Stø AS e-Signature Service Practice Statement

Version 1.2 Last updated 23. September 2025.

Contents

Document history

Version	Date	Changes	Approved by
1.2	24.09.2025	Reflecting name change to Stø	ID Policy Board
1.1.2	12.11.2024	Minor changes for clarification Accepted all changes for readability	ID Policy Board
1.1.1	28.10.2024	Editorial change in section 3.1.8	As above
1.1	24.09.2024	Incorporating comments from Stage 1 audit	As above
1.0	08.05.2024	First approved version	ID Policy Board
0.9	03.05.2024	Temporary version	
0.8	08.04.2024	Initial complete version	

1 Introduction

This document describes the practices established by Stø AS for the e-Signing Service.

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.

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

This Practice Statement (PS) specifies the procedures, activities and rules implemented in order to fulfill the role as a Server Signing Application Service Provider (SSASP) operating a Server Signing Application Server Component (SSASC) providing Qualified and Advanced Remote electronic Signature Services in accordance with ETSI TS 119 431-1 [3].

This document provides a SSASC Policy (SCP) and a SSASC Practice Statement (SCPS) for the Remote e-Signing Service provided by BankID BankAxept AS and is structured according to, and complies with, the EU SSASC Policy (EUSCP) defined in ETSI TS 119 431-1 [3].

BankID BankAxept AS acts both as the SSASP providing Remote e-Signing services and as the TSP issuing Certificates for this Service.

1.1 Overview

BankID BankAxept AS e-Signing Service is a remote electronic signature service supporting Qualified Electronic Signature according to the Regulation (EU) No 910/2014 (eIDAS regulation) [i.1].

The service meets the requirements defined by the EUSCP in ETSI TS 119 431-1 [3] Annex A, for Qualified Electronic Signature:

- An EU SSASC Policy (EUSCP) which offers the same quality as that offered by the NSCP but with specific requirements from the related to QSCD management.

The policy and practices described herein is based on the Sole Control Assurance Level 2 (SCAL2) according to CEN EN 419 241-1 [4]:

- Sole Control Assurance Level 2 (SCAL2):
  - The signing keys are used, with a high level of confidence, under the sole control of the signer.
  - The authorized signer's use of its key for signing is enforced by the SAM by means of SAD provided, by the signer, using the SAP, in order to enable the use of the corresponding signing key.

NOTE: The SAP is aimed to achieve the same sole control assurance level as what would be achieved by a stand-alone QSCD as defined in the Regulation (EU) No 910/2014 [i.1].

Figure 1, taken from Figure 2 in ETSI TS 119 431-1 [3], illustrates the interrelationships between the eSigning service sub-components, the BankID BankAxept services issuing signing certificates and external parties.

Figure 1 also provides an overview of the scope of this document.

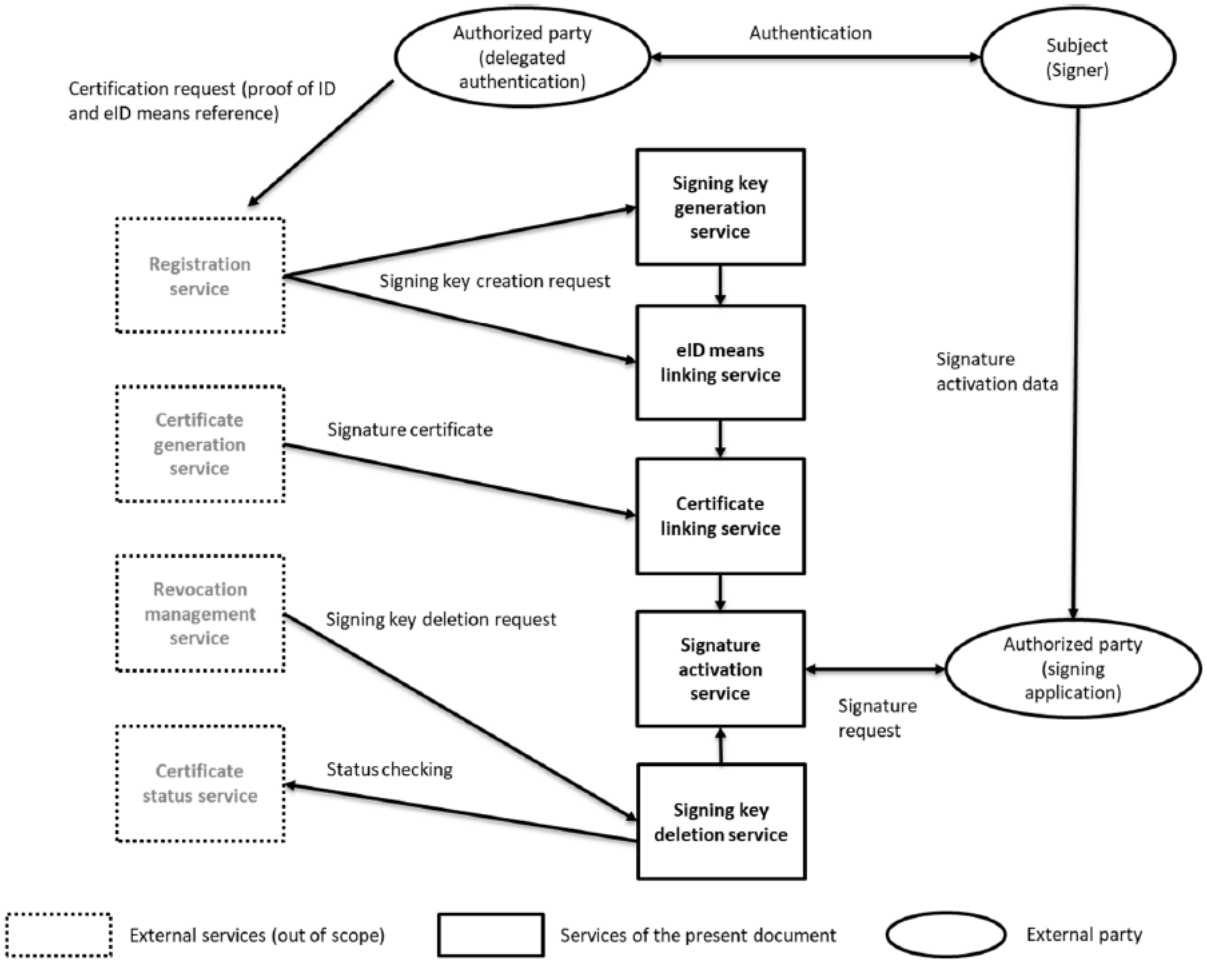

Figure 1:Illustration of subdivision of BankID BankAxept2 SSASC sub-components with delegated authentication

1.2 Document Name and Identification

The name of this document is:

“BankID BankAxept AS e-Signature Service Practice Statement”.

