Stø AS Trust Services Practice Statement

Version 1.2 Last updated 23. September 2025

Table of contents

Document history.

Version	Date	Changes	Approved by
1.2	24.09.2025	Reflecting name change to Stø	ID Policy Board
1.1.2	03.12.2024	Added one link to 1.5.2	Editorial change only
1.1.1	28.10.2024	Mainly editorials. Updated 4.7.g)	ID Policy Board
1.1	24.09.2024	Incorporating stage 1 audit comments	ID Policy Board
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.

BankID BankAxept AS established Trustworthy Systems (TWS) for providing the following Trust Services:

- Certificate Services;
  PKI infrastructure consisting of BankID BankAxept Root-CA (level 0), issuing Certificates to two subordinate (level 1) CAs:
  - Issuing CA (e-Sign CA) issuing Qualified and non-qualified e-Signature Short-lived Certificates to Subjects/Signers.
  - Timestamping Authority CA (TSA CA) issuing Certificates to Timestamping Units (TSU) providing Qualified Timestamping Services.
- Qualified Timestamping Services:
  Timestamping Authority system providing Qualified Time-Stamping Services
- e-Signature Services:
  Trustworthy Systems providing Qualified and Advanced Remote e-Signature Services

1.1 Overview

The following figure provides a logical architectural overview of BankID BankAxept AS TWS facilitating production and delivery of e-Signature and Timestamping Services.

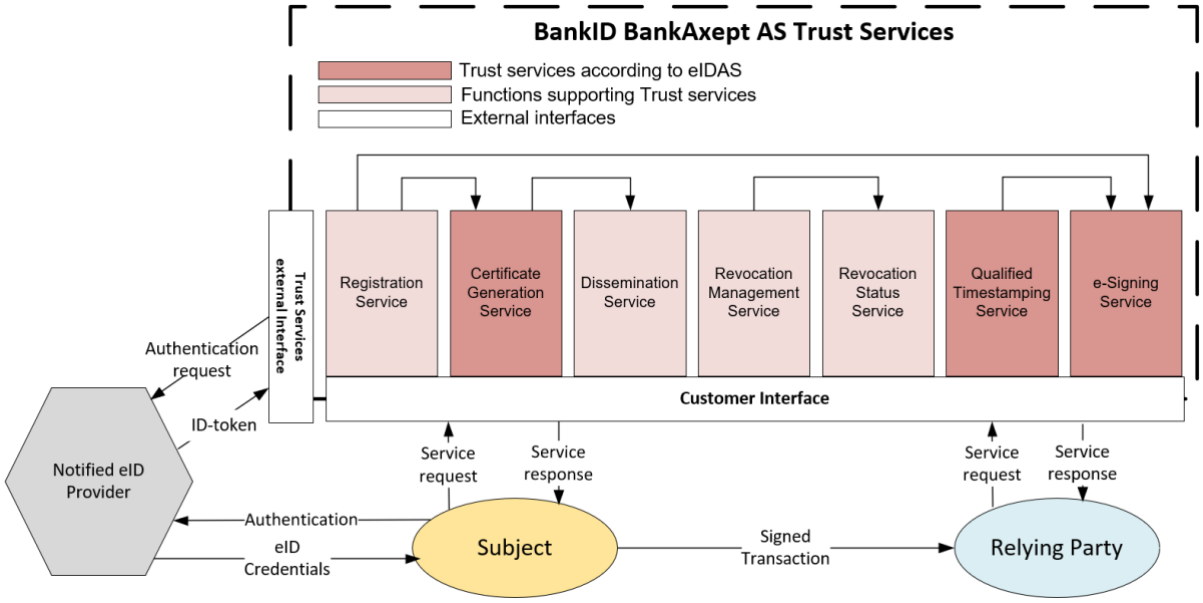

Figure 1: Logical Architecture BankID BankAxept AS Trust Services

BankID BankAxept TWS as shown in Figure 1 consists of:

Registration Service	Verification of the identity and, if applicable, any specific attributes of Subjects/Signers requesting access to BankID BankAxept AS Trust Services
Certificate Generation Service	Creating Certificates for BankID BankAxept AS Trust Services as well as Qualified and non-Qualified Signers Certificates to users of BankID BankAxept AS Remote e-Signature Service, see [10]
Dissemination Service	Providing certificates (Root-CA), policy and TSPS information, terms and conditions to Subjects and Relying parties.
Revocation Management Service	Processing of revocation requests related to Certificates issued by BankID BankAxept AS Root-CA and TSA CA
Revocation Status Service	Providing revocation status information to Relying Parties
Qualified Timestamping Service	Providing Qualified Time-stamping Service, see [11]
e-Signing Service	Server signing application to create a digital signature value on behalf of a Signer/Subject, see [10]
Customer Interface	Interface available to Subjects and Relying Parties for access to BankID BankAxept AS Trust Services
Trust Services external Interface	Interface between BankID BankAxept AS Trust Services and Notified eID Providers

1.2 Scope

The scope for this document is to provide an overall description of BankID BankAxept AS Trust Services, their interaction and dependencies, and the Policy and operational practices applicable to all Services described in this document.

This document also describes operational practices specific to the individual Trust Services where the Service operational practices are directly related to the practices mandated in [3].

1.2.1 TSPS document structure

The following figure provides an overview of the structure of TSPS documents documenting policies and practices applied for BankID BankAxept Trust Services.

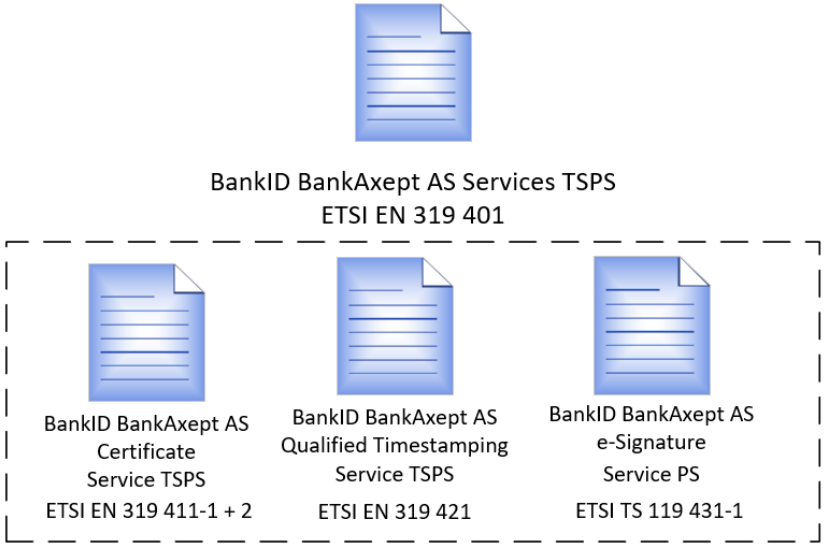

Figure 2: BankID BankAxept AS TSPS document structure

1.3 Document Name and Identification

Document Name: Stø AS Qualified Trust Services Practice Statement. No OID has been allocated for this document.

1.3.1 Conventions

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 [4].

1.4 Participants and responsibilities/obligations

1.4.1 Trust Service Provider

BankID BankAxept AS is the Trust Service Provider providing the Services described in chapter 1.1.

1.4.2 Registration authorities

BankID BankAxept AS is the Registration authority (RA) 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 [9] chapter 3.2.

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 [10] chapters 3.2 and 3.3.

1.4.3 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 AS TSA CA.

Subjects of Certificates issued by BankID BankAxept AS e-Sign CA are natural persons using BankID BankAxept AS e-Signature Service.

Subjects of Certificates issued by BankID BankAxept AS TSA CA are BankID BankAxept AS TSU providing Qualified Timestamping Service.

1.4.4 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 [10] and BankID BankAxept AS Qualified Timestamping Service [11].

1.4.5 Other participants

This includes auditors, supervisory bodies, Subcontractors and other stakeholders.

1.5 Policy administration

1.5.1 Organization administering the Policies and TSPS documents

BankID BankAxept AS ID Policy Board (IPB) is the organization administering the policies and the TSPS documents for BankID BankAxept AS Services described in this document and the Services described in [9], [10] and [11].

1.5.2 Contact person

Questions related to policies and practices described in this document and the TSPS documents [9], [10] and [11] shall be addressed to:

BankID BankAxept AS ID Policy Board

c/o BankID BankAxept AS (https://bankid.no/en)

P.O. Box 9265 Grønland,

N-0134 Oslo

E-mail: IDpolicyboard@bidbax.no

1.5.3 Person determining TSPS suitability for the policy

All TSPS documents, including this document, are approved by IPB.

1.5.4 TSPS approval procedures

BankID BankAxept AS ID Policy Board has in place formal approval procedures for all changes in TSPS documents.

1.6 Definition of terms, symbols, abbreviations and notation

1.6.1 Terms

Authentication:	Provision of assurance in the claimed identity of an entity as defined in ISO/IEC 18014-2 [i.14].
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 Revocation List	Signed list indicating a set of certificates that are no longer considered valid by the Certificate issuer.
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 and repealing Directive 1999/93/EC [1]
Identity Provider	Entity that makes available identity information
Notified Identity Provider	Identity Provider issuing eIDs under an eID scheme notified under eIDAS [1]
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 [1]
Qualified Signature Creation Device	As specified in eIDAS [1]
Relying Party	Natural or legal person that relies upon an electronic identification or a Trust Service.
Remote signature creation device	Signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf
Signature Creation device (SCDev)	Configured software or hardware used to implement the signature creation data and to create a digital signature value
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 obligation set forth in terms and conditions
Subcontractor	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	Electronic service that enhances trust and confidence in electronic transactions
Trust Service Provider	Natural or a legal person who provides one or more trust services as defined in [1]
Trustworthy System	A system composed of computer hardware, software, network supported by procedures which: 1) are reasonably secure from intrusion and misuse. 2) provide a reasonable level of availability, reliability, and correct operation. 3) are reasonably suited to performing their intended functions; and 4) adhere to generally accepted security procedures. Source: [i.15]

1.6.2 Symbols

No stipulation

1.6.3 Abbreviations

CA	Certificate Authority
CARL	Certificate Authority Revocation List
CSR	Certificate Signing Request
IdP	Identity provider
IPB	ID Policy Board (BankID BankAxept AS ID Policy Board)
ISMS	Information Security Management System
NIdP	Notified Identity Provider
NDPA	Norwegian Data Protection Authority (Datatilsynet), the supervisory body in Norway supervising organizations adherence to Data privacy regulations [2]
NKOM	Norwegian Communications Authority, the supervisory body in Norway supervising Norwegian TSP according to [1]
PAM	Privilege Access Management
QSCD	Qualified Signature/seal Creation Device
SAP	Signature Activation Protocol
SCDev	Signature Creation Device
TSA	Timestamping Authority
TSPS	Trust Service Practice Statement
TSU	Timestamping Unit
TWS	Trustworthy Systems
TW4S	Trustworthy System Supporting Server Signing

1.7 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.

