Stø AS Qualified Time-stamping Services Practice Statement

Version 1.2.1 Last updated 11. November 2025.

Table of contents

Document history

Version	Date	Changes	Approved by
1.2.1	11.11.2025	Reflecting changes for BTSP for Timestamping	
1.2	24.09.2025	Reflecting name change to Stø	ID Policy Board
1.1.3	9.12.2024	Life time of TSU public key certificates	ID Policy Board
1.1.2	13.11.2024	Removed references to BTSP policy. Clarify that time stamp policy is according to eIDAS and standards	ID Policy Board
1.1.1	30.10.2024	Added text to section 2.2.g) + editorials	As above
1.0	08.05.2024	First approved version	ID Policy Board
0.9	18.04.2024	Temporary version	
0.8	08.04. 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 operation Trust Services compliant with the eIDAS regulation (REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC).The name BankID BankAxept AS is still used in this version of the TSPS. Future versions will incorporate the name change.

1.1 Overview

This document provides a Trust Service Practice Statement (TPS) for the Qualified Time-stamping service provided by BankID BankAxept AS. This document is structured according to and complies with ETSI EN 319 421 [8].

Figure 1 illustrates the interrelationships between the TSU issuing Qualified Time-stamps, the BankID BankAxept certificate generation service and users of BankID BankAxept AS Time-stamping Service described in this document.

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

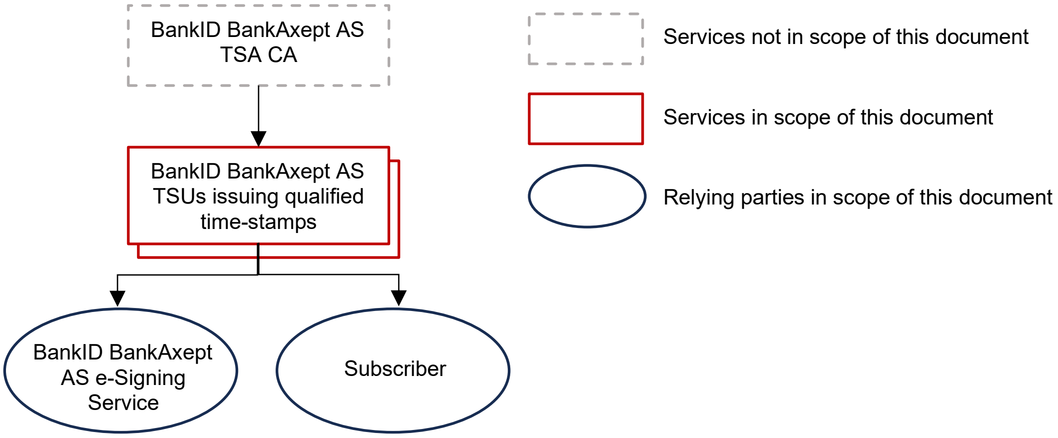

Figure 1 Logical overview of BankID BankAxept AS Qualified Time-stamp infrastructure

1.2 Document name and identification

The identifier of the time-stamp policy referred to in the present document is:

itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1).

By including the object identifier

{itu-t(0) identified-organization(4) etsi(0) id-tst-profile(19422) id-etsi-tsts(1) id-etsi-tsts-EuQCompliance(1)}

in a time-stamp, BankID BankAxept AS claims conformance to the identified time-stamp policy according to Regulation(EU) No910/2014 [i.4] and corresponding standards EN 319 421 [8] and EN 319 422 [5]."

a) **(319 421/ 5.2)**: A TSA shall include the identifier for the time-stamp policy being supported in the TSA disclosure statement made available to subscribers and relying parties to indicate its claim of conformance.

BankID BankAxept AS uses the Best Practice Time Stamp Policy according to:

```
itu-t(0) identified-organization(4) etsi(0)time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)
```

b) **(319 421/5.2)**: When the TSA uses its own identifier for the time-stamp policy, the TSA shall indicate in its policy document and in its TSA disclosure statement, the ETSI time-stamping identifier (i.e. BSTP) being supported.

See letter a) above

1.2.1 Conventions

The structure (headings and subheadings) in this TSPS is organized in accordance with recommendations in [8].