BankID BankAxept AS as a SSASP claims conformance to ETSI TS 119 431-1 [3] via the following specific trust service policy OID: EUSCP: EU SSASC Policy

itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE-policies(19431) ops (1) policy-identifiers(1) eu-remote-qscd (3)

1.2.1 Conventions

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

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 [11].

1.3 Participants

The BankID BankAxept AS Signature Service is based on a Remote Signing Service architecture, comprising the actors illustrated in Figure 2.

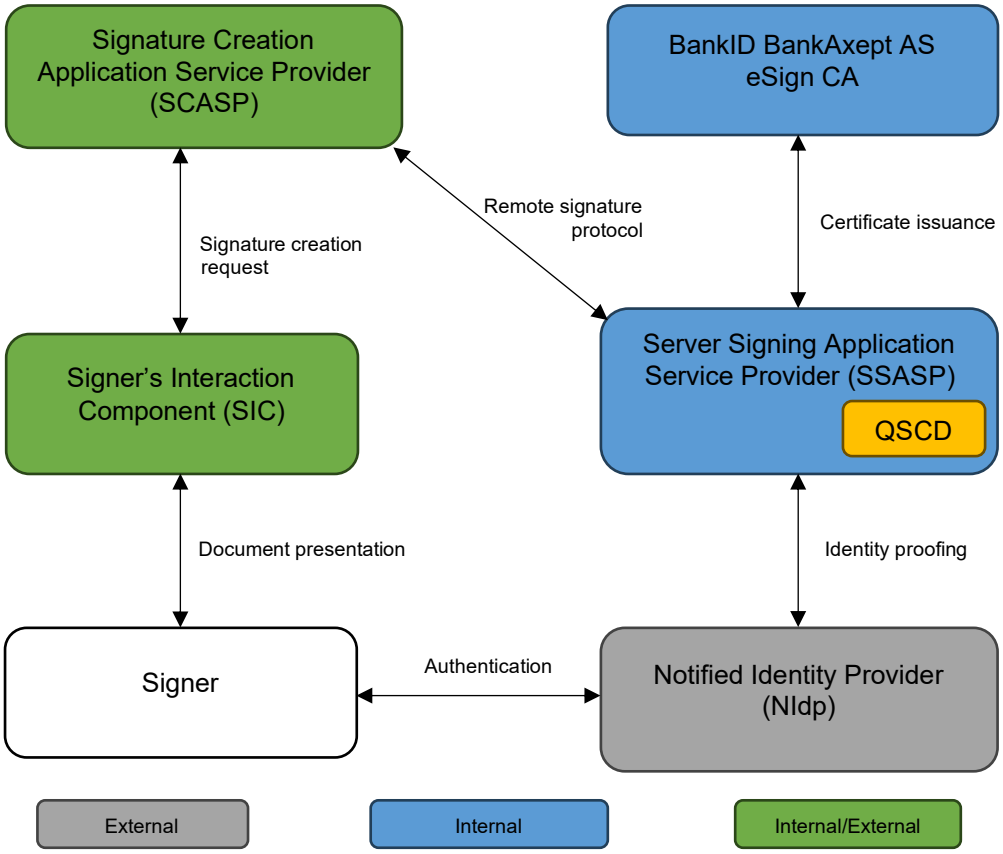

Figure 2: BankID BankAxept AS e-Signature Service architecture.

A **Server Signing Application Service Provider (SSASP)** is a Trust Service Provider (TSP) operating a Server Signing Application Server Component (SSASC). The SSASC is a server signing application used to create a digital signature on behalf of a Signer.

A **Signature Creation Application Service Provider (SCASP)** is a Trust Service Provider (TSP) operating a Signature Creation Application Service Component using the SSASP to create a digital signature.

BankID BankAxept AS is the Trust Service Provider (TSP) issuing certificates, both Qualified and non-qualified Certificates, as described in a Practice Statement (PS) for use by the SSASP in this architecture.

The Subjects/Signers are natural persons. The identity of the Signer is verified and confirmed by the Identity Service Provider (IdP) based on Signer authentication using an existing eID means under an eIDAS notified eID scheme. BankID BankAxept AS e-Signing Service supports use of existing eID means both LoA Substantial (non-qualified Certificate) and LoA High (Qualified Certificate).

The IdP in this architecture is referred to as the Notified Identity Service Provider (NIdP). The NIdP is responsible for the Identity Proofing of the Subject/Signer.

This document is intended for Notified Identity Service Providers, Subjects/Signers, Relying Parties (including the SSASP), Supervisory bodies, Auditors and possible Subcontractors.

1.3.1 Server Signing Application Service Provider (SSASP)

BankID BankAxept AS is the SSASP operating a remote QSCD on behalf of the Signers.

1.3.2 Certification Authorities

BankID BankAxept AS is the Certificate Authority (CA) issuing Certificates for Remote eSigning.

1.3.3 Subjects and signer

A Subject/Signer denotes the natural person that uses the BankID BankAxept eSigning service in order to create a digital signature on an electronic document managed by the SCASP.

1.3.4 Relying parties

Relying parties include any entity (natural and legal persons, systems, devices) accepting e-signatures provided by BankID BankAxept eSigning Service.

1.3.5 Other participants

This includes auditors, supervisory bodies, sub-contractors and other stakeholders needing detailed information about the BankID BankAxept eSigning Service.

1.4 Policy administration

For details related to policy and practices administration and responsibilities, please see [9] chapter 1.5.

1.5 Definitions and abbreviations

1.5.1 Definitions

For the purposes of the present document, the terms given ETSI TR 119 001 [i.2] and the following apply:

NOTE: Where a definition is copied from a referenced document this is indicated by inclusion of the reference identifier number at the end of the definition.