1.7.1 Normative references

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

[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

[2] Lov 15.juni 2018 nr 38 om behandling av personopplysninger (personopplysningsloven)

[3] ETSI EN 319 401 (v2.3.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".

[4] ETSI Drafting Rules (EDRs), accessed 29.02.2024: https://portal.etsi.org/Services/editHelp/How-to-start/ETSI-Drafting-Rules

[5] 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”.

[6] 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”.
[7] ETSI EN 319 421 (v1.1.1): “Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps“
[8] 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”
[9] Stø AS Certificate Service TSPS
[10] Stø AS e-Signature Service PS
[11] Stø AS Qualified Timestamping Services TSPS
[12] ISO/IEC 15408 (parts 1 to 3): "Information security, cybersecurity and privacy protection - Evaluation criteria for IT security".
[13] ISO/IEC 19790:2012: "Information technology - Security techniques - Security requirements for cryptographic modules".
[14] FIPS PUB 140-2 (2002): "Security Requirements for Cryptographic Modules".
[15] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".
[16] CEN EN 419221-5:2018: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).

1.7.2 Informative references

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

[i.1] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
[i.2] 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.3] ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management".
[i.4] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, Version 2.0.1”.
[i.5] ISO/IEC 27005:2011: “Information technology – Security techniques – Information security risk management”.
[i.6] ETSI EN 319 403-1 (v2.3.1): “Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment – Requirements for conformity assessment bodies assessing Trust Service Providers”.
[i.7] CA/Browser Forum: “Network and certificate system security requirements, Version 1.7".
[i.8] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[i.9] ETSI EN 319 411-1 (v1.4.1): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
[i.10] ETSI EN 301 549 (v3.2.1): "Accessibility requirements for ICT products and services".
[i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[i.12] 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".
[i.13] ISO/IEC 27701:2019: "Security techniques - Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management - Requirements and guidelines".
[i.14] ISO/IEC 18014-2: "Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens".
[i.15] NIST SP 800-12 Rev. 1: “An Introduction to Information Security”

[i.16] ETSI TS 119 312 (v1.4.1): "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".

1.8 Notation

Text that is outside text boxes is the applicable policy requirements. Requirements related to [3], [5], [6] and [8] are 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 the type of requirement.
- The clause number reflects the clause number in the referred standard.

Requirements related to [7] are identified with the following syntax:

In brackets: <6 digits>/<2-3 digits>-<clause index>

- The 6 digits reflect the standard stating the requirement.
- The 2-3 digits refer to the specific chapter of the reflected standard.
- The clause index, when present, reflects the letter (a), b), c), …) identifying the specific clause in the referred chapter.

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

2 Risk Assessment

a) **(319 401/REQ-5-01)**: The TSP shall carry out a risk assessment to identify, analyze and evaluate trust service risks taking into account business and technical issues.

BankID BankAxept AS ISMS has defined a risk management policy mandating regular risk assessments. The risk management policy covers all BankID BankAxept AS Services, see [9], [10] and [11], and takes into account both technical and business aspects.

b) **(319 401/REQ-5-02)**: The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results.
The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.

BankID BankAxept AS risk management policy ensures that appropriate risk treatment measures are identified and defined in a risk treatment plan.

c) **(319 401/REQ-5-03)**: The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).

BankID BankAxept AS risk management policy has defined processes ensuring that risk treatment measures are implemented appropriate to the risk identified through risk assessments.

d) **(319 401/REQ-5-04)**: The risk assessment shall be regularly reviewed and revised.

The risk assessment is as minimum reviewed and revised annually. Risk assessments is also performed for projects and changes that may impact TWS security.

e) **(319 401/REQ-5-05)**: The TSP's management shall approve the risk assessment and accept the residual risk identified.

The risk assessment is as minimum reviewed and revised annually. Risk assessments is also performed for projects and changes that may impact TWS security.

3 Policies and practices

3.1 Trust Service Practice statement

a) **(319 401/REQ-6.1-01)**: The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.

This document, BankID BankAxept AS Trust Services Practice Statement, provides:

- An overall description of BankID BankAxept AS Trust Services, their interaction and dependencies as well as mutual management practices and terms and conditions
- A list of policy requirements that are common to all BankID BankAxept AS Trust Services and a high-level practice statement related to these Services
- Practices specific for the individual Trust Service directly related to the common requirements described in this document are described in sub-chapters with headings reflecting the specific Service.

The document structure includes three Trust Service specific documents as shown in Figure 2. These TSPS documents describe the practices related to the individual Trust Service specific requirements.

For practices related to requirements common to all BankID BankAxept AS Trust Services, a link to this document with a reference to the correct chapter is provided in the Service specific TSPS document.

The structure (headings and subheadings) in this TSPS is organized in accordance with recommendations in [3].

b) **(319 401/REQ-6.1-02)**: The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant.

Policies and practices for all BankID BankAxept AS Trust Services are approved by BankID BankAxept AS ID Policy Board. Public policies are published on a web site. In general, policies and practices are shared with employees and relevant external parties and communicated to them.

BankID BankAxept AS refrains from making sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies publicly available in TSPS documents. Such documentation is made available to Auditors and Supervisory Authorities as required.

c) **(319 401/REQ-6.1-03A)**: The TSP shall have a statement of the practices and procedures used to address all the requirements of the applicable trust service policy as identified by the TSP.

This document in combination with the service specific TSPS documents, ref. [9], [10] and [11], addresses all requirements applicable to BankID BankAxept AS Trust Services.

d) **(319 401/REQ-6.1-04)**: The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.

This document in combination with the service specific TSPS documents, ref. [9], [10] and [11], identifies the obligations to be adhered to by all external organizations to which any task have has been outsourced. Such requirements obligations are detailed in the outsourcing contract.

BankID BankAxept AS is the operator of the service. Basic operations and network operations of the computer infrastructure for the service are carried out by DXC Technologies as a subcontractor.

Servers and data are physically located at an Uptime Tier III certified Data Center. Data Center employees do only perform physical and technical installation and maintenance of the components.

e) **(319 401/REQ-6.1-05A):** The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to demonstrate conformance to the trust service policy.

BankID BankAxept AS TSPS and other relevant documentation necessary to demonstrate conformance to the requirements for the Qualified Services offered, is available to Subjects and Relying Parties on the BankID BankAxept AS web site 24/7.

f) **(319 401/REQ-6.1-06)**: The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.

BankID BankAxept AS ID Policy Board is responsible for the policies TSPSs covering BankID BankAxept AS Qualified Services, Practice Statements, and their maintenance.

g) **(319 401/REQ-6.1-07)**: The TSP's management shall implement the practices.

BankID BankAxept AS' management implements the practices described in this document and in the service specific TSPS documents, see [9], [10] and [11].

h) **(319 401/REQ-6.1-08):** The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.

BankID BankAxept AS has in place a defined review process for the practices including responsibilities for maintaining the TSP's practice statements.

All substantial changes to practice statements shall be approved by a policy board, appointed by top management. The policy board will convene when changes are required, or at least annually.

i) **(319 401/REQ-6.1-09A)** [CONDITIONAL]: When the TSP intends to make changes in its practice statement that might affect the acceptance of the service by the subject, subscriber or relying parties, it shall give due notice of changes to subscribers and relying parties.

BankID BankAxept AS ID Policy Board may amend Policy or the Trust Practice Statement for any of the Services offered, at its own discretion.

Any such changes potentially affecting Trust Service acceptance by Subjects/Signers, Relying Parties or Subscribers, are notified at least 14 days before the change become effective.

j) **(319 401/REQ-6.1-10)**: The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above.

Revised TSPS documents covering any of BankID BankAxept AS Trust Services are made immediately available on BankID BankAxept AS' web site following approval from BankID BankAxept AS ID Policy Board.

k) **(319 401/REQ-6.1-11)**: The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).

See chapter 4.12

3.2 Terms and Conditions

a) **(319 401/REQ-6.2-01)**: TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.

Terms and conditions for BankID BankAxept AS e-Signing Services are available to all Subjects/Signers and Relying Parties at BankID BankAxept AS web site, ref. chapter 3.1, letter e).

Terms and conditions for BankID BankAxept AS Qualified Timestamping Service is available to Subscribers as part of the Service contract.

b) **(319 401/REQ-6.2-02)**: The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:
   a) the trust service policy being applied.
   b) any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations.
   c) the subscriber's obligations, if any;
   d) information for parties relying on the trust service;
   e) the period of time during which TSP's event logs are retained;
   f) limitations of liability;
   g) the applicable legal system;
   h) procedures for complaints and dispute settlement;
   i) whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;
   j) the TSP's contact information; and
   k) any undertaking regarding availability.

All relevant terms and conditions are made available to Subjects/Signers as part of the enrolment process described in [10] chapter 3.2 and at BankID BankAxept AS web site as described in chapter 3.1 letter e).

c) **(319 401/REQ-6.2-03)**: Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.

The terms and conditions associated with the e-Signature Service is made available to the Subject electronically as part of the enrolment process described in [10] chapter 3.2 and the Subject must accept these in order to make use of the signature service. If the Subject has authorized a third party to submit the document to-be-signed to BankID BankAxept AS e-Signature Service [10], the Subject has accepted the terms and condition at time of authorizing the third party.

The terms and conditions are made available to Relying Parties on BankID BankAxept AS web site. as described in chapter 3.1 letter e).

For Subscribers contracting with BankID BankAxept AS for the use of BankID BankAxept AS Qualified Timestamping Service, the terms and conditions are stated in the contract.

d) **(319 401/REQ-6.2-04)**: Terms and conditions shall be made available through a durable means of communication.

Terms and conditions are made available at the BankID BankAxept AS web site as described in chapter 3.1 letter e).

e) **(319 401/REQ-6.2-05)**: Terms and conditions shall be made available in readelliy understandable language.

BankID BankAxept AS will produce Terms & Conditions in Norwegian and English. Experts on public communication will be consulted.

f) **(319 401/REQ-6.2-06):** Terms and conditions shall be made available through a durable means of communication.

See letter c) above.