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

1.3.1 Time Stamping Authority

BankID BankAxept AS is the Time Stamping Authority providing the BankID BankAxept AS Qualified Time-stamping Service described in this document.

1.3.2 Subscribers

A subscriber denotes any entity (natural and legal person, system) that contracts with the TSA for the issuance of Qualified Time Stamps.

1.3.3 Relying parties

Relying parties includes any entity (natural and legal person, system) who is recipient of a time-stamp provided by BankID BankAxept Qualified Time-stamping Service and who relies on that time-stamp.

1.3.4 Other participants

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

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 EN 319 401 [4]-and the following apply:

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
Coordinated Universal Time (UTC)	Time scale based on the second as defined in Recommendation ITU-R TF.460-6 [1]
Relying Party	Natural or legal person being the recipient of a time-stamp who relies on that time-stamp
Sub-contractor	An entity (organization, legal or individual person) contracted to carry out tasks as part of a Trust Service Provider's Services.
Subject	Entity (natural person, system, device) identified in a Certificate as the holder of the private key associated with the public key given in the Certificate
Subscriber	The entity (natural or legal person) that is contracted with BankID BankAxept AS for use of the Qualified Time-stamping Service.
Time-stamp	Data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time
Time-stamp Policy	Named set of rules that indicates the applicability of a time-stamp to a particular community and/or class of application with common security requirements
Time-Stamping Authority (TSA)	TSP providing time-stamping services using one or more time-stamping units
Time-stamping Service	Trust service for issuing time-stamps

Time-Stamping Unit (TSU)	Set of hardware and software which is managed as a unit and has a single time-stamp signing key active at a time
Trust Service	Electronic service that enhances trust and confidence in electronic transactions
Trust Service Provider (TSP)	Entity which provides one or more trust services
TSA Disclosure Statement	Set of statements about the policies and practices of a TSA that particularly require emphasis or disclosure to subscribers and relying parties, for example to meet regulatory requirements
TSA Practice Statement	Statement of the practices that a TSA employs in issuing time-stamp
TSA System	Composition of IT products and components organized to support the provision of time-stamping services
UTC(k)	Time scale realized by the laboratory "k" and kept in close agreement with UTC, with the goal to reach ±100 ns

1.5.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 401 [4] and the following apply:

BIPM	Bureau International des Poids et Mesures
CA	Certification Authority
TSA	Time-Stamping Authority
TSP	Trust Service Provider
TSU	Time-Stamping Unit
UTC	Coordinated Universal Time

1.6 References

1.6.1 Normative 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.

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

[1] Recommendation ITU-R TF.460-6 (2002): "Standard-frequency and time-signal emissions".
[2] ISO/IEC 19790:2012: "Information technology -- Security techniques -- Security requirements for cryptographic modules".
[3] ISO/IEC 15408 (parts 1 to 3): "Information security, cybersecurity and privacy protection -- Evaluation criteria for IT security ".
[4] ETSI EN 319 401 (v2.3.1): "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
[5] ETSI EN 319 422 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles".
[6] FIPS PUB 140-2 (2002): "Security Requirements for Cryptographic Modules".
[7] FIPS PUB 140-3 (2019): "Security Requirements for Cryptographic Modules".
[8] ETSI EN 319 421 (v1.1.1): "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps".
[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

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.