Authentication	Provision of assurance in the claimed identity of an entity NOTE: As defined in ISO/IEC 18014-2 [i.7].
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 Policy	A document containing rules for how certificates are issued and processed and thereby defining the trustworthiness of the certificates.
Certificate Signing Request	A formatted message sent from an applicant to a certificate authority containing the public key for which the certificate should be issued, Subject identifying information and a proof of authenticity including integrity protection (e.g. a digital signature).
Data To Be Signed Representation	Data formatted which is used to compute the digital signature value (e.g. hash value)

Digital Signature Value:	Result of the cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient electronic identification (eID): process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person NOTE: As defined in Regulation (EU) No 910/2014 [i.1].
eIDAS	Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, see [i.1]
Electronic Identification Means	Material and/or immaterial unit containing person identification data and which is used for authentication for an online service. NOTE: As defined in Regulation (EU) No 910/2014 [i.1].
Electronic Identification Means Reference	Data used in the SSASC as a reference to an electronic identification means in order to authenticate the signer EXAMPLE: When the eID means uses asymmetric keys, the public key can be the reference. When a signed assertion is generated after a successful authentication of the signer, the assertion signer id and the user id can be the reference. When the eID means uses a secret key (e.g. one time password generator) the secret key can be the reference.
Identity Provider	Entity that makes available identity information
Notified Identity Provider	Identity Provider issuing eIDs under an eID scheme notified under eIDAS [i.1]
Object Identifier	A sequence of integers which uniquely identifies an object. Objects in this context, means i.e. a defined information structure or a specification.
OpenID Connect	An identity authentication protocol that is an extension of open authorization (OAuth) 2.0 providing support for inclusion of profile information (attributes) related to the end user
Person Identification Data	Set of data enabling the identity of a natural or legal person, or a natural person representing a legal person to be established. NOTE: As defined in Regulation (EU) No 910/2014 [i.1].
Qualified electronic Signature/seal Creation Device (QSCD)	As specified in Regulation (EU) No 910/2014 [i.1].
Remote Signature Creation Device	Signature creation device used remotely from signer perspective and provides control of signing operation on the signer's behalf
Server Signing Application Service Component (SSASC)	TSP service component employing a server signing application to create a digital signature value on behalf of a signer

Server Signing Application Service Provider (SSASP)	TSP operating a server signing application service component
Signature Activation Data	Set of data, which is collected by the SAP, used to control with a high level of confidence a given signature operation, performed by a cryptographic module on behalf of the signer, that this under sole control of the signer
Signature Activation Module	Configured software that uses the SAD in order to guarantee with a high level of confidence that the signing keys are used under sole control of the signer
Signature Activation Protocol	Protocol that collects the SAD used to control a signature operation on a (set of) DTBS/R, using the signing key of the signer
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 the holder of the private key associated with the public key given in the Certificate (see Subject), acknowledging and adhering to any Subscriber obligations set forth in terms and conditions
Subject	Entity (natural person, system, device) identified in a Certificate as the holder of the private key associated with the public key given in the Certificate
Subscriber	See Signer
Trust Service	Electronic service that enhances trust and confidence in electronic transactions
Trust Service Provider (TSP)	Entity which provides one or more trust service
Trustworthy System Supporting Server Signing	Client-server system using signing keys under control of the signer, in order to create digital signatures

1.5.2 Abbreviations

CA	Certificate Authority
CP	Certificate Policy
CEN	Comité Européen de Normalisation (European Committee for Standardization)
CSR	Certificate Signing Request
DTBS/ R	Data To Be Signed Representation
eID	electronic Identification
EUSCP	EU SSASC Policy
IdP	Identity Provider
LoA	Level of Assurance
LSCP	Lightweight SSASC Policy
NIdP	Notified Identity Provider

NSCP	Normalized SSASC Policy
PID	Person Identification Data
OID	Object Identifier
OIDC	OpenID Connect
QSCD	Qualified electronic Signature/Seal Creation Device
SAD	Signature Activation Data
SAM	Signature Activation Module
SAP	Signature Activation Protocol
SCA	Signature Creation Application
SCASP	Signature Creation Application Service Provider
SCDev	Signature Creation Device
SCP	SSASC Policy
SIC	Signer's Interaction Component
SSA	Server Signing Application
SSASC	Server Signing Application Service Component
SSASP	Server Signing Application Service Provider
TSP	Trust Service Provider
TW4S	Trustworthy Systems Supporting Server Signing

1.6 References

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

1.6.1 Normative references

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

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

[2] 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".

[3] 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"

[4] CEN EN 419241-1:2018: "Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements", produced by CEN.

[5] ISO/IEC 15408:2022: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[6] CEN EN 419 221-5:2018: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services", produced by CEN.

[7] CEN EN 419 221-2:2018: “Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing”, produced by CEN

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

[9] Stø AS Trust Services Practice Statement

[10] Stø AS Certificate Service TSPS

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

1.6.2 Informative references

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

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

[i.2] ETSI TR 119 001 (v1.2.1): "Electronic Signatures and Infrastructures (ESI); The framework for standardization of signatures; Definitions and abbreviations".

[i.3] ETSI EN 319 403-1 (v2.3.1): "Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment; Part 1: Requirements for conformity assessment bodies assessing Trust Service Providers".

[i.4] ETSI TS 119 432 (v1.2.1): "Electronic Signatures and Infrastructures (ESI); Protocols for remote digital signature creation".

[i.5] IETF RFC 3647: "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

[i.6] ISO/IEC 15408:2022: "Information technology -- Security techniques -- Evaluation criteria for IT security".

[i.7] ISO/IEC 18014-2:2021: "Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens".

[i.8] CEN EN 419241-2:2019: "Trustworthy Systems Supporting Server Signing Part 2: Protection Profile for QSCD for Server Signing", produced by CEN.

[i.9] CEN EN 419221-5:2018: " Protection Profiles for TSP Cryptographic Modules - Part 5: Cryptographic Module for Trust Services", produced by CEN.

[i.10] ETSI TS 119 431-2 (v1.2.1): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 2: TSP service components supporting AdES digital signature creation".

[i.11] Commission Implementing Decision (EU) 2015/1502 of 8 September 2015, on setting out minimum technical specifications and procedures for assurance levels for electronic identification means.

1.7 Notations

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

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

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

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

1.8 General provisions

a) **(119 431-1/OVR-5.1-01):** The general requirements specified in ETSI EN 319 401 [1] clause 6.1 shall apply.

See [9], clause 3.1 with subsections.

b) **(119 431-1/OVR-5.1-02):** The TSPs practice statement shall include the signature algorithms and parameters applied, the algorithms applied for key pair generation and any other algorithms that are critical to the security of the SSASC operation.

Subject key pairs are from NIST P-256 curve (secp256r1).
Supported signature algorithms are ecdsa-with-SHA256 (OID: 1.2.840.10045.4.3.2)

CA keypairs are ECDSA using NIST P-384 (secp384r1) and supported signature algorithm are ecdsa-with-SHA384.

Regarding key pair generation, see [9] section 4.5 a).

c) **(119 431-1/OVR-5.1-03):** The TSPs shall publicly disclose its practice statement through an online means that is available on a 24x7 basis.

The information identified in the practice statement shall be available 24 hours per day, 7 days per week on the BankID BankAxept AS website.

d) **(119 431-1/OVR-5.2-01):** If changes are made to a SCP as described in clause 4.3.2 which affects the applicability then the policy identifier should be changed.