3.3 Information security policy

a) **(319 401/REQ-6.3-01)**: The TSP shall define an information security policy which is approved by management, and which sets out the organization's approach to managing its information security.

BankID BankAxept AS management has established and approved an information security policy covering all BankID BankAxept AS services including BankID BankAxept AS Trust Services.

The information security policy states BankID BankAxept AS security goals and BankID BankAxept AS management commitment to security and quality in accordance with business requirements and relevant laws and regulations.

b) **(319 401/REQ-6.3-02)**: Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies.

BankID BankAxept AS information security policy and any changes to the information security policy is communicated to relevant external parties where applicable.

c) **(319 401/REQ-6.3-03)**: A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

BankID BankAxept AS information security policy is documented and maintained by BankID BankAxept AS management. The information security policy is the governing document for BankID BankAxept AS Information Security Management System (ISMS). The ISMS defines the security controls and operating procedures for BankID BankAxept AS Trust Services mandated by the information security policy. The ISMS and the information security policy are supported by a number of standards for acceptable use of information assets and secure operations. All these documents are maintained annually.

BankID BankAxept AS ISMS is designed in line with ISO/IEC 27001:2022.

d) **(319 401/REQ-6.3-04)**: The TSP shall publish and communicate the information security policy to all employees who are impacted by it.

BankID BankAxept AS information security policy is communicated to all employees. This includes both BankID BankAxept AS employees and consultants, as well as Subcontractors' employees.

e) **(319 401/REQ-6.3-05)**: The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers.

BankID BankAxept AS is overall responsible for the services set out in this TSPS and information security policies and will oversee that the underlaying procedures are sufficient, even if these are carried out by third party. This means the TSP will ensure adequate and appropriate security controls and operating procedures for TSP facilities, systems and information assets providing the services.

f) **(319 401/REQ-6.3-06)**: TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP.

Subcontractors to whom any parts of BankID BankAxept AS Trust Services are outsourced must comply with terms regulated in a legal agreement between BankID BankAxept AS and the subcontractor. Contracts outline scope and guarantees for the outsourced service, in addition to defining liability. There is also an annex to any standard agreement which fully specifies security controls which the subcontractor is bound to implement.

g) **(319 401/REQ-6.3-07)**: The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

BankID BankAxept AS information security policy and inventory of assets are reviewed annually and when significant changes occur.

h) **(319 401/REQ-6.3-08)**: Any changes that will impact on the level of security provided shall be approved by the management body referred to in REQ-6.1-07.

Changes impacting the level of security identified through the risk assessment process is communicated and approved by BankID BankAxept AS ID Policy Board.

i) **(319 401/REQ-6.3-09)**: The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.

The configurations of BankID BankAxept AS TWS are audited and controlled regularly and changed if required by the security policy, defined in an approved risk treatment plan and when deviations from defined security baseline is detected.

The following scans and audits are performed regularly:

- Configuration baseline scanning - Monthly
- Vulnerability scanning - Quarterly
- Penetration testing - Annually
- Firewall audits – Annually

j) **(319 01/REQ-6.3-10)**: The maximum interval between two checks shall be documented in the trust service practice statement.

The configuration is checked at least annually.

4 TSP management and operation

4.1 Internal organization

4.1.1 Organization reliability

a) **(319 401/REQ-7.1.1-01)**: The TSP organization shall be reliable.

BankID BankAxept AS is a reliable organization, duly registered with The Brønnøysund Register Center in The Register of Business Enterprises operating in accordance with Norwegian law.

b) **(319 401/REQ-7.1.1-02)**: Trust service practices under which the TSP operates shall be non-discriminatory.

BankID BankAxept AS Trust Services are available to any Subscriber, Subject/Signer and Relying Party adhering to the terms and conditions for the Services.

c) **(319 401/REQ-7.1.1-03)**: The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.

See letter b) above.

d) **(319 401/REQ-7.1.1-04)**: The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.

BankID BankAxept AS has in place a combination of funds and insurance arrangements covering potential damage reflected in the applicable Subject/Signer terms and conditions.

Funds will be set aside to cover the cost of a termination, indcluding continued storage of mandatory data.

e) **(319 401/REQ-7.1.1-05)**: The TSP shall have the financial stability and resources required to operate in conformity with this policy.

BankID BankAxept AS is a financially sound company, registered with The Brønnøysund Register Center in The Register of Business Enterprises with the processes, economic, technical and human resources required for operating in conformity with the policy and practice requirements applicable to BankID BankAxept AS Trust Services.

f) **(319 401/REQ-7.1.1-06)**: The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.

BankID BankAxept AS have in place dispute resolution processes and procedures in line with applicable Norwegian law as stipulated in terms and conditions.

Any dispute that is not resolved by alternative dispute resolution shall be brought to a Norwegian court for settlement. Oslo District Court shall be the exclusive first instance venue for all such disputes.

g) **(319 401/REQ-7.1.1-07)**: The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third-party arrangements.

BankID BankAxept AS have in place contracts with third parties to whom any parts of the Trust Services operations are outsourced.

h) **(319 401REQ-7.1.1-08)** [CONDITIONAL]: When the TSP makes use of other parties, including trust service component providers, to provide parts of its service through subcontracting, outsourcing or other third-party arrangements, it shall maintain overall responsibility for meeting the requirements defined in the trust service policy.

BankID BankAxept AS maintains overall responsibility for meeting the requirements applicable to the Trust Services offered, also for any parts of the Services outsourced to a third-party.

i) **(319 401/REQ-7.1.1-09)** [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the use of the component interface meets the requirements as specified by the trust service component provider.

Not applicable

j) **(319 401/REQ-7.1.1-10)** [CONDITIONAL]: When the TSP makes use of a trust service component provided by another party it shall ensure that the security and functionality required by the trust service component are meeting the appropriate requirements of the applicable policy and practices.

Not applicable.

4.1.2 Segregation of duties

a) **(319 401/REQ-7.1.2-01)**: Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of TSP's assets.

There is a defined role matrix for the TSP documenting the separation of functions and roles to be performed in the operation of the TSP. Role descriptions are documented and defines the tasks and responsibility of the role.

4.1.3 Trust services specific controls

Certificate services

a) **(319 411-1/OVR-6.9.1-02)**: The parts of the TSP concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies.

The parts of BankID BankAxept AS organization responsible for certificate generation and revocation management are organized independently of the BankID BankAxept AS organization structure to ensure that important decisions regarding certificate issuance and revocation are made

without influence from other parts of BankID BankAxept AS and other organizations, and according to certificate profiles [QCP-n-qscd] and [NCP+] as applicable.

b) **(319 411-1/OVR-6.9.1-03)**: The senior executive, senior staff and staff in trusted roles, of the TSP concerned with certificate generation and revocation management shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

See letter a) above

c) **(319 411-1/OVR-6.9.1-04)**: The parts of the TSP concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.

Safeguarding impartiality of operations is central for the organization as described in letter a) above. This organization structure is documented and communicated to all persons involved in the operations.

Timestamping services

d) **(319 421/7.2-a))**: The TSA shall be a legal entity according to national law.

See chapter 4.1.1 letter a)

e) **(319 421/7.2-b))**: The TSA shall have a system or systems for quality and information security management appropriate for the time-stamping services it is providing.

See chapter 3.3 letter a)

f) **(319 421/7.2-c))**: It shall employ a sufficient number of personnel having the necessary education, training, technical knowledge and experience relating to the type, range and volume of work necessary to provide time-stamping services.

BankID BankAxept AS has processes in place to ensure that there will be a sufficient number of trained personnel available for service delivery.

For personnel requirements regarding necessary education, training, technical knowledge and experience, see chapter 4.2

4.2 Human resources

a) **(319 401/REQ-7.2-01)**: The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations.

In order to ensure trustworthy operation of BankID BankAxept AS TWS, information security responsibilities for employees, contractors and subcontractors' personnel, BankID BankAxept AS have in place defined security processes and instructions providing detailed guidance on the operation of BankID BankAxept AS TWS. A background check will be performed of every person who shall be onboarded to a trusted role.

Responsibilities for the protection of BankID BankAxept AS TWS, components and information are defined and detailed guidance for specific sites and processing facilities are identified, reflecting the systems criticality and classification.

b) **(319 401/REQ-7.2-02)**: The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.

BankID BankAxept AS has HR processes and routines in place ensuring that no personnel are granted access to TWS until they have undergone thorough training and demonstrated a sufficient level of proficiency. All personnel must, before access to the TWS is granted, have demonstrated their reliability, knowledge and skills.

c) **(319 401/REQ-7.2-03)**: TSP's personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.

Personnel working with BankID BankAxept AS TWS are individuals fulfilling the requirement of expert knowledge, experience and qualifications expertise. Verification of the individual's claimed certification and experience is done as part of the hiring process and before assuming a trusted role. All BankID BankAxept AS personnel are given proper training before they can access the TWS.

d) **(319 401/REQ-7.2-04)**: This should include regular (at least every 12 months) updates on new threats and current security practices.

BankID BankAxept AS personnel working with TWS are regularly updated on threats and security practice relevant to their individual job function at least every 12 months. Personnel in trusted roles are obliged to perform an annual security interview.

e) **(319 401/REQ-7.2-05)**: Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.

All personnel having access to BankID BankAxept AS TWS are responsible for their actions and are made aware of consequences and disciplinary actions as a reaction to violations of BankID BankAxept AS policies and practices, either negligently or intentionally. This is described in employment contracts and appointment forms.

f) **(319 401/REQ-7.2-06)**: Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.

BankID BankAxept AS information security policy describing security roles and responsibilities are available electronically for all personnel, both BankID BankAxept AS employees and any third-party and Subcontractor personnel involved in any part of the Services.

g) **(319 401REQ-7.2-07)**: Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.

BankID BankAxept AS has identified and defined a set of trusted roles and written instructions for people assuming these trusted roles.

h) **(319 401/REQ-7.2-10)**: TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.

Personnel having access to BankID BankAxept AS TWS (both permanent and temporary) have job descriptions reflecting the principle of segregation of duties and least privilege.

BankID BankAxept AS have established HR routines ensuring background screening as well as training and awareness for personnel assigned to trusted roles.

i) **(319 401/REQ-7.2-11)**: Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.

BankID BankAxept AS job descriptions are reflecting the information security expectations, the terms and conditions and the required skills and qualifications relevant for the different roles.

j) **(319 401/REQ-7.2-12)**: Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.

