AGENCY FOR DIGITAL GOVERNMENT

Den Danske Stat

TSA Practice Statement

Contents

Changelog 4
References 4
1 Introduction 6
2 Definitions and abbreviations 7
3 General concepts 8
3.1 Time stamping services 8
3.2 Time stamping authority 8
3.3 Subscriber 8
3.4 Time stamping policy and TSA Practice Statement 8
4 Time Stamping Policies 9
4.1 Overview 9
4.2 Identification 9
User Community and Applicability 9
5 Introduction to time-stamping policy and general requirements 10
5.1 General requirement 10
5.2 Identification 10
5.3 Infrastructure and applicability 10
5.3.1 Best practices time-stamp policy 10
6 Policies and implementation 11
6.1 Risk assessment 11
6.2 TSA practice statement 11
6.3 Terms and conditions 13
6.4 Information security policy 14
6.5 TSA obligations 15
6.5.1 General obligations 15
6.5.2 TSA obligations towards subscribers 15
6.6 Information for relying parties 16
7 TSA management and operation 17
7.1 Introduction 17
7.2 Internal organization 17
7.3 Personnel controls 18
7.4 Asset management 20
7.4.1 General requirements 20
7.4.2 Media handling 20
7.5 Access control 20
7.6 Cryptographic controls 21

7.6.1 General controls 21
7.6.2 TSU key generation 21
7.6.3 TSU private key protection 22
7.6.4 TSU certificate 23
7.6.5 Rekeying TSU's key 23
7.6.6 Life cycle management of signing cryptographic hardware 23
7.6.7 Termination of TSU private key 24
7.7 Time-stamping 25
7.7.1 Time-stamp issuance 25
7.7.2 Clock synchronization with UTC 26
7.8 Physical and environmental security 27
7.9 Operation security 28
7.10 Network security 29
7.11 Incident management 31
7.12 Collection of evidence 33
7.13 Business Continuity Plan 34
7.14 TSA termination and termination plans 35
7.15 Compliance 36

Changelog

Date	Version	Change description
30.9.2021	1.0	Initial version
21.2.2023	1.1	Updated with ECDSA with SHA256 as signature algorithm for Time Stamp Tokens.
06.02.2024	1.2	Updated with changes from updated CP's

References

Term	Reference
[TSA Policy]	Public Policy for qualified time-stamping. Digitaliseringsstyrelsen. Version 1.2, August 2023. https://certifikat.gov.dk/politikker-for-tillidstjenester/
[AdES]	AdES Signature Profile, Digitaliseringsstyrelsen, 1.0.6, April, 2022. https://www.ca1.gov.dk/efterlevelseserklaeringer/
[CPS]	Den Danske Stat Trust Services, Certification Practice Statement, Digitaliseringsstyrelsen, Version 1.2 https://www.ca1.gov.dk/efterlevelseserklaeringer/
[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
[ETSI EN 319 421]	ETSI EN 319 421, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, ETSI ESI, Version 1.2.0, January 2023. https://www.etsi.org/standards
[ETSI EN 319 422]	ETSI EN 319 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, ETSI ESI, Version 1.1.1, March 2016. https://www.etsi.org/standards
[Profile]	Certificate Profiles, NemLog-in, Digitaliseringsstyrelsen, Version 1.0.9, August 2022. https://www.ca1.gov.dk/efterlevelseserklaeringer/
[RFC 3161]	Internet X.509 Public Key Infrastructure, Time-Stamp Protocol (TSP), Network Working Group, Request for Comments: 3161, August 2001 https://datatracker.ietf.org/doc/rfc3161/

Term	Reference
[RFC 5816]	ESSCertIDv2 Update for RFC 3161, Internet Engineering Task Force (IETF), Request for Comments: 5816, March 2010 https://datatracker.ietf.org/doc/rfc5816/

1 Introduction

Den Danske Stat's Time Stamping Services issue assertions of proof that an electronic data existed before a particular time. These assertions may be used to support non-repudiation services to establish the existence of data before a specified time. For validation of electronic signatures this can aid to prove the signature was created during the validity period of the certificate, which was used to create the signature.

The Time Stamping services are provided to meet the requirements in [TSA Policy], which again for most of the requirements points to [ETSI EN 319 421]. As the Time Stamp Tokens (TST) issued by the Time Stamp Authority uses recognized and recommend algorithms, the profile [AdES] of the TST meets [RFC 3161] using the modifications as specified in [RFC 5816].

The Time Stamp Tokens are signed by a certificate issued by Den Danske Stat Qualified Root CA.

This document describes the practices used by Den Danske Stat as Qualified Trust Service Provider to implement a Time Stamp Authority that adheres to the danish policy [TSA Policy] for qualified time stamping services.

Den Danske Stat's Time Stamp Authority is part of a Public Key Infrastructure, which also provides a Certification Authority with a remote Signing Service as well as Validation Service.

The Time Stamp Service is used by the Signing Service to create signature formats [ADES], which can be verified even after the expiry of the signing certificate. The service is not available to other services.

Most of the requirements from [TSA Policy] are similar to the general practices used by Den Danske Stat for implementing other qualified trust services. These are described in Den Danske Stat Certification Practice Statement [CPS] and whenever relevant referenced to from this document.

[REQ 1.3.4-01] Qualified trust service providers issuing time stamps under this policy shall publish the policy on their website together with the EU trust label for qualified trust services on a 24/7 basis and without access limitations.

The timestamping policy is accessible via https://ca1.gov.dk. The EU Trust mark will be presented on the same site when the TSP is approved by supervisory body.