BankID BankAxept AS will use a defined signature creation policy. (See clause 1.2.) The policy identifier will only be changed if there are major changes to the policy.

e) **(119 431-1/OVR-A.3-01):** [EUSCP]: The TSP's practice statement shall include the reference to the certification that the QSCD employed against the requirements of Regulation (EU) No 910/2014 [i.1], annex II..

The BankID BankAxept AS deploys a QSCD certified according to:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model; CCMB-2017-04-001, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Components; CCMB-2017-04-002, Version 3.1, Revision 5, April 2017
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements; CCMB-2017-04-003, Version 3.1, Revision 5, April 2017,
    - EAL 4 assurance package augmented by AVA_VAN.5 defined in the CC Part 3.
- EN 419 241-2: Trustworthy Systems Supporting Server Signing Part 2: Protection Profile (PP) for QSCD for Server Signing.

Attestation of the certification is found on:

https://www.ocsi.gov.it/documenti/accertamenti/ascertia/ac_rda_eidas_adss_sam_702_v1.0.pdf

2 Publication and Repository Responsibilities

a) **(119 431-1/OVR-6.1-01)**: The TSP shall make available to subscribers and relying parties the applicable SCPs, practice statements and terms and conditions regarding the use of signing keys.

BankID BankAxept AS SCP, practice statement, terms and conditions regarding the use of signing keys are made available according to the practices described in [9] chapter 3.

b) **(119 431-1/OVR-6.1-02)**: The applicable terms and conditions shall be readily identifiable for a given signing key or for the associated certificate.

The applicable terms and conditions version agreed to for a given signature is logged and stored for 7 years.

All historical terms and conditions are also available on BankID BankAxept websites.

c) **(119 431-1/OVR-6.1-03)**: The information identified in OVR-6.1-01 and OVR-6.1-02 above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the TSP, the TSP shall apply best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the SSASC practice statement.

BankID BankAxept AS e-Signature Service Practice Statement (this document) is available as described in [9] chapter 3.1.

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

d) **(119 431-1/OVR-6.1-04)**: The information identified in OVR-6.1-01 above should be publicly and internationally available.

This document is accessible in English on BankID BankAxept AS web site.

3 Signing key initialization

3.1 Signing key generation

a) **(119 431-1/GEN-A.4-01)** [EUSCP]: Signer's signing key shall be generated in a QSCD.

Signer’s signing key is generated and used within a system evaluated and certified as a QSCD in accordance with ISO/IEC 15408 [5] and CEN EN 419 221-5 (PP HSM) [6].

b) **(419 241-1/SRA_SKM.1.1)**: Signer's signing key SHALL be generated and used in a SCDev that:

- is a trustworthy system which is ensured to EAL 4 or higher, augmented by AVA_vAN.5 in accordance with ISO/IEC 15408, 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 nontechnical security measures; or
- meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140-2 level 3.

See letter a) above

c) **(419 241-1/SRG_KM.1.2)**: The SCDev SHALL support cryptographic algorithms and key lengths corresponding to the appropriate level of security, which fulfils the security needs identified during the system design.

The QSCDs used support algorithms and key lengths providing an appropriate level of security according to recommendations in [8].

The QSCD is certified in accordance with ISO/IEC 15408 with assurance level EAL 4+ and ISO 19790, and fulfils the evaluation criteria in EN 419 221-5 as a QSCD.

See also 1.8 b) above.

d) **(419 241/ SRG_KM.1.3)**: When the private or secret keys (including signer's signing key, Infrastructure and Control Keys) are held outside the SCDev, these keys SHALL be protected to ensure the confidentiality and integrity of the keys.

BankID BankAxept AS have processes and mechanisms in place ensuring that private and secret Infrastructure and Control keys when held outside the QSCD, they are protected to the same security level as provided by the QSCD.

Subjects/Signers private signing key are never held outside the QSCD.

e) **(419 241/SRG_KM.1.4)**: SCDev SHALL be initialised, before generating or containing any signing key, with technical mechanisms that requires at least two operators in the SCDev.

The QSCD is initialized before any signing keys can be generated.

The initialization procedure requires use of authentication mechanisms enforcing dual control.

f) **(119 431-1/GEN-A.4-02)** [EUSCP]: The QSCD 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.

The QSCD is operated in its configuration as described in the certification documentation and according to vendor's guidance documentation.

g) **(419 241-1/SRC_SKS.1.1)**: Algorithm parameters to be used for signature creation by trustworthy systems SHALL be chosen so that can resist during the lifetime of the signer's certificate.

Signature algorithm used for e-Signing is ecdsa with 256 bit keys, and the certificates are valid only for 15 minutes in accordance with [8]. Certificate lifetime is very short.

h) **(419 241-1/SRC_SKS.1.3)**: Signer's signing key MAY be generated in advance (i.e. not linked to a public key certificate).

BankID BankAxept AS does not generate the signing key in advance.

i) **(119 431-1/GEN-6.2.1-08)** [CONDITIONAL]: If the SSASC and the certificate generation service component are managed separately, then the SSASC shall support the requirement defined in clause REG-6.3.1-01 of ETSI EN 319 411-1 [2].

When the Subject has been identified and authenticated at the required LoA, a signed token with the Subject's attributes authorizes use of the Subject's Private Key to sign a CSR which is passed to the BankID BankAxept eSign CA.

3.2 eID means linking

a) **(419 241-1/SRC_SA.1.1)**: The enrolment of the signer SHALL be as specified in Annex A, A.1, for assurance level low or higher.
The electronic identification means characteristics and design SHALL be as specified in Annex A, A.2.1, for assurance level low or higher.
The authentication mechanism SHALL be as specified in Annex A, A.2.2, for assurance level low or higher.

See letter b) below. Signer authentication will always be SCAL2.

b) **(419 241-1/SRA_SAP.1.1)** [NSCP] [CONDITIONAL]: The enrolment of the signer SHALL be as specified in Annex A, A.1, for assurance level low or higher.
The electronic identification means characteristics and design SHALL be as specified in Annex A, A.2.1, for assurance level low or higher.
The authentication mechanism SHALL be as specified in Annex A, A.2.2, for assurance level low or higher.

The enrolment of the Signer is based on using an eID means issued under a notified scheme under eIDAS with LoA Substantial and/or LoA High.

c) **(119 431-1/LNK-6.2.2-03)**: The SSASP shall link signing keys with the appropriate signer's eID means reference.

The public key and the eID means reference are included in the Short-term Certificate issued as part of the signature process.

d) **(119 431-1/LNK-6.2.2-04)**: The SSASP may generate eID means reference and provide the corresponding eID means to the signer (see clause 6.2.4).

The eID means reference is derived from a unique identifier provided by the NIdP.

e) **(119 431-11/LNK-6.2.2-05)**: The SSASP shall ensure that the person identification data linked to the eID means reference is the same as the one linked to the subject of the associated certificate.