BankID BankAxept AS personnel must adhere to administrative procedures and processes defined in the Information Security Management System (ISMS).

k) **(319 401/REQ-7.2-13)**: Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

BankID BankAxept AS managerial personnel have training and experience with respect to the trust services provided. They are familiar with security procedures for personnel with security responsibilities and have experience with information security and risk assessment sufficient to carry out their management functions.

l) **(319 401/REQ-7.2-14)**: All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.

BankID BankAxept AS have processes in place evaluating potential conflict of interests prior to appointing a person to a trusted role.

m) **(319 401/REQ-7.2-15)**: Trusted roles shall include roles that involve the following responsibilities:
   a. Security Officers: Overall responsibility for administering the implementation of the security practices.
   b. System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.
   c. System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup.
   d. System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.

Trusted roles defined for BankID BankAxept AS TWS operations:

a. **Security Officer:** Overall responsible for administering the implementation of security policy and practices which falls within the specific services delivered and authorizes security critical operations.
b. **System Administrator:** Authorized to install, configure and maintain the TWS used in BankID BankAxept AS Services. There are defined specific System Administrator roles within each technology.

System Supervisors: Authorized to supervise installation, configuration and maintenace of the TWS used in BankID BAnkAxept AS services. There are defined specific System Supervisor roles within each technology.

c. **System Administrators Backup:** Responsible for operating BankID BankAxept AS TWS and perform backup and recovery. Covering the System Operator role according to requirement.
d. **System Auditor:** Authorized to view archives and audit logs of BankID BankAxept AS TWS

To perform administration of the BankID BankAxept AS TWS there is enforced dual control through Privileged Access Management (PAM). Both System Administrator and System Supervisor are needed to perform any tasks in the production environment.

n) **(319 401/REQ-7.2-16A)**: TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security.

Personnel in trusted roles are appointed by BankID BankAxept AS management.

o) **(319 401/REQ-7.2-16B)**: Trusted roles shall be accepted by the appointed person to fulfil the role.

Personnel appointed to trusted roles must accept their role by accepting their job description and signing the appointment letter.

p) **(319 401/REQ-7.2-17)**: Personnel shall not have access to the trusted functions until the necessary checks are completed.

BankID BankAxept AS has established HR routines ensuring background screening of personnel in-line with Norwegian law.
Personnel who shall be appointed to trusted roles must complete their training before accesses are given.

4.3 Asset management

4.3.1 General requirements

a) **(319 401/REQ-7.3.1-01)**: The TSP shall ensure an appropriate level of protection of its assets including information assets.

BankID BankAxept AS maintains an inventory and location of all assets, including information assets, associated with BankID BankAxept AS Qualified Services in order to ensure proper level of protection. All assets are classified based on risk exposure and criticality. For each classification level it is defined a protection level ensuring an appropriate level of protection for the life-cycle of the asset.

b) **(319 401/REQ-7.3.1-02)**: The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.

See letter a) above.

4.3.2 Media handling

a) **(319 401/REQ-7.3.2-01)**: All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.

BankID BankAxept AS has media management procedures in place mandating secure handling of media in line with the classification of information contained in the media.

All media containing sensitive information is securely decommissioned and destroyed as part of disposal procedures.

b) **(319 401/REQ-7.3.2-02)**: Media used within the TSP's systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.

BankID BankAxept AS media management procedures mandates secure handling and protection of media from damage, theft, unauthorized access and obsolescence.

Media are stored in the same security zones as BankID BankAxept AS TWS and have the same level of physical and logical access as the Trustworthy system itself.

c) **(319 401/REQ-7.3.2-03)**: Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

BankID BankAxept AS media management procedures mandates processes and routines facilitating protection against obsolescence and deterioration of media taking into account the period of time information stored are required to be retained.

4.4 Access control

a) **(319 401/REQ-7.4-01)**: The TSP's system access shall be limited to authorized individuals.

BankID BankAxept AS have in place an access control policy covering both physical and logical access, ensuring that access to BankID BankAxept AS TWS are limited to authenticated and authorized individuals.

b) **(319 401/REQ-7.4-04A)**: The TSP shall administer user access of operators, administrators and system auditors applying the principle of "least privileges" when configuring access privileges.

BankID BankAxept AS access control policy ensures that access rights for personnel appointed to a trusted role are based upon the principle of segregation of duties and least privilege.

c) **(319 401/REQ-7.4-05)**: The administration shall include user account management and timely modification or removal of access.

User access privileges are regularly reviewed. When personnel change positions and functions internally their access rights are modified and when personnel leave BankID BankAxept AS their access rights are removed.

d) **(319 401/REQ-7.4-06)**: Access to information and application system functions shall be restricted in accordance with the access control policy.

Only personnel that has been granted access according to BankID BankAxept AS access policy, will be granted access to information and specific applications.

Access rights are reviewed twice a year.

e) **(319 401/REQ-7.4-07)**: The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation of security administration and operation functions.
Particularly, use of system utility programs shall be restricted and controlled.

BankID BankAxept AS TWS provide sufficient computer security controls for the separation of trusted roles, including the separation of security administration and operation functions in line with BankID BankAxept AS access control policy.

Privileged access management is implemented.

Use of system utility programs are controlled and restricted to specially authorized personnel.

f) **(319 401/REQ-7.4-08)**: TSP's personnel shall be identified and authenticated before using critical applications related to the service.

All personnel appointed to trusted roles are identified and authenticated before getting access to BankID BankAxept AS Trustworthy system.

g) **(319 401/REQ-7.4-09)**: TSP's personnel shall be accountable for their activities.

Personnel appointed to trusted roles are accountable for their activities. Their actions in BankID BankAxept AS TWS are logged in accordance with log-policy.

h) **(319 401/REQ-7.4-10)**: Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) or media (see clause 7.3.2) being accessible to unauthorized users.

BankID BankAxept AS have processes in place ensuring that media with production data shall never leave the security zone to which they have belonged. Media and storage objects containing sensitive data are shredded in a controlled process which shall destroy all information stored on the media completely. The shredding will be carried out by personell in trusted roles.

4.4.1 Trusted services specific controls

Certificate Services

a) **(319 411-1/GEN-6.4.3-02)**: Certificate issuance by the root CA shall be under at least dual control by authorized, trusted personnel such that one person cannot sign subordinate certificates on his/her own.

BankID BankAxept AS have processes in place ensuring that issuance by the root CA is performed under at least dual control. Procedures state that 4 persons in trusted roles will be present during Certificate issuance by the Root CA; PKI Administrator, PKI Supervisor, Root CA key custodian and Security Officer

4.5 Cryptographic controls

a) **(319 401/REQ-7.5-01)**: Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.

All cryptographic keys used by any of BankID BankAxept AS Trust Services are generated, stored and used within HSMs.

Critical cryptographic keys are managed by HSMs certified in accordance with ISO/IEC 15408 with assurance level EAL 4+ and ISO 19790. Other cryptographic keys are stored according to their criticality, at least in key vaults using HSMs conforming to FIPS 140-2, level 2.

HSMs used for the signature generation services shall be certified according to the standards listed above and also fulfilling evaluation criteria in EN 419 221-5 as a QSCD.

Established management practices, operations and security controls are in line with vendors recommendations for maintaining the operational requirements in line with the HSMs certification.

When cryptographic keys are backed up, the backups will be encrypted by a key protected by equivalent security controls to the key to be backed up.

4.5.1 Trusted services specific controls

Certificate Service

a) **(319 411-1/OVR-6.5.2-01)**: TSP's key pair generation, including keys used by revocation and registration services, shall be carried out within a secure cryptographic device which is a trustworthy system which:

a) is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [12], or equivalent national or internationally recognized evaluation criteria for IT security provided this is a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or
b) meets the requirements identified in ISO/IEC 19790 [13], FIPS PUB 140-2 [14] level 3 or FIPS PUB 140-3 [15] level 3.

See chapter 4.5 letter a)

b) **(319 411-1/OVR -6.5.2-02)**: The secure cryptographic device shall be operated in its configuration as described in the appropriate certification guidance documentation or in an equivalent configuration which achieves the same security objective.

See chapter 4.5 letter a)

c) **(319 411-1/OVR -6.5.2-03)**: The above secure cryptographic device should be assured using ISO/IEC 15408 [12], as per OVR-6.5.2-01-a), above.

See chapter 4.5 letter a)

d) **(319 411-1/GEN-6.5.2-04)**: The CA private signing key shall be held and used within a secure cryptographic device meeting the requirements of OVR-6.5.2-01 and OVR-6.5.2-02 above.

See chapter 4.5 letter a)

e) **(319 411-1/GEN-6.5.2-05)** [CONDITIONAL]: When outside the secure cryptographic device (see GEN-6.5.2-04 above) the CA private key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.

BankID BankAxept AS CAs Private signing Keys are stored and protected by an HSM where access control mechanisms, physical and logical, ensure that CA's Private Keys are not accessible outside the HSM.

f) **(319 411-1/GEN-6.5.2-06)**: The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 6.4.2).

Only authorized personnel in trusted roles under dual control have access to HSMs located in High security zones, see chapter 0 sub-heading "Certificate Services".

Backup and restore of private keys require a key custodian in addition to a system administrator and a supervisor.

g) **(319 411-1/GEN-6.5.2-07)**: The number of personnel authorized to carry out the CA private signing key back up, storage and recovery shall be kept to a minimum and be consistent with the CA'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 chapter 4.2 above. The number of personnel in these roles are in line with resource requirements to maintain the service operations and security requirements.

h) **(319 411-1/GEN-6.5.2-08)**: Copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.

See letter e) above

i) **(319 411-1/GEN-6.5.2-09)** [CONDITIONAL]: Where the CA private signing keys and any copies are stored in a dedicated secure cryptographic device, access controls shall be in place to ensure that the keys are not accessible outside this device.

See letter e) above

j) **(319 411-1/OVR -6.5.2-10)**: The secure cryptographic device shall not be tampered with during shipment.

BankID BankAxept AS has in place procedures in line with manufacturers recommendations verifying the integrity of the HSM on reception. Shipment is a strictly controlled process where units are controlled, and production serial numbers verified before they are unwrapped.

k) **(319 411-1/OVR -6.5.2-11)**: The secure cryptographic device shall not be tampered with while stored.

BankID BankAxept AS has in place procedures in line with manufacturers recommendations verifying the correctness of the HSM functionality at deployment and startup.

l) **(319 411-1/OVR -6.5.2-12)**: The secure cryptographic device shall be functioning correctly.

See letter k) above. The devices perform regular self tests and stop functioning if errors are detected.

m) **(319 411-1/GEN-6.5.2-13)**: The CA private signing keys stored on the CA's secure cryptographic device shall be destroyed upon device retirement.