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] ETSI EN 319 122-1 (v1.2.1): "Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures".
[i.2] IETF RFC 3161 (2001): "Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP)".
[i.3] IETF RFC 5816: "ESSCertIDV2 update to RFC 3161".
[i.4] 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.5] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[i.6] BIPM Circular T, Available from the BIPM website https://www.bipm.org/.
[i.7] ETSI TS 119 312 (v1.4.1): "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
[i.8] ETSI TS 102 023 (v1.2.2): "Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities"
[i.9] 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.10] ETSI EN 319 411-1 (v1.2.2): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
[i.11] ETSI EN 319 411-2 (v2.2.2): "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".
[i.12] CEN EN 419231:2019: "Protection profile for trustworthy systems supporting time stamping", (produced by CEN).
[i.13] CEN TS 419221-2:2016: "Protection profiles for TSP Cryptographic modules - Part 2: Cryptographic module for CSP signing operations with backup", (produced by CEN).
[i.14] CEN TS 419221-3:2016: "Protection profiles for TSP Cryptographic modules - Part 3: Cryptographic module for CSP key generation services", (produced by CEN).
[i.15] CEN TS 419221-4:2016: "Protection profiles for TSP Cryptographic modules - Part 4: Cryptographic module for CSP signing operations without backup", (produced by CEN).
[i.16] CEN EN 419221-5:2018: "Protection profiles for TSP Cryptographic modules - Part 5: Cryptographic module for trust services", (produced by CEN).
[i.17] ETSI TS 119 612 (v2.2.1): "Electronic Signatures and Infrastructures (ESI); Trusted Lists".

1.7 Notations

Text that is outside text boxes is the applicable policy requirements, see [8]. Requirements is 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 reflects the letter (a), b), c), …) identifying the specific clause in the referred chapter.

2 Policies and practices

2.1 Risk assessment

a) **(319 421/6.1)**: The requirements identified in ETSI EN 319 401 [4], clause 5 shall apply.

See [9] chapter 2

2.2 Trust Service Practice Statement

a) **(319 421/6.2)**: The requirements identified in ETSI EN 319 401 [4], clause 6.1 shall apply.

See [9] chapter 3.1

b) **(319 421/ 6.2)**: In addition, the statement shall at least specify for each time-stamp policy supported by the TSA:
   a) at least one hashing algorithm used to represent the datum being time-stamped;
   b) the accuracy of the time in the time-stamps with respect to UTC;
   c) any limitations on the use of the time-stamping service;
   d) the subscriber's obligations as defined in clause 6.5.2, if any;
   e) the relying party's obligations as defined in clause 6.6;
   f) information on how to verify the time-stamp such that the relying party is considered to "reasonably rely" on the time-stamp (see clause 6.6) and any possible limitations on the validity period; and
   g) any claim to meet the requirements on time-stamping services under national law.

a) The following hashing algorithms are used to represent the datum being time-stamped: SHA-256, SHA-384, SHA-512
b) The accuracy of the time in the time-stamps with respect to UTC is 1 second;
c) Limitations of use of BankID BankAxept AS Time-stamping Service are regulated in contracts with Subscribers.
d) Subscribers' obligations are regulated in Subscriber contract.
e) Relying Party's obligations are defined in terms and conditions.
f) The Relying Party is obligated, when relying on a time-stamp, to:
   1. verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised at the time of the verification;
   2. take into account any limitations on the usage of the time-stamp as described in terms and conditions.
g) Dispute resolution is described in section 7 of Terms & Conditions for the Qualified Signing Service.

c) **(319 421/6.2)**: The TSA should include in its time-stamping disclosure statement availability of its service.

The BankID BankAxept AS time-stamping service are required to have a general availability of at least 99.7% measured over a one-month period.

d) **(319 421/6.2)**: The model TSA disclosure statement given in annex B may be used. Alternatively, this may be provided as part of a subscriber/relying party agreement.

BankID BankAxept AS does not use the template from Annex B.

e) **(319 421/6.2)**: The TSA disclosure statement may be included in a TSA practice statement provided that it is conspicuous to the reader.

BankID BankAxept AS TSA disclosure statement are reflected in Subscriber contracts and terms and conditions.

2.3 *Terms and conditions*

a) **(319 421/ 6.3)**: The general obligations specified in ETSI EN 319 401 [4], clause 6.2 shall apply.

See [9] chapter 3.2.

2.4 *Information security policy*

a) **(319 421/6.4)**: The requirements identified in ETSI EN 319 401 [4], clause 6.3 shall apply.

See [9] chapter 3.3.

2.5 *TSA obligations*

2.5.1 General

a) **(319 421/6.5.1)**: The TSA shall adhere to any additional obligations indicated in the time-stamp either directly or incorporated by reference.

BankID BankAxept AS adheres to obligations indicated in the time-stamp, as described in this document.