Person Identification Data (PID) linked to the eID means are provided as Identity attributes from the NIdP. These identity attributes are linked to Subject attributes when requesting and issuing the certificate.

f) **(119 431-1/LNK-6.2.2-06)**: The signer's eID means reference may be provided by an authorized (external) party.

See letter d) above.

g) **(119 431-1/LNK-6.2.2-07)** [LSCP] [CONDITIONAL]: If all or part of the authentication process is delegated to an external party the SSASP shall ensure the external party meets the requirements specified in LNK-6.2.2-01.

Not applicable. Always NSCP.

h) (119 431-1/LNK-6.2.2-08 [NSCP] [CONDITIONAL]): If all or part of the authentication process is delegated to an external party the SSASP shall ensure that the external party meets the requirements specified in LNK-6.2.2-02 and LNK-6.2.2-03.

The Authentication process is delegated to an NIdP which complies to Commission Implementing Regulation (EU) 2015/1502 [i.11]

i) **(119 431-1/LNK-6.2.2-09)** [NSCP] [CONDITIONAL]: If all or part of the authentication process is delegated to an external party the SSASP shall ensure that:
- the external party fulfils all the relevant requirements of the present document and the requirements for registration according to the applicable regulatory requirements; or
- the authentication process delegated to the external party uses an eID means issued under a notified scheme in accordance with the applicable regulatory requirements.

See letter h) above.

j) **(119 431-1/LNK-6.2.2-10)**: The SSASP shall protect the integrity of links between signer's signing key and its eID means reference.

The integrity of the links between the Signer's signing key and its eID means reference is assured by including both the Subject's public key and the eID means reference in the Subject's/Signer's Certificate.

3.3 Certificate linking

a) **(419 241-1/SRC_SKS.1.2)**: TW4S SHALL link signer's signing keys with the appropriate signer's public key certificate.

The link between Signer's private signing key and public key is verified by verifying the signed CSR before certificate issuance. The signer's private signing key is used to sign the CSR containing the public key (using the QSCD).

b) **(419 241-1/SRC_SKS.1.4)**: A signing key SHOULD NOT be used before its public key certificate is linked by the TW4S.

The Signer's private signing key is used to sign a CSR representing proof of possession of the private signing key before the certificate is issued.

When generating signatures, the QSCD checks that the Signer's private signing key has a valid certificate before use.

c) **(419 241-1/SRC_SKS.1.5)**: TW4S SHALL protect the integrity of links between signer's signing key and public key certificate.

The integrity of the link between Signer's private signing key and the public key certificate is protected by the Certificate signed by BankID BankAxept AS eSign CA.

3.4 eID means provision

a) **(119 431-1/EID-6.2.4-01)** [CONDITIONAL]: If the SSASP provides the signer's eID means, the eID means shall be securely passed to the signer.

Not applicable. BankID BankAxept AS does not provide the eID means.

b) **(119 431-1/EID-6.2.4-02 [CONDITIONAL])**: If the SSASP personalizes the signer's eID means with an associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the signer's eID means.

Not applicable, see letter a) above

4 Signing key life-cycle operational requirements

4.1 Signature activation

a) **(419 241-1/SRC_SA.1.2)**: SSA SHALL require each signer to be successfully identified and authenticated before allowing any actions that can impact the sole control of any signing key.

The Signer is always required to be successfully identified and authenticated by the NIdP before the Signer's private signing key is generated and used.

b) **(419 241-1/SRC_SA.1.3)**: Protocols in use SHALL prevent man-in-the-middle attacks, replay attacks, and more generally any form of attacks where a malicious user can use authentication credentials which do not belong to him/her.

Identification and authentication of the Signer are undertaken by the NIdP which also provides the authentication credentials used by the Signer. The NIdP must comply to eIDAS and the implementing act 2015/1502 [i.11] which requires controls preventing a malicious user from using eID means belonging to another user.

Additionally, protocols in use between BankID BankAxept AS e-Signing Service and the NIdP include controls to prevent man-in-the-middle and replay attacks such as TLS, certificate pinning, use of nonce values, and returning signed/sealed responses that are validated by BankID BankAxept AS and compared to expected values.

c) **(419 241-1/SRA_SAP.1.3)**: SAP SHALL provide cryptographic strength mechanisms that protect the authentication factors against compromise by the protocol threats as well as trusted third party impersonation attacks.

See letter b) above.

d) **(419 241-1/SRC_SA.1.4)**: Access controls SHALL ensure that a signer does not have access to sensitive system objects and any functions which gives the user control over another's signing key.

Access controls are implemented ensuring that the Signer's private signing key is generated and will only be available to the Signer as part of that signing session.

A Signer will never obtain access to any part of BankID BankAxept TW4S nor another Signer's private signing key.

e) **(419 241-1/SRC_SA.1.5)**: The TW4S SHALL ensure that the DTBS/R provided under control of the signer is only signed by the signing key belonging to this signer.

The signature flow ensures that DTBS/R provided under control of the Signer is only signed by the private signing key belonging to that Signer.

f) **(419 241-/SRA_SKM.2.1)**: The TW4S SHALL require the signer to present a SAD to the SAM in order to be authenticated and to activate the signing key.

To activate and authorize use of the private signing key, the SAM requires a SAD. The SAD is constructed from verified data obtained from the NIdP.

See also 4.2 a) below.

g) **(419 241-1/SRA_SAP.1.2)**: Controls SHALL be provided, as determined necessary by a risk assessment, in order to counter the following threats on SAD and SAD use: online guessing, offline guessing, credential duplication, phishing, eavesdropping, replay, session hijacking, man-in-the middle, credential theft, spoofing and masquerading attacks.

BankID BankAxept AS implements controls, based on risk assessment, to protect against threats to the SAD. Risk assessments are described in [9], section 2 with subsections.

The SAD and SAD use is controlled. Protocols implemented for communication with external parties, see letter b) above, are deemed to provide sufficient protection against external threats.

Risk assessment covers these threats:

- Threats such as guessing, credential duplication, replay, session hijacking, spoofing, eavesdropping, replay and MITM attacks, are covered and primarily mitigated by the following controls:

-- TLS and mTLS (where applicable).

-- Security monitoring of the service.

-- Anti-fraud monitoring and detection alarms.

-- High entropy session identifiers.

- Phishing and "evil-proxy" like MITM attacks are much harder to protect against, especially since phishing-resistant credentials are not yet in use by all Notified IDPs.

-- Against these threats the only effective control we have in place is anti-fraud monitoring.

h) **(419 241-1/SRA_SAP.1.4)** The SAP SHALL be protected against replay, bypass and forgery attack between signer and the remote SCDev (e.g. with a nonce, timestamp or session token).