Retired HSM will be handled according to BankID BankAxept AS decommission and destruction process.

Timestamping Service

The following particular requirements apply:

n) **(319 421/ 7.6.2- a))**: The generation of the TSU's signing key(s) shall be undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under, at least, dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practices.

The generation of the TSU's signing key(s) is undertaken in a physically secured environment by personnel in trusted roles (as per chapter 3.3) under, at least, dual control.

The personnel authorized to carry out this function is limited to those required to do so under the BankID BankAxept AS' practices.

o) **(319 421/7.6.2-b))**: The generation of the TSU's signing key(s) shall be carried out within a secure cryptographic device which:
   1. is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [12], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or
   2. meets the requirements identified in ISO/IEC 19790 [13] or FIPS PUB 140-2 level 3 [14].

The generation of the TSU's signing key(s) is carried out within a secure cryptographic device which is a trustworthy system assured to EAL 4+ in accordance with ISO/IEC 15408 [12], to a protection profile from EN 419221-5 [16].

p) **(319 421/7.6.2-c))**: The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key should be as specified in ETSI TS 119 312 [i.16].

The TSU key generation algorithm, the resulting signing key length and signature algorithm used for signing time-stamps key are as specified in ETSI TS 119 312 [i.16]. The signature algorithm used is ECDSA NIST P256.

q) **(319 421/7.6.2-d))**: A TSU's signing key should not be imported into different cryptographic modules.

TSU signing key is not imported into different cryptographic modules.

r) **(319 421/7.6.2-e))** [CONDITIONAL]: If there are same keys in different cryptographic modules, they shall be associated with the same public key certificate into all the different cryptographic modules.

Each TSU signing key is always associated with only one public key certificate.

s) **(319 421/7.6.2-f))**: A TSU shall have a single time-stamp signing key active at a time.

A TSU has a single time-stamp signing key active at a time.

TSU private key protection

The TSU private keys shall remain confidential and their integrity shall be maintained with at least the following particular requirements:

t) **(319 421/7.6.3-a))**: The TSU private signing key shall be held and used within a cryptographic module which:
   1. is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [12], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or
   2. meets the requirements identified in ISO/IEC 19790 [13] or FIPS PUB 140-2 level 3 [14].

The TSU private signing key is held and used within a cryptographic module which is a trustworthy system which is assured to EAL 4+ in accordance with ISO/IEC 15408 [12], to a protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

u) **(319 421/7.6.3-b))**: If TSU private keys are backed up, they shall be copied, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8). The personnel authorized to carry out the backup function shall be limited to those required to do so under the TSA's practices.

TSU private keys are recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

The backup function is automated and configured by authorized personnel.

v) **(319 421/7.6.3-c))**: Any backup copies of the TSU private signing keys shall be protected to ensure its integrity and confidentiality by the cryptographic module before being stored outside that device.

Backup copies of TSU private signing keys are manually sent to a backup HSM through built-in secure mechanisms.

TSU Life cycle management of signing cryptographic hardware

The following particular requirements apply:

w) **(319 421/7.6.6-a))**: Time-stamp signing cryptographic hardware shall not be tampered with during shipment.

See chapter 4.5.1 letter j).

x) **(319 421/ 7.6.6-b))**: Time-stamp signing cryptographic hardware shall not be tampered with when and while stored.

See chapter 4.5.1 letter k).

y) **(319 421/7.6.6-c))**: Installation, activation and duplication of TSU's signing keys in cryptographic hardware shall be done only by personnel in trusted roles using, at least, dual control in a physically secured environment (see clause 7.8).

Installation, activation, and duplication of TSU's signing keys in cryptographic hardware is done only by personnel in trusted roles (see chapter 4.2) using, at least, dual control in a physically secured environment (see chapter 4.6).

z) **(319 421/7.6.6-d))**: TSU private signing keys stored on TSU cryptographic module shall be erased upon device retirement in a way that it is practically impossible to recover them.

See chapter 4.3.2 and chapter 4.5.1 letter m).

4.6 Physical and environmental security

a) **(319 401/REQ-7.6-01)**: The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security.

Physical security barriers and controls are implemented to protect areas containing BankID BankAxept AS TWS and information related to BankID BankAxept AS Trust Services. This includes all IT systems and components such as servers, HSMs that allow access to private keys and other limited data in the central storage facility, as well as any external cryptographic hardware module or smart card.

b) **(319 401/REQ-7.6-02)**: Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.

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

Access to High Security Zones requires dual control involving two authorized persons.

c) **(319 401/REQ-7.6-03)**: Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.

BankID BankAxept AS maintains and enforces controls covering secure and trusted handling of all assets related to the TWS, including transport of security sensitive and critical assets off-site. Physical controls such as restricted access with dual access control and regular inventory control are designed to prevent and detect unauthorized movement of assets.

d) **(319 401/REQ-7.6-04)**: Controls shall be implemented to avoid compromise or theft of information and information processing facilities.

BankID BankAxept AS maintains and enforces controls covering secure and trusted handling of all assets related to the TWS, including information and information processing facilities. Physical controls such as restricted access with dual access control and regular inventory control are designed to prevent and detect unauthorized movement of assets.

e) **(319 401/REQ-7.6-05)**: Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.

All TWS for the secure operation of BankID BankAxept AS Trust Services are located and operated within defined security locations (datacenters) providing multiple layers of physical and logical security including alarms and CCTV monitoring.

All critical system components (e.g. HSM, SAM, QSCD) are protected in High Security Zones. High Security Zones are located within security locations, separated with enforced walls. The High Security Zones are monitored by cameras outside/inside the room.

4.6.1 Trust Services specific controls

Certificate Services

a) **(319 411-1/OVR-6.4.2-02)**: The facilities concerned with certificate generation and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data.

BankID BankAxept AS operations facilities are specifically designed for computer operations and have been customized to meet the security requirements that apply to BankID BankAxept AS Trust Services including Certificate Services. Relevant prevention and detection mechanisms are in place to address environmental incidents, hereunder power loss, loss of communication, water exposure, fire and temperature changes.

b) **(319 411-1/OVR-6.4.2-03)**: Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area.

Access to BankID BankAxept AS facilities containing TWS including CA operations are restricted to authorized personnel in trusted roles only. Non-authorized personnel, including visitors, are only allowed to access the facilities under escort and continuous surveillance by authorized personnel. Dual control has been implemented for physical access to the TWS including CA operations facilities. Access requires physical presence of two authorized persons, each with their own personal authentication token.

Established routines ensure that no authorized person will stay in the TWS including CA operations facilities alone. Visitors and non-authorized persons are not at any circumstances permitted to stay alone within the TWS including CA operations facilities.

c) **(319 411-1/OVR-6.4.2-04)**: Every entry and exit shall be logged.

Established routines and access control mechanisms ensure that every entry and exit is logged. Access by authorized personnel is logged electronically. Visitors are logged manually in a visitor log.

d) **(319 411-1/OVR-6.4.2-05)**: Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation and revocation management services.

See chapter 4.6, letters b) and e).

e) **(319 411-1/OVR-6.4.2-06)**: Any parts of the premises shared with other organizations shall be outside the perimeter of the certificate generation and revocation management services.

BankID BankAxept AS TWS facilities including CA operations are protected with several tiers of defined security perimeters. The inner tiers being Security Zones and High Security Zones are dedicated to BankID BankAxept AS operations alone and are only accessible to authorized personnel.

High Security and Security Zones are physically separated from parts of the premises shared with other organizations.

f) **(319 411-1/OVR-6.4.2-07)**: Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation.

See letter a) above

g) **(319 411-1/OVR-6.4.2-08)**: The TSP's physical and environmental security policy for systems concerned with certificate generation and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

See letter a) above

h) **(319 411-1/OVR-6.4.2-09)**: Controls shall be implemented to protect against equipment, information, media and software relating to the TSP's services being taken off-site without authorization.

BankID BankAxept AS maintains and enforces controls ensuring secure and trusted asset handling, including transport of security sensitive assets off-site. Physical and dual access control combined with regular inventory control are implemented to prevent and detect unauthorized movement of assets.

When a hardware component inside the High Security Zone is replaced, it shall be retained inside the zone for later destruction in a controlled process.

i) **(319 411-1/OVR-6.4.2-10)**: Other functions relating to TSP's operations may be supported within the same secured area provided that the access is limited to authorized personnel.

Other functions related to BankID BankAxept AS role as operator of Norwegian BankID COI, TSP offering Qualified Timestamping and Remote QSCD services are supported in the same secured area with the same access restrictions as for the CA operations.

j) **(319 411-1/OVR-6.4.2-11)**: Root CA private keys shall be held and used physically isolated from normal operations such that only designated trusted personnel have access to the keys for use in signing subordinate CA certificates.

BankID BankAxept AS Root CA Private Keys are held and used in standalone and air gapped equipment. All operations using the Root CA Private Keys are authorized by designated personnel in trusted roles for use when signing subordinate CA certificates and issuing CARL.

Timestamping Services

The following particular requirements apply:

k) **(319 421/ 7.8-a)**: Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clause 7.6.

Access controls are applied to TSU cryptographic modules as described in chapter 4.4 and 4.5

l) **(319 421/ 7.8-b)**: The time-stamping management facilities shall be operated in an environment which physically and logically protects the services from compromise through unauthorized access to systems or data.

The time-stamping management facilities are operated in an environment which physically and logically protects the services as described in chapter 4.6.

m) **(319 421/ 7.8-b)**: Every entry to the physically secure area shall be subject to independent oversight and non-authorized person shall be accompanied by an authorized person whilst in the secure area. Every entry and exit shall be logged.

See chapter 4.6 and 4.6.1 letters b) and c)

n) **(319 421/ 7.8-b)**: Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the time-stamping management. Any parts of the premises shared with other organizations shall be outside this perimeter.

See chapter 4.6 and chapter 4.6.1 letter e) and i).

o) **(319 421/ 7.8-b)**: Physical and environmental security controls shall protect the facility that houses system resources, the system resources themselves, and the facilities used to support their operation. The TSA's physical and environmental security policy for systems concerned with time-stamping management shall address as a minimum the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery.

