See [22] chapter 4.13 letters a) and b)

9.16 Miscellaneous provisions

No Stipulation

9.17 Other provisions

9.17.1 Risk management

9.17.2 Organizational

Please refer to [22] chapter 4.1 and 4.1.3, sub-heading “Certificate Services” for a detailed description of practices related to organizational requirements.

9.17.3 Additional testing

a) **(319 411-1/OVR-6.9.2-01)**: The TSP shall provide the capability to allow third parties to check and test all the certificate types that the TSP issues.

BankID BankAxept AS provides a test environment that allows third parties to check and test all certificate types.

c) **(319 411-1/OVR-6.9.2-02A):** Any certificates issued for test purposes should clearly indicate that they are for testing purposes (e.g by the subject name).

Certificate issued for test purposes are issued by a dedicated test PKI that is clearly marked as a testing environment.

9.17.4 Disabilities

a) **(319 411-1/OVR-6.9.3-01)**: The requirements REQ-7.13-03 and REQ-7.13-04 identified in ETSI EN 319 401 [8], shall apply.

See [22] chapter 4.13 letters c) and d)

9.18 Terms and conditions

a) **(319 411-1/OVR-6.9.4-01)**: The requirements identified in ETSI EN 319 401 [8], clause 6.2 shall apply.

See [22] chapter 3.2

b) **(319 411-1/OVR-6.9.4-02)**: The terms and conditions shall include at minimum the following elements:

a) the indication of what constitutes certificate acceptance, as specified in;
b) the period of time for which the records are retained according to OVR-6.3.4-17;
c) the subscriber's obligations as specified in OVR-6.3.5-01;
d) where applicable, the subject's obligations as specified in OVR-6.3.5-02;
e) the notice to relying parties as specified in OVR-6.3.5-03;
f) the ways in which a specific policy adds to or further constrains the requirements of the CP as defined in the present document, see OVR-7.2-01.

All the above elements regarding use of BankID BankAxept AS Trusted Services including Certificate acceptance are reflected in the terms and conditions and in the PKI Disclosure Statement.

c) **(319 411-2/OVR-6.9.4-02)**: The certificate policy shall include a clear statement indicating that the policy is for EU qualified certificates and whether the policy requires use of a QSCD.

The Certificate policy covering issuance of Certificates to Subjects/Signers by BankID BankAxept AS e-Sign CA requires the use of a QSCD for both EU qualified and non-qualified Certificates.

This is also indicated by use of an ETSI-standardized OID.

d) **(319 411-2/OVR-6.9.4-03)**: A PKI disclosure statement shall be supported.

The PKI Disclosure Statement is available on BankID BankAxept web site.

e) **(319 411-2/OVR-6.9.4-04)**: The PKI disclosure statement should be structured according to annex A in ETSI EN 319 411-1 [15].

The PKI disclosure statement is structured in accordance with ETSI EN 319 411-1, annex A.

10 Framework for the definition of other certificate policies

Not applicable.

The CPs declared in this document is in line with the CPs defined in ETSI 319 411-1 v1.3.1 and ETSI 319 411-2 v2.4.1