The SAP is protected against replay, bypass and forgery using TLS, nonce and integrity protection on the SAD.

i) **(419 241-1/SRA_SKM.2.5)**: Activated signing key SHALL be used to sign only DTBS/ R authorized by the SAP.

See letter e) above.

Each signing key exists only during one SAP session. The DTBS/R is provided in the same session.

j) **(119 431-1/SIG-6.3.1-08)**: The SSASP should ensure that the public key certificate is valid before using the corresponding signing key.

See chapter 3.3, letter b).

k) **(119 431-1/SIG-6.3.1-09)**: Signing keys shall be usable in only those cases for which the signer's consent has been obtained.

Subject's/Signer's consent will be obtained before the private signing key is generated and used.

l) **(419 241-1/SRC_DSC.1.1)**: Algorithm parameters for being used for signature creation by trustworthy systems SHALL be chosen so that can resist during the life time of the signer's certificate.

The Certificates have a short validity period of 15 minutes.

Algorithms for signature creation are in accordance with recommendations in [8].

m) **(419 241-1/SRA_SAP.1.5)**: The SAM SHALL be used in a tamper protected environment that:
- is a trustworthy system which is ensured to EAL 4 or higher in accordance with ISO /!EC 15408, 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
- meets the requirements identified in ISO/IEC 19790 or FIPS PUB 140- 2 level 3.

The SAM resides and is operated in a tamper protected environment evaluated in accordance with ISO/IEC 15408 and compliant with CEN EN 419 221-2 [7].

n) **(419 241-1/SRA_SAP.1.6)**: The SAP SHALL be designed such that it can be assumed that the SAD is always reliably protected against duplication or tampering against an attacker with high attack potential.

The SAP employs controls to ensure that the SAD is protected against replay, bypass and forgery attack using a nonce, a validity period and the authorization signature of the Signer. The SAP provides confidentiality for all sensitive transmitted data and integrity protection for all transmitted data, including the authentication, authorization data and DTBS/R.

The signing authorization is at Sole Control Assurance Level 2 (SCAL2) according to EN 419 241-1 [4] for qualified signatures.

o) **(419 241-1/SRA_SAP.1.7)**: The SAP SHALL be designed such that the signer can always reliably protect the signing key activation by the SAD against an attacker with high attack potential.

See letter n) above.

4.2 Signature activation data management

a) **(419 241-1/SRA_SAP.2.1)**: The SAD MAY be a set of data or be a result of cryptographic operations using mandatory parameters listed below.

The signed SAD cryptographically binds together:

- The Signer's identity and authentication
- An ID of the application which requested the signature
- The unique transaction ID
- The User's remote Signing Key ID held within the QSCD
- The data to be signed (DTBS/R)
- Random nonce information to prevent replay attacks
- Validity date/time for the authorization response

Each of the above elements within the signed SAD are verified by the SAM before allowing the Signer's key to be used for signing the data identified in the SAD.

b) **(419 241-1/SRA_SAP.2.2)**: The SAD MAY be collected or generated in the signer's environment by the SIC or remotely using the SIC under control of signer.

The SAD is generated remotely by a SIC under control of the signer.

c) **(419 241-1/SRA_SAP.2.3)**: The SAD SHALL link with a high level of confidence at least the following parameters:
- a given DTBS/R or a set of DTBS/R,
- items to identify the authenticated signer, and
- default or selected signing key.

If supported, it SHALL be possible to disable use of more than one DTBS/R in contexts where it is not legally permitted.

See letter a) above.

d) **(419 241-1/SRA_SAP.2.4)**: The SAD SHALL be used to activate signing key only if signer authentication succeeds (by e.g. computing SAD after successful authentication, or by other cryptographic means).

The SAD is only produced following successful authentication by NIdP. Signers maintain exclusive control of the signing key at Sole Control Assurance Level 2 (SCAL2) in accordance with EN 419 241-1 [4].

e) **(419 241-1/SRA_SAP.2.5)**: The SAD SHALL be passed to the SAM in the SAP

SAD is passed to SAM in the SAP and is integrity and confidentiality protected.

f) **(419 241-1/SRA_SAP.2.6)**: The SAD SHALL:
- be collected in a way that is under the control of the signer with a high level of confidence,
- be protected so that any keys held within devices are secure, and
- protect any secret used (one time or long term one) as defined in SRA_SAP.1.4

SAD is collected and under the control of the signer according to Sole Control Assurance Level 2.

The SAD is signed by a key stored in a High Security Environment

The SAD is asymmetrically signed and the corresponding private key is protected against tampering.

g) **(419 241-1/SRA_SAP.2.7)**: The SAP SHALL be designed such that if SAD are received by the SAM, it can be assumed that the SAD were submitted under sole control of the signer by means that are in possession of the signer.

See letter d) above.

h) **(419 241-1/SRA_SAP.2.8)**: The SAD SHALL be verified such that it is highly unlikely that activities such as guessing, eavesdropping, replay or manipulation of communication by an attacker with high attack potential can subvert the authentication for signature activation.

See letter a) above.

4.3 Signing key deletion

a) **(119 431-1/DEL-6.3.2-01):** Clause SRG_KM.7.1 of EN 419 241 shall apply. If the public key certificate is revoked, the corresponding signing key shall be destroyed.

See letter b) below. Signing keys are Short-term keys, and revocation does not occur.

b) **(419 241-1/SRG_KM.7.1)**: A signing key SHALL be destroyed after the expiration of the public key certificate or if the signing key is useless for the signer.

The signing key is destroyed immediately after signing operations session.

c) **(119 431-1/DEL-6.3.2-02)**: The SSASP shall destroy a signing key when requested by the signer.

Not applicable. See letter a) above.

d) **(419 241-1/SRG_KM.7.2)**: If the link between the signing key and the signer is not maintained after the signing operations session, then the signing key SHALL be destroyed at the end of the signing operations session.

See letter a) above.

e) **(419 241-1/SRG_KM.7.3)**: Signing key destruction mechanism and procedure SHOULD ensure that all backups of the destroyed signing key are also destroyed and that no residual information can be used to reconstruct the signing key.

Signing keys are destroyed by securely deleting them from the SCDev immediately after signing and are never backed-up nor replicated.

4.4 Signing key backup and recovery

a) **(419 241-1/SRG_KM.2.1)**: All private or secret keys (including signer's signing key, Infrastructure and Control Keys) SHALL be securely stored, i.e. never be stored in an unprotected state.

All private and secret keys are always protected by mechanisms provided by QSCD or HSM.

Subjects/Signers private signing keys are generated and used within a QSCD and are destroyed immediately after use and is never backed-up nor replicated.