See chapter 4.6

p) **(319 421/ 7.8-b)**: Controls shall protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

See chapter 4.3.1, 4.3.2 and chapter 4.6.1 letter h).

q) **(319 421/ 7.8)**: Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

See chapter 4.6.1 letter e) and i)

4.7 Operation security

a) **(319 401/REQ-7.7-01)**: The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

BankID BankAxept AS TWS and their components are protected against unauthorized modification by the operational processes supporting the TWS. The processes focus on enhancing technical security and reliability of systems and include operations like change management, purchase and development of systems and components, development as well as management of suppliers delivering components or software intended to be incorporated into BankID BankAxept AS TWS.

b) **(319 401/REQ-7.7-02)**: An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.

BankID BankAxept AS product development process mandates early identification of relevant compliance and security requirements for any product or system development to ensure that adequate level of security is built into the system or component.

BankID BankAxept AS software development process, applicable to both in-house and third-party development, ensures that security is built into BankID BankAxept AS TWS.

c) **(319 491/REQ-7.7-03)**: Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies to the TSP's security policy.

BankID BankAxept AS have in place and enforce formal change control procedures covering the implementation of software, scheduled software releases and emergency software fixes as well as configuration changes on systems or components affecting TWS security.

d) **(319 401/REQ-7.7-04)**: The procedures shall include documentation of the changes.

BankID BankAxept AS formal change control procedures mandates documentation of alle process steps maintaining an audit trail of all changes.

e) **(319 401/REQ-7.7-05)**: The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

Anti-virus/malware systems are installed to protect the integrity of BankID BankAxept AS TWS and information against viruses, malicious and unauthorized software.

f) **(319 401/REQ-7.7-08)**: Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.

BankID BankAxept AS has established and implemented procedures for all trusted and administrative roles impacting the provision of BankID BankAxept AS Trust Services.

g) **(319 401/REQ-7.7-09)**: The TSP shall specify and apply procedures for ensuring that:
   a) security patches are applied within a reasonable time after they become available.
   b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and
   c) The reasons for not applying any security patches are documented.

BankID BankAxept AS has in place formal change control procedures which are followed for the implementation of software, scheduled software releases and deployment of security patches.

A patch routine is implemented which involves the Change Acceptance Board. Patches that for some reason are not applied will also be discussed in a monthly meeting between BankID BankAxept AS and subcontractor. There is also defined a routine for how to perform roll-back if a patch has unexpected negative effects.

4.8 Network security

a) **(319 401/REQ-7.8-01)**: The TSP shall protect its network and systems from attack.

BankID BankAxept AS has implemented security controls to protect its TWS network from attack, these security controls include, but are not limited to: Network separation, traffic monitoring, firewalls, dedicated physical lines, redundant infrastructure, and denial of service protections.

b) **(319 401/REQ-7.8-02)**: The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.

BankID BankAxept AS segregates its TWS systems into three logical and physical zones, the cloud zone, the secure zone and the high secure zone. Low to medium risk systems are distributed between the cloud zone and the secure zone, whilst systems integral to the overall security of the services are placed in the high secure zone.

c) **(319 401/REQ-7.8-03)**: The TSP shall apply the same security controls to all systems co-located in the same zone.

BankID BankAxept AS has a standard for required security controls in each zone, and routines in place for ensuring compliance.

d) **(319 401/REQ-7.8-04)**: The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.

BankID BankAxept AS limits communication between zones to only the strictly necessary.

e) **(319 401/REQ-7.8-05)**: The TSP shall explicitly forbid or deactivate not needed connections and services.

BankID BankAxept AS actively hardens each runtime environment and configures firewalls according to the principle of least access.

f) **(319 401/REQ-7.8-06)**: The TSP shall review the established rule set on a regular basis.

BankID BankAxept AS routinely reviews firewall and other network configurations.

g) **(319 401/REQ-7.8-07)**: The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.9]).

BankID BankAxept AS ensures that TWS systems integral to the overall security of the services are operated in the high secure zone.

h) **(319 401/REQ-7.8-08)**: The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.

BankID BankAxept AS has a separate dedicated administration system for TWS operations, which includes a dedicated network and separate access scopes according to the privilege of least access.

i) **(319 401/REQ-7.8-09)**: The TSP shall not use systems used for administration of the security policy implementation for other purposes.

BankID BankAxept AS uses dedicated systems for administration of the security policy implementation. These systems are not used for other purposes.

j) **(319 401/REQ-7.8-10)**: The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).

BankID BankAxept AS ensures complete isolation between TWS production systems and other systems used during development.

k) **(319 401/REQ-7.8-11A)**: The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are isolated using logical, cryptographic or physical separation from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

BankID BankAxept AS ensures trusted authenticated channels of communications between TWS using logical, cryptographic or physical security controls. This is documented in low level design documents.

l) **(319 401/REQ-7.8-12)**: If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.

BankID BankAxept AS TWS external network connections and network infrastructure are both redundant.

m) **(319 401/REQ-7.8-13)**: The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

BankID BankAxept AS performs regular vulnerability scans against all parts of the Trusted Services. This testing is performed by competent specialized personnel, using industry standard tools. The personnel is independent of other operations of the TSP and has a code of ethics mandating them to disclose any findings.

n) **(319 401/REQ-7.8-13A)**: The vulnerability scan requested by REQ-7.8-13 should be performed once per quarter.

BankID BankAxept AS has implemented routines that ensure vulnerability scans are performed at least once per quarter.

o) **(319 401/REQ-7.8-14)**: The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.

BankID BankAxept AS performs yearly penetration tests against all parts of its Trusted Services. In addition new systems or systems with significant changes are penetration tested on demand.

p) **(319 401/REQ-7.8-14A)**: The penetration test requested by REQ-7.8-14 should be performed at least once per year.

BankID BankAxept AS has implemented routines that ensure penetration tests are performed at least once per year.

q) **(319 401/REQ-7.8-15)**: The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.

BankID BankAxept AS has implemented routines ensuring the evidence and reports from the penetration tests are retained and available to Auditors. This includes requirements on suitability of the testers.

r) **(319 401/REQ-7.8-16)**: Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.

BankID BankAxept AS ensures access to internal network domains are only accessible through the strictly required channels. Internal domains are protected by firewalls and acan only be reached from dedicated workstation in secure zones.

s) **(319 401/REQ-7.8-17)**: Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.

Firewalls in BankID BankAxept AS are configured to only allow strictly necessary communications, as such all unnecessary protocols and ports are prohibited.

4.8.1 Trust Services specific controls

Timestamping service

The following particular requirements apply:

a) **(319 421/ 7.10-a))**: The TSA shall maintain and protect all TSU systems in a secure zone.

See chapter 4.8 letters b) and g).

b) **(319 421/ 7.10-b)**: The TSA shall configure all TSU systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the TSA's operations.

See chapter 4.8 letter e).

c) **(319 421/ 7.10-c)**: Only trusted roles shall access secure zones and high security zones.

See chapter 4.6 letter b)

4.9 Incident management

a) **(319 401/REQ-7.9-01)**: System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.
NOTE 1: See clause 16 of ISO/IEC 27002:2013 [i.3] for guidance.

All system activities in BankID BankAxept AS TWS are continuously monitored, with alerts for security-sensitive events and traces of hostile behavior.

b) **(319 401/REQ-7.9-02)**: Monitoring activities should take account of the sensitivity of any information collected or analysed.

Sensitive, confidential information such as keys are never logged. Personal information is only logged in separate, protected audit logs. Access to log information and performing analyses is restricted to authorized personnel only.

c) **(319 401/REQ-7.9-03)**: Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.
NOTE 2: Abnormal network system activities can comprise (external) network scans or packet drops.

BankID BankAxept AS monitoring systems are set up to detect any abnormal activities in TWS and report such activities as alarms ensuring timely reaction to any unauthorized or irregular attempts to access resources.

d) **(319 401/REQ-7.9-04)**: The TSP shall monitor the following events:
   a) start-up and shutdown of the logging functions; and
   b) availability and utilization of needed services with the TSP's network.

BankID BankAxept AS TWS are monitoring and logging the events stipulated in this requirement.

e) **(319 401/REQ-7.9-05):** The TSP shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.

BankID BankAxept AS has in place several layers of security and monitoring of security measures combined with procedures for incident handling in order to quickly respond to incidents and reduce the impact and potential damage from security incidents and malfunctions.

f) **(319 401/REQ-7.9-06):** The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.

Information security incidents are responded to in accordance with BankID BankAxept AS documented procedures by an incident manager who will involve a Security Officer upon suspicion on a security event.

g) **(319 401/REQ-7.9-07)**: The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.

BankID BankAxept AS has procedures in place ensuring notification of any breach of security of loss of integrity impacting TWS or information therein. The procedures ensure timely notification to:

- NKOM within 24 hours after identifying security breach impacting any of BankID BankAxept AS Trust Services, and
- NDPA within 24 hours after identifying security breach impacting personal data managed within any of BankID BankAxept AS Trust Services. The NPDA's time limit of 72 hours for incident reporting will be used to collect further information for a complete report

h) **(319 401/REQ-7.9-08)**: Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

BankID BankAxept AS notification procedures ensure timely notification to natural and legal persons affected by the incident identified.

i) **(319 401/REQ-7.9-09)**: The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.

See letter c) above.

Logs with alerts for security-sensitive events and traces of hostile behavior are reviewed by trained personnel with sufficient privileges.

j) **(319 401/REQ-7.9-10)**: The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.

As a result of monitoring the given system, components and logs, BankID BankAxept AS has in place procedures to address any discovered vulnerability within 48 hours and create a plan to mitigate the vulnerability or document the reason why remediation is not required/feasible.

k) **(319 401/REQ-7.9-11)**: For any vulnerability, given the potential impact, the TSP shall [CHOICE]:
- create and implement a plan to mitigate the vulnerability; or
- document the factual basis for the TSP's determination that the vulnerability does not require remediation.

See letter j) above

l) **(319 401/REQ-7.9-12)**: Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

BankID BankAxept AS incident management and reporting procedures are designed and implemented with the goal of minimizing the potential damage.

4.10 Collection of evidence

a) **(319 401/REQ-7.10-01)**: The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

BankID BankAxept AS Trust Services have established audit logging procedures ensuring that all relevant information to ensure secure operation of BankID BankAxept AS TWS and providing evidence in case of legal proceedings.

Issuance of certificates and time stamps will be logged and retrievable from log files and archives.

Audit logs and registration records are stored for 7 years.

b) **(319 401/REQ-7.10-02)**: The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.

Confidentiality and integrity of audit logs are protected at least at the same security level as the classification of data in the TWS the audit log originates from.

Manual logs are stored in the same physical security zone as the TWS.

Only personnel in trusted roles with authorized access to the TWS can access the audit logs

c) **(319 401/REQ-7.10-03)**: Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.