2.5.2 TSA obligations towards subscribers

The present document places no specific obligations on the subscriber beyond any TSA specific requirements stated in the TSA's terms and conditions.

2.6 *Information for relying parties*

a) **(319 421/6.6)**: The terms and conditions made available to relying parties (see clause 6.3) shall include an obligation on the relying party, when relying on a time-stamp, to:

1. verify that the time-stamp has been correctly signed and that the private key used to sign the time-stamp has not been compromised until the time of the verification;
2. take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy; and
3. take into account any other precautions prescribed in agreements or elsewhere.

Relying Party obligations mandated in above requirement is reflected in terms and conditions.

3 TSA management and operation

3.1 Internal organization

a) **(319 421/7.2)**: The requirements identified in ETSI EN 319 401 [4], clause 7.1 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.1.

For description on BankID BankAxept AS practices related to TSA internal organization see [9] chapter 4.1.3 sub-heading “Time-stamping Service”, letters d) through f).

3.2 Personnel security

a) **(319 421/7.3)**: The requirements identified in ETSI EN 319 401 [4], clause 7.2 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.2

3.3 Asset management

a) **(319 421/7.4)**: The requirements identified in ETSI EN 319 401 [4], clause 7.3 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.3

3.4 Access control

a) **(319 421/ 7.5)**: The requirements identified in ETSI EN 319 401 [4], clause 7.4 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.4

3.5 Cryptographic controls

3.5.1 General

a) **(319 421/7.6.1)**: The requirements identified in ETSI EN 319 401 [4], clause 7.5 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.5

3.5.2 TSU key generation

For description on BankID BankAxept AS practices related to TSU key generation please see [9] chapter 4.5.1 sub-heading “Time-stamping Service” letters n) through s).

3.5.3 TSU private key protection

For description on BankID BankAxept AS practices related to TSU key generation please see [9] chapter 4.5.1 sub-heading “Time-stamping Service” letters t) through v).

3.5.4 TSU public key certificate

The TSA shall guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements:

a) **(319 421/7.6.4-a))**: TSU signature verification (public) keys shall be made available to relying parties in a public key certificate.

TSU signature verification (public) keys are made available to Relying Parties in a public key Certificate signed by the BankID BankAxept AS TSA CA [10] and returned as part of the technical time-stamping protocol.

b) **(319 421/7.6.4-b))**: The TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-1 [i.10].

The TSU signature verification (public) key Certificate is issued by BankID BankAxept AS TSA CA, see [10].

c) **(319 421/ 7.6.4-c))**: The TSU shall not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.

The TSU does not issue time-stamp before its signature verification (public key) certificate is loaded into the TSU or its cryptographic device.

d) **(319 421/ 7.6.4)**: When obtaining a signature verification (public key) certificate, the TSA should verify that this certificate has been correctly signed (including verification of the certificate chain to a trusted certification authority).

When obtaining a TSU signature verification (public key) certificate, BankID BankAxept AS has processes in place verifying that this certificate has been correctly signed (including verification of the certificate chain to its trusted certification authority).

e) **(319 421/8.1)**: If a time-stamp is claimed to be a qualified electronic time-stamp as per Regulation (EU) No 910/2014 [i.4], the TSU signature verification (public) key certificate should be issued by a certification authority operating under ETSI EN 319 411-2 [i.11] certificate policy.

The time-stamps issued by BankID BankAxept AS's TSU are Qualified electronic time-stamps as per Regulation (EU) No 910/2014 [i.4], and the TSU signature verification (public) key Certificate is issued by BankID BankAxept AS TSA CA operating in accordance with ETSI EN 319 411-2 [i.11] certificate policy, see [10].

f) **(319 421/8.2)**: If a TSU issues time-stamps that are claimed to be qualified electronic time-stamps as per Regulation (EU) No 910/2014 [i.4], this TSU shall not issue non-qualified electronic time-stamps.

BankID BankAxept AS TSU does not issue non-qualified electronic time-stamps.

3.5.5 Rekeying TSU's key

a) **(319 421/ 7.6.5)**: The validity period of TSU's certificate shall not be longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose (see clause 7.6.2c).