Protection of key material is according to [9] 4.5 letter a).

b) **(419 241-1/SRG_KM.2.2)**: If any private or secret key (including signer's signing key, Infrastructure and Control Keys), is exported from that SCDev, it SHALL be protected to ensure its confidentiality and integrity to the same or higher security level as within the SCDev. Wherever the private/secret key is protected by encryption, only cryptographic algorithms and algorithm parameters of equivalent or higher strength SHALL be used.

Subjects/Signers private signing keys are destroyed immediately after signing and is never backed-up nor replicated.

Whenever a private or secret key (infrastructure- or control key) exists outside the QSCD/HSM, it is protected by mechanisms provided by the QSCD/HSMs.

c) **(419 241-1/SRG_KM.2.3):** TW4S SHALL ensure that backup, storage and restoration of private or secret keys (including signer's signing key, Infrastructure and Control Keys) are only performed by authorized personnel. Master keys used to protect both user and working keys SHALL be backed up, stored and reloaded under at least dual control. Such master keys SHALL only be held outside the SCDev in protected form.

Signing keys are destroyed immediately after signing and is never backed-up nor replicated.

Backup, storage and restoration of infrastructure and control keys as well as Master keys are only performed under dual control by authorized personnel.

Master keys held outside QSCD/HSMs are protected with mechanisms providing a security level equal to QSCD/HSM.

d) **(119 431-1/GEN-6.3.3-04)**: The number of duplicated datasets shall not exceed the minimum needed to ensure continuity of the service.

Signing keys are destroyed immediately after signing and is never backed-up nor replicated.

BankID BankAxept AS have processes in place ensuring redundancy of the service. The number of duplicated datasets is aligned with service continuity needs.

5 Facility, management, and operational controls

5.1 General

a) **(119 431-1/OVR-6.4.1-01)**: The requirements identified in ETSI EN 319 401 [1], clauses 5, 6.3 and 7.3, shall apply.

See [9] chapter 2, 3.3 and 4.3 respectively.

5.2 Physical security controls

a) **(119 431-1/OVR-6.4.2-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.6 shall apply.

See [9] chapter 4.6

b) **(119 431/OVR-6.4.2-02)**: The requirements identified in ETSI EN 319 411-1 [2], clause OVR-6.4.2-02 to OVR-6.4.2-10 shall apply mutatis mutandis to signing key generation and activation management services.
(Mutatis mutandis, the same rules can be applied to this similar case.)

The same practices as described in [9] chapter 4.6.1 sub-heading “Certificate Services” letters a) through j) is applied.

5.3 Procedural controls

a) **(119 431-1/OVR-6.4.3-01)**: The requirements REQ-7.4-04 to REQ-7.4-09 in ETSI EN 319 401 [1] shall apply.

See [9] chapter 4.4 letters b) through g)

5.4 Personnel controls

a) **(119 431-1/OVR-6.4.4-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.2 shall apply.

See [9] chapter 4.2

5.5 Audit logging procedures

For description on BankID BankAxept AS practices related to e-Signature Service audit logging procedures, please see [9] chapter 4.10.1 sub-heading “e-Signature Service” letters m) through w)

5.6 Records archival

a) **(119 431-1/OVR-6.4.6-01)**: The SSASP shall retain the audit data records for at least seven years after any certificate based on these records ceases to be valid and within the constraint of applicable legislation.

Records of the central audit log repository are kept for 7 years.

5.7 Key changeover

No policy requirement.

5.8 Compromise and disaster recovery

a) **(119 431-1/OVR-6.4.8-01)**: The requirements identified in ETSI EN 319 401 [1], clauses 7.9 and 7.11 shall apply.

See [9] chapter 4.9 and 4.11.

5.9 SSASP service termination

a) **(119 431-1/OVR-6.4.9-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.12 shall apply.

See [9] chapter 4.12.

6 Technical security controls

6.1 Systems and security management

a) **(419 241-1/SRG_M.1.1)**: TW4S SHALL support roles with different privileges.

See [9] chapter 4.2

b) **(419 241-1/SRG_M.1.2)**: As a minimum the TW4S SHALL support the following roles:
Security Officers: having overall responsibility for administering the implementation of the security policies, practices and have access to security related information.
System Administrators: are authorized to install, configure and maintain the TW4S but with controlled access to security-related information.
System Operators: are responsible for operating the TW4S on a day-to-day basis and are authorized to perform system backup and recovery.
System Auditors: are authorized to view archives and audit logs of the TW4S for the purposes of auditing the operations of the system in line with security policy.
Security officers and system administrators are privileged system users.
System operators and system auditors have privileged roles but are not able to administer or configure the TW4S.

See [9] chapter 4.2 letters m) and n)

c) **(419 241-1/SRG_M.1.3)**: As a minimum the TW4S SHALL support the following non-privileged roles:
Signer: is authorized to use the TW4S by passing the SAD as part of the SAP in order to sign the document or the DTBS/ R, which potentially can be passed through the SAP as well.
SCA: is authorized to send the DTBS/R request to the TW4S in order to be signed by a signer.

RA: is authorized to send the public key certificate to the TW4S in response of a certificate signing request.

The above listed non-privileged roles are supported and implemented as follows:

Signer: this is the natural person who is authenticated by NIdP using existing eID means. The signed identity token provided by the NIdP, together with the DTBS/R provided by the SCASP is used to generate the SAD. The SAD is passed to the SAM along with the DTBS/R.

SCA: this is the component of SCASP which is authorized to request signing operations on behalf of the Signer following successful authentication of the Signer by the NIdP.

RA: BankID BankAxept AS is the RA and performs identity proofing through the use of a NIdP and orders certificates on behalf of the Subject.

d) **(419 241-1/SRG_M.1.4)**: One privileged user SHALL NOT be able to take on all the privileged roles and SHOULD NOT take on more than one of the privileged roles.

BankID BankAxept AS have controls in place to ensure segregation of duties so that no person can assume conflicting roles. See also [9] chapter 4.4.

e) **(419 241-1/SRG_M.1.5)**: Users associated with privileged roles SHALL NOT be associated with non-privileged role.
Users associated with non-privileged roles SHALL NOT be associated with privileged role.

See letter d) above.

f) **(419 241-1/SRG_M.1.6)**: TW4S SHALL be capable of ensuring that a user authorized to assume a Security Officer role is not authorized to assume a System Auditor role.

These roles are mutually exclusive.

See [9] chapter 4.2.

g) **(419 241-1/SRG_M.1.7)**: TW4S SHALL be capable of ensuring that a user authorized to assume a System Administrator role and/ or a System Operator role is not authorized to assume a System Auditor role and/ or a Security Officer role.