Log records concerning operation of services are backed up to a central log repository. Central log repository is replicated to two separate disc cabinets in two separate datacenters. Only authorized personnel can access the central log repository. All access to information in the central log repository is requested and logged in BankID BankAxept AS Change management system.

d) **(319 401/REQ-7.10-04)**: Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.

Records will be available (within the retention period) if required for legal proceedings.

e) **(319 401/REQ-7.10-05)**: The precise time of significant TSP's environmental, key management and clock synchronization events shall be recorded.

BankID BankAxept AS Trust Services procedures ensure that all events significant to the secure operation of BankID BankAxept AS TWS are recorded with the precise time. Key management operations and clock synchronization events are examples of significant events for logging.

f) **(319 401/REQ-7.10-06)**: The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

BankID BankAxept AS TWS are set to automatically sync clocks several times pr. hour using NTP service. In addition, there are daily scheduled tasks to verify the connection with the NTP server.

The NTP server is synchronized with UTC at least every 24th hour.

g) **(319 401/REQ-7.10-07)**: Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.3).

Logs are stored according to a defined log retention policy. Subjects are informed about the privacy policy in the PKI Disclosure Statement.

h) **(319 401/REQ-7.10-08)**: The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.

BankID BankAxept AS TWS are logging all events in a central log repository separated from the online system from which the log entry is originating. To ensure that all requirements for availability, integrity and confidentiality are met during the retention period, the central log repository is replicated to two separate disk cabinets in two separate datacenters accessible only for authorized personnel in trusted roles

4.10.1 Trusted Services specific controls

Certificate Services

a) **(319 411-1/OVR-6.4.5-02)**: All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and PKI system access attempts.

All activity performed in the production environment is recorded in the PAM solution. In addition, security events are logged by the PAM solution and the SecOps team have a defined set off alarms that are triggered by abnormal activity in the production environment. Firewall and router activities are logged and monitored by trained and authorised personnel.

b) **(319 411-1/REG-6.4.5-03)**: All events related to registration including requests for certificate re-key or renewal shall be logged.

See letter g) below

c) **(319 411-1/REG-6.4.5-04)**: All registration information including the following shall be recorded:

a) type of document(s) presented by the applicant to support registration;
b) record of unique identification data, numbers, or a combination thereof (e.g. applicant's identity card or passport) of identification documents, if applicable;
c) storage location of copies of applications and identification documents, including the subscriber agreement (see requirement REG-6.3.4-07);
d) any specific choices in the subscriber agreement (e.g. consent to publication of certificate, see requirement REG-6.3.4-07);
e) identity of entity accepting the application;
f) method used to validate identification documents, if any; and
g) name of receiving TSP and/or submitting Registration Authority, if applicable.

With reference to the letter index the following registration information is recorded:
Root-CA:

- Specially defined process for registration of information related to issuance of certificates to subordinate CAs.

TSA-CA:

- Specially defined process for registration of information related to issuance of certificates to TSU

eSign CA:

a) Not applicable – Subject/Signer authenticate to NIdP using existing eID means.
b) Unique identification data provided by the NIdP
c) Subject/Signer agreement obtained as part of e-Signature Service enrolment.
d) Not applicable, Subject/Signer Certificate are included in document signature for validation purpose.
e) Not applicable. Accepting entity is always BankID BankAxept AS
f) Not applicable. Authentication of Subject/Signer is delegated to NIdP
g) Not applicable

d) **(319 411-1/OVR-6.4.5-04A)**: The TSP shall document how the information recorded as per REG-6.4.5-04 is accessible.

See chapter 4.10 letter d)

e) **(319 411-1/REG-6.4.5-05)**: The TSP shall maintain the privacy of subject information.

BankID BankAxept AS maintains the privacy of Subject information in accordance with Norwegian laws and relevant EU regulations, ref. [1] and [2].

f) **(319 411-1/GEN-6.4.5-06)**: The TSP shall log all events relating to the life-cycle of CA keys.

All events related to the life-cycle of CA-keys, both Root-CA, eSign CA and TSA-CA, are logged.

g) **(319 411-1/OVR-6.4.5-07A)**: The TSP shall log all events relating to the life-cycle of certificates as requested by REV-6.3.9-18, REG-6.4.5-03, GEN-6.4.5-08, REV-6.4.5-09, SDP-6.4.5-10 as well as all events relating to certificates generation and dissemination.

For all BankID BankAxept AS Certificate services and related processes, BankID BankAxept AS ensures that appropriate audit logs are produced providing auditable proof of events. All events considered to have potential value as evidence in possible future disputes and/or legal proceedings are logged, and such logs are retained for 7 years.

Audit logs retained may be a combination of electronic logs and paper-based logs.

Logging is carried out in compliance with Norwegian laws and relevant EU regulations, ref. [1] and [2].

h) **(319 411-1/GEN-6.4.5-08)**: The TSP shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA.

BankID BankAxept AS CAs only manage keys used by the individual CA, see letter f) above. Subjects/Signers keys are managed by BankID BankAxept AS e-Signing service, see [10] chapters 3 and 4.

i) **(319 411-1/REV-6.4.5-09)**: The TSP shall log all requests and reports relating to revocation, as well as the resulting action.

All requests and reports relating to revocation of any BankID BankAxept AS CA and TSU Certificates as well as the resulting action is logged as part of established incident procedures. Subject/Signer Certificates are non-revocable Short-term certificates and revocation is not available for these Certificates, see [9] chapter 3.4 letter a)

j) **(319 411-1/SDP-6.4.5-10)** [NCP+]: The TSP shall log all events relating to the preparation of the subject's device.

Not applicable. Authentication is based on existing eID means prepared and issued by the NIdP.

k) **(319 411-1/OVR-6.4.5-11)**: The TSP shall document precisely the period of retention of the information mentioned above in its practices statements and shall indicate which information is subject to be handed-over through its termination plan.

The retention period for information mentioned above is as given in chapter 4.10 letter a).

Audit logs potentially providing evidence in case of legal proceedings may be part of information handed over in case of termination of services, see chapter 4.12

l) **(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 letter k) above.

e-Signature Service

m) **(119 431-1/OVR-6.4.5-02)**: All security events shall be logged, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and SSASC system access attempts.

All security events related to the e-Signature service are logged. See 4.10.1 letter a).

n) **(419 241-1/SRG_AA.1.1)**: As a minimum, the following events SHALL be logged:
- significant TW4S environmental, key management events (generation, usage and destruction);
- user signing events (e.g. successful signing with a signer's signing key and DTBS/R request management);
- user authentication during SAP;
- signer's SAD management by TW4S;
- start up and shut down of the audit data generation function;
- changes of the audit parameters.

User signing events SHALL include associate certificate to the signing key.

All access attempts to TW4S SHOULD be logged.

All required and significant events related to the signing operation including system and audit management events are logged.

o) **(419 241-1/SRG_AA.1.2)**: The TSP SHALL specify what is done (i.e. actions taken) in case of failure of passing audit information to any external storage.

All audit data from the TW4S systems involved are sent to a central audit log repository, ref chapter 4.10 letter c). In case of failing in this process, the failure will be logged, and the information will be resent later.

p) **(419 241-1/SRG_AA.2.1)**: TW4S SHALL maintain audit data and ensure that measures are taken for all audit data to be stored.

See chapter 4.10 letter c).

q) **(419 241-1/SRG_AA.2.2)**: The audit function SHALL only append information.

All audit log records are append only, this is valid both for information created in the TW4S and stored in the central audit log repository.

r) **(419 241-1/SRG_AA.2.3)**: TW4S SHALL protect the stored audit records in the audit trail from unauthorized deletion.

The central audit log repository is protected to ensure that no audit records are deleted unauthorized.

s) **(419 241-1/SRG_AA.2.4)**: Audit records MAY be deleted when archived to an external storage.

Audit records not required to be retained for 7 years by other requirement are deleted when archived to external storage. All audit records are deleted after 7 years.

The central audit log repository is kept in accordance with the retention period ref. chapter 4.10 letter g).

t) **(419 241-1/SRG_AA.3.1)**: All audit records (including service specific audit logging) SHALL contain the following parameters:
   - Date and time of event;
   - Type of event;
   - Identity of the entity (e.g. user, administrator, process) responsible for the action;
   - Success or failure of the audited event.

Each audit log entry contains an event description, type of event, date and time of event, result of the event and a reference to the entity that triggered the event.

u) **(419 241-1/SRG_AA.7.1)**: TW4S SHALL ensure the integrity of the audit data.

All audit log records are individually protected using HMAC with secret key stored in HSM.

v) **(419 241-1/SRG_AA.7.2)**: TW4S SHALL provide a function to verify the integrity of the audit data.

The integrity of audit data is verified by performing HMAC operation on the audit data and comparing the new HMAC result with the HMAC stored with the audit data.

w) **(419 241-1/SRG_SO.2.2)**: In order to ensure time accuracy of audited events, a time source suitably synchronized with a standard time source SHOULD be used.

The time in all TW4S is synchronized with a standard time source, an NTP server.

Timestamping Service

TSU key management

x) **(319 421/7.12-a))**: Records concerning all events relating to the life-cycle of TSU keys shall be logged.

Records concerning all events relating to the life-cycle of TSU keys are logged.

y) **(319 421/7.12-b))**: Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

Records concerning all events relating to the life-cycle of TSU certificates are logged.

Clock Synchronization

z) **(319 421/7.12-c))**: Records concerning all events relating to synchronization of a TSU's clock to UTC shall be logged. This shall include information concerning normal re-calibration or synchronization of clocks used in time-stamping.

Records concerning all events relating to synchronization of a TSU's clock to UTC are logged. Records include information concerning normal re-calibration or synchronization of clocks used in time-stamping.

aa) **(319 421/OVR-7.12-06)**: Records concerning all events relating to detection of loss of synchronization shall be logged.

Records concerning all events relating to detection of loss of synchronization are logged.

4.11 Business continuity management

a) **(319 401/REQ-7.11-01)**: The TSP shall define and maintain a continuity plan to enact in case of a disaster.

BankID BankAxept AS has a continuity plan covering all of its Trust Services that shall be followed in case of a crisis.

The document is maintained at least annually. The appendix with names and addresses of people in specific roles, are updated when there are changes.

b) **(319 401/REQ-7.11-02)**: In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.

BankID BankAxept AS has a routine for security incident management which describes technical and practical measures for detection and remediation.

4.11.1 Trusted services specific controls

Certificate services

a) **(319 411-1/OVR-6.4.8-01)**: The requirements identified in ETSI EN 319 401 [3], clauses 7.9 and 7.11, shall apply.