The validity period of TSU's certificate is never longer than the period of time that the chosen algorithm and key length is recognized as being fit for purpose, see [9] chapter 4.5.1 sub-heading “Time-stamping Service”, letter p).

3.5.6 Life cycle management of signing cryptographic hardware

For description on BankID BankAxept AS practices related to TSU key generation please see [9] chapter 4.5.1 sub-heading “Time-stamping Service” letters w) through z).

3.5.7 End of TSU key life cycle

a) **(319 421/ 7.6.7)**: The TSA shall define an expiration date for TSU's keys.

BankID BankAxept AS defines expiration dates for TSU's keys.

b) **(319 421/ 7.6.7)**: This date shall not be longer than the end of validity of the associated public key certificate.

The expiration date for TSU's keys is not longer than the end of validity of the associated public key certificate.

c) **(319 421/TIS-7.6.7-03)**: This date should take into account the lifetime defined in 'recommended key sizes versus time' from ETSI TS 119 312 [i.7].

This date takes into account the lifetime defined in 'recommended key sizes versus time' from ETSI TS 119 312 [i.7].

d) **(319 421/ 7.6.7)**: However, in order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's signing key should be reduced.

In order to be able to verify during a sufficient lapse of time the validity of the time-stamps, the validity of the TSU's signing key is reduced. Public key certificates are valid for 6 years. Private key crypto period is reduced to 1 year by using the private key usage period certificate extension.

e) **(319 421/ 7.6.7)**: The expiration date for TSU's keys may be defined when the TSU cryptographic module is initialized or by setting a private key usage period within the TSU's public key certificate.

The expiration date for TSU's keys is defined by setting a private key usage period within the TSU's public key certificate.

f) **(319 421/ 7.6.7)**: The TSU private signing keys shall not be used beyond the end of their validity period.

The TSU private signing keys are not used beyond the end of their validity period.

In particular:

g) **(319 421/ 7.6.7-a)**: Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU's key expires.

BankID BankAxept AS have operational and technical procedures in place to ensure that a new key is generated and certified when a TSU's key expires.

h) **(319 421/ 7.6.7-b)**: The TSU private signing keys, or any key part, including any copies shall be destroyed such that the private keys cannot be retrieved.

After the validity period of the TSU private signing keys expires, the private key is destroyed such that the private keys cannot be retrieved.

3.6 Time-stamping

3.6.1 Time-stamp issuance

a) **(319 421/ 7.7.1)**: Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

Time-stamps conform to the time-stamp profile as defined in ETSI EN 319 422 [5].

The time-stamps shall be issued securely and shall include the correct time.

In particular:

b) **319 421/ 7.7.1-a)**: The time values the TSU uses in the time-stamp shall be traceable to at least one of the real time values distributed by a UTC(k) laboratory.

The time values the TSU uses in the time-stamp are traceable to at least one of the real time values distributed by a UTC(k) laboratory.

c) **(319 421/ 7.7.1-b)**: The time included in the time-stamp shall be synchronized with UTC [1] within the accuracy defined in the policy and, if present, within the accuracy defined in the time-stamp itself.

The time included in the time-stamp is synchronized with UTC as defined in [1] within the accuracy defined in chapter 3.6.2 letter b). The accuracy of the time in the time-stamp is defined in the time-stamp itself.

d) **(319 421/ 7.7.1-c)**: If the time-stamp provider's clock is detected (see clause 7.7.2c)) as being out of the stated accuracy (see clause 7.7.1b)) then time-stamps shall not be issued.

BankID BankAxept AS has automated controls monitoring the accuracy of the time-stamp clock and ensure that in the event that the accuracy is being out of the stated accuracy, see chapter 3.6.2 letter b) then time-stamps will not be issued.

e) **(319 421/ 7.7.1-d)**: The time-stamp shall be signed using a key generated exclusively for this purpose.

The time-stamps are signed using a key generated exclusively for this purpose.

f) **(319 421/ 7.7.1-e)**: The time-stamp generation system shall reject any attempt to issue time-stamps when the end of the validity of the TSU private key has been reached.

The TSU has mechanisms in place rejecting any attempt to issue time-stamps when the end of the usage period of the TSU private key has been reached.