These roles are mutually exclusive.

See [9] chapter 4.2.

h) **(419 241-1/SRG_M.1.8)**: Individuals that are part of a group of privileged system users SHALL be named and trained persons.

See [9] chapter 4.2.

i) **(419 241-1/SRG_M.1.9)**: Only privileged system users SHALL have physical access to the hardware and can administer the TW4S..

See [9] chapter 4.6.

j) **(419 241-1/SRG_M.1.10)**: Only privileged system users SHALL have extensive privileges to administer the TW4S through all relevant applications and interfaces.

Only personnel in trusted roles authorized to administer the TW4S can administer the TW4S through all relevant applications and interfaces.

6.2 Systems and operations

a) **(419 241-1/SRG_SO.1.1)**: TW4S manufacturers SHALL ensure instructions are provided to allow the TW4S to be:
- correctly and securely operated;
- deployed in such a way that the risk of systems failure is minimized;
- protected against viruses and malicious software to ensure the integrity of the systems and the information they process.

TW4S manufacturer have provided instructions detailing deployment and operational processes.

b) **(419 241-1/SRG_SO.1.2):** TW4S manufacturers SHALL provide system documentation covering the responsibilities of the four privileged roles mentioned in SRG_M.1.2. It SHOULD include:
- Installation Guidance;
- Administration Guidance;
- User Guidance.

TW4S manufacturer have provided documentation on all the above listed topics.

c) **(419 241-1/SRG_SO.2.1)**: TW4S manufacturers SHALL state the time accuracy of TW4S and how this is ensured.

BankID BankAxept AS uses a time source that is synchronized at least once a day. The accuracy of the time is with deviation up to 1 second from UTC. Time source is synchronized using NTP.

d) **(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.

See letter c) above

e) **(419 241-1/SRG_SO.2.3)**: In order to check whether a certificate has expired, a time source suitably synchronized with the UTC SHALL be used.

See letter c) above

6.3 Computer security controls

a) **(119 431-1/OVR-6.5.3-01)**: The requirements REQ-7.4-01, REQ-7.4-02, REQ-7.4-03 and REQ-7.4-10 in ETSI EN 319 401 [1] shall apply.

See [9] chapter 4.4.

b) **(419 241-1/SRG_AA.6.1)**: TW4S SHALL generate a warning notifying in a timely manner unusual events which can have impact on the ability of the signing server system to meet the security requirements identified in this standard.
A mechanism that issues a warning whenever an unusual event is detected SHOULD be implemented. The warning SHOULD trigger a notification to relevant administrator personnel. A warning MAY also trigger further actions to react to possible attacks such as cutting off the path of potential attack.
Examples of unusual events related to user activities can be (but not limited to):
- User actions outside of standard usage hours.
- User actions executed with an abnormal speed (in order to detect non-human interventions).
- User actions skipping standard activities within defined processes.
- Duplicated user sessions.

Application monitoring is in place for all TW4S components.

An alert system is established and will be continuously improved as more experience is gathered about threats and attack patterns.

6.4 Life cycle security controls

a) **(119 431-1/OVR-6.5.4-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.7 shall apply for all service components.

See [9] chapter 4.7.

6.5 Network security controls

a) **(119 431-1/OVR-6.5.5-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.8 shall apply.

See [9] chapter 4.8.

7 Compliance audit and other assessment

NOTE: See ETSI EN 319 403 [i.3].

See [9] chapter 4.13

8 Other business and legal matters

8.1 Fees

These policy requirements are not meant to imply any restrictions on charging for TSP's services.

No stipulation

8.2 Financial responsibility

NOTE: Financial responsibility is covered in clause 6.8.1 of the present document by OVR-6.8.1-01.

See [9] chapter 4.1.1 letters d) and e)

8.3 Confidentiality of business information

No policy requirement.

BankID BankAxept AS will provide logical separation of uploaded documents that may contain relying party business information.

8.4 Privacy of personal information

a) **(119 431-1/OVR-6.7.4-01)**: The requirement REQ 7.13-05 identified in ETSI EN 319 401 [1] shall apply.

See [9] chapter 4.13 letter e)

8.5 Intellectual property rights

No policy requirement.

No stipulation

8.6 Representations and warranties

a) **(119 431/OVR-6.7.6-01)**: The requirements REQ-6.3-05 and REQ-6.3-06 identified in ETSI EN 319 401 [1] shall apply.

See [9] chapter 3.3 letters e) and f)

8.7 Disclaimers of warranties

See clause 6.7.6.

See chapter 8.6 letter a)

8.8 Limitations of liability

Limitations on liability are covered in the terms and conditions as per clause 6.8.4.

See [9] chapter 3.2 letter b).

8.9 Indemnities

No policy requirement.

See [9] chapter 3.2 letter b).

8.10 Term and termination

No policy requirement.

No stipulation.

8.11 Individual notices and communications with participants

No policy requirement.

See [9] chapter 3.1 letter i).

8.12 Amendments

No policy requirement.

See [9] chapter 3.1 letter i).

8.13 Dispute resolution procedures

NOTE: Dispute resolution procedures is covered in clause 6.8.1 and 6.8.1 of the present document by OVR-6.8.1-01 and OVR-6.8.4-04.

See [9] chapter 4.1.1 letter f).

8.14 Governing law

Not in the scope of the present document.

Governing law is Norwegian laws

8.15 Compliance with applicable law

a) **(119 431-1/OVR-6.7.15-01)**: The requirements REQ-7.13-01 and REQ-7.13-02 identified in ETSI EN 319 401 [1] shall apply.

See [9] chapter 4.13 letters a) and b)

8.16 Miscellaneous provisions

No policy requirement.

No stipulation

9 Other provisions

9.1 Organizational

a) **(119 431-1/OVR-6.8.1-01)**: The requirements identified in ETSI EN 319 401 [1], clause 7.1 shall apply.

See [9] chapter 4.1.

9.2 Additional testing

No policy requirement.

No stipulation.

9.3 Disabilities

a) **(119 431-1/OVR-6.8.3-01)**: The requirements REQ-7.13-03 and REQ-7.13-04 identified in ETSI EN 319 401 [1] shall apply.

See [9] chapter 4.13 letters c) and d).

9.4 Terms and conditions

a) **(119 431-1/OVR-6.8.4-01)**: The requirements identified in ETSI EN 319 401 [1], clause 6.2 shall apply.

See [9] chapter 3.2.

10 Framework for definition of server signing application service component policy built on the present document.

a) **(119 431-1/OVR-7-01)** [CONDITIONAL]: When building a SCP from requirements defined in the present document, the policy shall incorporate, or further constrain, all the requirements identified in clauses 5 to 6.

Not applicable.