See chapters 4.9 and 4.11 respectively.

b) **(319 411-1/OVR-6.4.8-02)**: TSP's systems data necessary to resume CA operations shall be backed up and stored in safe places, preferably also remote, suitable to allow the TSP to timely go back to operations in case of incident/disasters.

BankID BankAxept AS TWS including CA operations are deployed in two physical separate locations, each location capable of handling normal load operations for several days. All essential software, information and systems data necessary to resume BankID BankAxept AS Trust services are kept and backed up in a version control system.

c) **(319 411-1/OVR-6.4.8-03)**: In line with ISO/IEC 27002 [i.3], clause 12.3: Back-up copies of essential information and software should be taken regularly.

Back-ups as described in letter b) above, are taken regularly.

d) **(319 411-1/OVR-6.4.8-04)**: Adequate back-up facilities should be provided to ensure that all essential information and software can be recovered following a disaster or media failure.

See letter b) above

e) **(319 411-1/OVR-6.4.8-05)**: Back-up arrangements should be regularly tested to ensure that they meet the requirements of business continuity plans.

Back-ups are tested as part of BankID BankAxept AS disaster recovery test program.

f) **(319 411-1/OVR-6.4.8-06)**: Backup and restore functions shall be performed by the relevant trusted roles specified in clause 6.4.4.

Backup and restore are performed by the relevant trusted roles, see chapter 4.2. letter c).

g) **(319 411-1/OVR-6.4.8-07)** [CONDITIONAL]: If risk analysis identifies information requiring dual control for management, for example keys, then dual control should be applied to recovery.

Dual control is applied to all recovery operations that also requires dual control for daily operations.

h) **(319 411-1/OVR-6.4.8-08)**: The TSP's business continuity plan (or disaster recovery plan) shall address the compromise, loss or suspected compromise of a CA's private key as a disaster.

BankID BankAxept AS business continuity plan defines the event of any of its CAs Private key being compromised, suspected compromised or lost as a disaster. See chapter 4.11.

i) **(319 411-1/OVR-6.4.8-09)**: The processes planned as per requirement OVR-6.4.8-08 shall be in place.

BankID BankAxept AS business continuity plan are in place and regularly tested and revised.

j) **(319 411-1/OVR-6.4.8-10)**: Following a disaster, the TSP shall, where practical, take steps to avoid repetition of a disaster.

BankID BankAxept AS have in place procedures for incident handling, including procedures for root-cause analysis.

k) **(319 411-1/OVR-6.4.8-11)**: The TSP shall inform the following of the compromise: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties and TSPs.

BankID BankAxept AS business continuity plan includes communications plan ensuring that all relevant parties are informed, including supervisory authorities, NKOM and NDPA

l) **(319 411-1/OVR-6.4.8-12)**: The TSP shall make the information in OVR-6.4.8-11 available to other relying parties.

The above information OVR-6.4.8-11 is available to all relying parties, in the relaying party self-service portal.

m) **(319 411-1/OVR-6.4.8-13)**: The TSP shall indicate that certificates and revocation status information issued using this CA key may no longer be valid; and

BankID BankAxept AS will, in case of key compromise, indicate on the BankID BankAxept AS website that certificates and revocation status information issued by the affected CA may no longer be valid.

n) **(319 411-1/OVR-6.4.8-14A)**: The TSP shall revoke any CA certificate it has issued when the TSP is informed of the compromise of such a CA (including when the compromised CA is part of the TSP or is managed by another TSP).

CA certificates revoked by BankID BankAxept AS Root-CA will be published in the Root-CA's CARL and published on BankID BankAxept AS web site.

o) **(319 411-1/OVR-6.4.8-15)**: Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall inform all subscribers and relying parties with whom the TSP has agreement or other form of established relations. In addition, the TSP shall make this information available to other relying parties.

BankID BankAxept AS will inform subscribers and relying parties with whom there is an agreement, and make information available to a wider audience. The process for information sharing depends upon the urgency of the compromise situation.

p) **(319 411-1/OVR-6.4.8-16)**: Should any of the algorithms, or associated parameters, used by the TSP or its subscribers become insufficient for its remaining intended usage then the TSP shall schedule a revocation of any affected certificate.

BankID BankAxept AS has routines for handling a potential key compromise.

Timestamping Service

q) **(319 421/ 7.13-a)**: The TSA's disaster recovery plan shall address the compromise or suspected compromise of TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued.

BankID BankAxept AS' business continuity plan addresses all of the above stated incidents.

r) **(319 421/ 7.13-b)**: In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp the TSA shall make available to all subscribers and relying parties a description of compromise that occurred.

BankID BankAxept AS will indicate on the BankID BankAxept AS website that a compromise has occurred.

s) **(319 421/ 7.13-c)**: In the case of compromise to a TSU's operation (e.g. TSU key compromise), suspected compromise or loss of calibration the TSU shall not issue time-stamps until steps are taken to recover from the compromise.A TY

In the case of compromise to a TSU's operation (e.g. TSU key compromise), suspected compromise or loss of calibration the TSU will not issue time-stamps until steps are taken to recover from the compromise.

t) **(319 421/ 7.13-d)**: In case of major compromise of the TSA's operation or loss of calibration, the TSA shall make available to all subscribers and relying parties information which can be used to identify the timestamps which may have been affected, unless this breaches the privacy of the TSAs users or the security of the TSA services.

In case of major compromise of BankID BankAxept AS' operation or loss of calibration, BankID BankAxept AS will make available to all subscribers and relying parties information which can be used to identify the timestamps which may have been affected, unless this breaches the privacy of BankID BankAxept AS' users or the security of BankID BankAxept AS' services.

4.12 TSP termination and termination plans

a) **(319 401/REQ-7.12-01)**: Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued

maintenance of information required to verify the correctness of trust services shall be provided.

If BankID BankAxept AS should decide to terminate their services, a pre-produced termination plan will be activated. This plan describes how customer data will be maintained during a termination process.

b) **(319 401/REQ-7.12-02)**: The TSP shall have an up-to-date termination plan.

BankID BankAxept AS has in place termination plans ensuring smooth termination of the Trust Service(s).

The termination plan will be revised annually or when there are major services in organization or services.

c) **(319 301/REQ-7.12-03)**: Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.

The termination plans for Trust Services have a list of actors and entities BankID BankAxept is obliged to contact in case of termination. This include:
- National Supervisory Body for Trust Services (NKOM),
- BankID BankAxept AS' eIDAS Conformance Assessment Body (Tüv Nord),
- Subscribers, including relying parties,
- Providers of other BankID BankAxept AS' services
- Subcontractors

d) **(319 401/REQ-7.12-04)**: Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.

For a scheduled or controlled termination, public information shall be provided at least 3 months in advance.

For unscheduled termination, information on the termination will be provided on BankID BankAxept AS' public website no more than 24 hours after termination.

e) **(319 401/REQ-7.12-05)**: Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.

Termination of contracts with subcontractors is a part of the termination plan.

The notification message to subcontractors shall make it clear that operation is halted and contracts terminated. Subcontractors will be instructed not to act on behalf of BankID BankAxept unless directly encouraged to, as part of the termination process.

f) **(319 401/REQ-7.12-06)**: Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.

Before the services terminate, BankID BankAxept AS will transfer obligations to a reliable party according to the termination plan.

g) **(319 401/REQ-7.12-07)**: Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

As a final step in the termination process, private keys, including backup copies, shall be destroyed in a process that involve at least two people in trusted roles as described in termination procedures.

h) **(319 401/REQ-7.12-08)**: Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.

When termination is decided, BankID BankAxept will investigate the possibilities for transferring provision of the trust services to another TSP.

i) **(319 401/REQ-7.12-09)**: The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.

See chapter 4.1.1 letter d)

j) **(319 401/REQ-7.12-10)**: The TSP shall state in its practices the provisions made for termination of service. This shall include:
   a) notification of affected entities; and
   b) where applicable, transferring the TSP's obligations to other parties.

Termination of services will be performed according to termination plan including:

- Notification to affected entities (see list in 4.12 letter c))

- Transferring the obligations to other parties if applicable

A part of the termination procedure will be to see if another actor can take over the service and the obligation. If that is not found, an arrangement for storage of data is provided.

k) **(319 401/REQ-7.12-11)**: The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.

Transfer of the public key will be a part of the data transfer after termination.

BankID BankAxept will ensure that the public keys of terminated services are kept published together with an explanation of the key's status for a reasonable time.

4.13 Compliance

a) **(319 401/REQ-7.13-01)**: The TSP shall ensure that it operates in a legal and trustworthy manner.

BankID BankAxept AS is a reliable organization, duly registered with The Brønnøysund Register Center in The Register of Business Enterprises.

BankID BankAxept AS is operating in a trustworthy manner in accordance with applicable Norwegian laws as well as applicable policies for the Trust Services described in this document.

b) **(319 401/REQ-7.13-02)**: The TSP shall provide evidence on how it meets the applicable legal requirements.

BankID BankAxept AS has provided the following evidence to eIDAS auditors:

- Third-party financial audit reports showing compliance with Norwegian business- and tax-laws,
- Relevant policies governing BankID BankAxept AS' business,
- Supporting documentation substantiating claims in this document

c) **(319 401/REQ-7.13-03)**: Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.

The Trust Services described in this document is available to any natural person who is:

- Capable of authenticating using eID means issued by a Notified eID issuer with LoA Substantial or High from an eID issuer trusted by BankID BankAxept AS, and
- Adhering to the applicable terms and conditions.

d) **(319 401/REQ-7.13-04)**: Applicable standards on accessibility such as ETSI EN 301 549 [i.10] should be taken into account.

BankID BankAxept AS has considered applicable accessibility standards when designing the Trust Services.

e) **(319 401/REQ-7.13-05)**: Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
NOTE 1: TSPs operating in Europe are required to ensure that personal data is processed in accordance with Directive 95/46/EC [i.1] until 25 May 2018, and from 25 May 2018 in accordance with Regulation (EU) 2016/679 [i.11] that repeals the Directive 95/46/EC [i.1]. In this respect, authentication for a service online concerns processing of only those identification data which are adequate, relevant and not excessive to grant access to that service online.
NOTE 2: See ISO/IEC 27701:2019 [i.13] for requirements and guidance on the extension to 27002 for privacy information management.

BankID BankAxept AS follows the Norwegian law for data protection which is equivalent to GDPR [i.1].

BankID BankAxept AS has a group of data protection officers that inspect products and services for GDPR conformance. They are consulted when trust services are developed or undergo major changes.