3.6.2 Clock synchronization with UTC

The TSU clock shall be synchronized with UTC [1] within the declared accuracy with at least the following particular requirements:

a) **(319 421/ 7.7.2-a)**: The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.

BankID BankAxept AS has processes in place maintaining the calibration of the TSU clocks such that the clocks do not drift outside the accuracy declared in letter b) below

b) **(319 421/ 7.7.2-b)**: The declared accuracy shall be of 1 second or better.

The accuracy of BankID BankAxept AS TSU clocks is at least 1 second.

c) **(319 421/ 7.7.2-c)**: The TSU clocks shall be protected against threats which could result in an undetected change to the clock that takes it outside its calibration.

The TSU clocks are protected against threats which could result in an undetected change to the clock that takes it outside its calibration, see letter a) above.

d) **(319 421/ 7.7.2-d)**: The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

BankID BankAxept AS has automated mechanisms in place detecting if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

e) **(319 421/ 7.7.2-e)**: If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.

If it is detected that the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU stops time-stamp issuance.

f) **(319 421/ 7.7.2-f)**: The clock synchronization shall be maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second shall occur during the last minute of the day when the leap second is scheduled to occur. A record shall be maintained of the exact time (within the declared accuracy) when this change occurred. See annex C for more details.

The clock synchronization is maintained when a leap second occurs as notified by the appropriate body. The change to take account of the leap second occurs during the last minute of the day when the leap second is scheduled to occur. A record is maintained of the exact time (within the declared accuracy) when this change occurred.

3.7 Physical and environmental security

a) **(319 421/ 7.8)**: The requirements identified in ETSI EN 319 401 [4], clause 7.6 shall apply.

See [9] chapter 4.6.

For description on BankID BankAxept AS practices related to TSA particular requirements related to physical and environmental security please see [9] chapter 4.6.1 sub-heading “Time-stamping Service” letters k) through q)

3.8 Operation security

a) **(319 421/ 7.9)**: The requirements identified in ETSI EN 319 401 [4], clause 7.7 shall apply.

See BankID BankAxept AS TSPS [9] chapter 4.7

In addition, the following particular requirements apply:

System Planning

b) **(319 421/ 7.9-a)**: Capacity demands shall be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

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

3.9 Network security

a) **(319 421/ 7.10)**: The requirements identified in ETSI EN 319 401 [4], clause 7.8 shall apply.

See [9] chapter 4.8.

For description on BankID BankAxept AS practices related to TSA particular Network security requirements, please see [9] chapter 4.8.1 sub-heading “Time-stamping Service” letters a) through c).

3.10 Incident management

a) **(319 421/7.11)**: The requirements identified in ETSI EN 319 401 [4], clause 7.9 shall apply.

See [9] chapter 4.9.

3.11 Collection of evidence

a) **(319 421/7.12)**: The requirements identified in ETSI EN 319 401 [4], clause 7.10 shall apply.

See [9] chapter 4.10.

For description on BankID BankAxept AS practices related to TSA particular requirements related to collection of evidence, please see [9] chapter 4.10.1 sub-heading “Time-stamping Service” letters x) through aa).

3.12 Business continuity management

a) **(319 421/7.13)**: The requirements identified in ETSI EN 319 401 [4], clause 7.11 shall apply.

See [9] chapter 4.11.

For description on BankID BankAxept AS practices related to TSA particular requirements related to business continuity, please see [9] chapter 4.11.1 sub-heading “Time-stamping Service” letters q through t).

3.13 TSA termination and termination plans

a) **(319 421/ 7.14)**: The requirements identified in ETSI EN 319 401 [4], clause 7.12 shall apply

See [9] chapter 4.12.

In addition, the following particular requirements apply:

b) **(319 421/ 7.14-a)**: When the TSA terminates its services, the TSA shall revoke the TSU's certificates.

When BankID BankAxept AS terminates its services, BankID BankAxept AS will revoke the TSU's certificates.

3.14 Compliance

a) **(319 421/ 7.15)**: The requirements identified in ETSI EN 319 401 [4], clause 7.13 shall apply.

See [9] chapter 4.13.