2 Definitions and abbreviations

Term	Description
PKI System	See [CPS]
Time Stamp Authority (TSA)	A TSA is a Trusted Third Party that provides a Time Stamp Service. It uses one or more Time Stamp Unit's to produce Time Stamp Tokens
Time Stamp Service (TSS)	A TSS is a specific trusted service that offers Time Stamp Tokens.
Time Stamp Token (TST)	An assertion of proof that an electronic data existed before a particular time.
Time Stamp Unit	A set of software and hardware acting as a unit and using one active time stamp signing key to issue time stamp tokens.

3 General concepts

3.1 Time stamping services

The Time Stamping Services (TSS) consists of an infrastructure which provides Time Stamp Tokens. This is provided by the Den Danske Stat's Time Stamp Authority to the Subscribers – through the Signing Service - and is part of the PKI offered by Den Danske Stat as a qualified trust service provider under the eIDAS regulation [eIDAS].

The TSA uses a reliable time source as well as management of all system components.

3.2 Time stamping authority

As mentioned above Den Danske Stats's Time Stamping Authority (TSA) is responsible for the TSS and has the responsibility for the operation of the Time Stamp Units that issues the actual Time Stamp Tokens.

The user of the TSS trusts the TSA to issue Time Stamp Tokens.

3.3 Subscriber

The Subscriber uses the TSS through the Signing Service. As such, the Subscriber can be a natural person, legal person or a natural person associated to a legal person. In all cases, the Subscriber is notified of its obligations through the Signing Service. For legal persons, a natural person associated with the legal person, will authorize the signature creation, including the request for issue of TST.

3.4 Time stamping policy and TSA Practice Statement

Den Danske Stat TSA Practice Statement, this document, describes how the qualified trust service provider, Den Danske Stat, has met the requirements in the Danish policy for a qualified trust service providing TSS.

4 Time Stamping Policies

4.1 Overview

The Agency for Digitisation has established a trust service provider Den Danske Stat, which provides time stamping services which meets the requirements described in the eIDAS regulation [eIDAS].

The purpose is to provide end users in Denmark with an infrastructure that can provide time stamp services for electronic signatures and electronic seal used within public and private organisations.

The trust service provider Den Danske Stat acts as the legal entity providing time stamp services and bears the responsibility and liability for the services.

The profile of the public key certificates used by the Den Danske Stat in general and for SA are described [Profile]. Note that for high availability, the Den Danske Stat TSA uses two TSUs each with their own certificate and private key. The Time Stamp Tokens issued by Den Danske Stat TSA are described in [AdES].

The accuracy of the TST is 500 ms.

4.2 Identification

This version of the TSA practice can be identified through the OID
1.2.208.169.1.2.2.1.2
iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) practice-statements(2) timestamp(2) major-ver(1) minor-ver(2)

User Community and Applicability

The [TSA Policy] does not pose any limitations on who are eligible to use the TSS. However, as the service is only usable through the Signing Service offered by Den Danske Stat, Subscribers must be eligible to use that service.

The TSS is applicable through the Signing Service to form advanced signature and seal objects as described in [AdES].

5 Introduction to time-stamping policy and general requirements

5.1 General requirement

[REQ 5.1-01] TSAs issuing electronic time-stamps under this policy shall be qualified trust service providers, cf. [eIDAS], and issue time-stamps with an accuracy of 1 second.

Den Danske Stat TSA will only issue electronic timestamps after approval as qualified timestamp authority by the Danish supervisory body.

The Time stamp tokens provided by the TSA has an accuracy of 500 ms.

[REQ 5.1-02] If an accuracy of better than 1 second is provided by the TSA, then the accuracy shall be indicated in the published part of the TSA practice statement and in the issued time-stamps.

See REQ 5.1-01.

5.2 Identification

[REQ 5.2-01] Time-stamps issued under this policy shall include the 'object identifier' value:

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

in the 'policy' field in a time-stamp request, unless the response is an error message, whereby the TSA claims conformance with the BTSP, cf. [ETSI EN 319 421].

Time-stamps issued by the TSUs includes the policy identifier itu-t(0) identified-organization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) best-practices-ts-policy (1)

5.3 Infrastructure and applicability

5.3.1 Best practices time-stamp policy

[REQ 5.3.1-01] This policy is aimed at meeting the requirements of time-stamp for long term validity of electronic signatures (e.g. as defined in [ETSI EN 319 122]) but is generally applicable to any use which has a requirement for security and quality of requested electronic time-stamps where allowed by TSA terms and conditions.

Den Danske Stat TSA is operated by the Agency for Digitalisation only issues timestamps for the signing service which is also provided by the Agency.

[REQ 5.3.1-02] This policy may be used by qualified TSAs which provide time-stamping as an open service and/or to a closed group of subscribers.

See REQ 5.3.1-01.

6 Policies and implementation

6.1 Risk assessment

[REQ 6.1-01] The TSA shall carry out a risk assessment to identify, analyse and evaluate business and technical risks.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-02 for details.

[REQ 6.1-02] The TSA shall implement 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-03 for details.

[REQ 6.1-03] The TSA shall determine and document all security requirements and operational procedures that are necessary to comply with this policy. The documentation must be part of the TSA practice statement, cf. clause 6.2.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-04 for details.

[REQ 6.1-04] The risk assessment shall be reviewed and revised at least once a year.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-05 for details.

[REQ 6.1-05] The TSA's management shall approve the risk assessment and accept the residual risk identified.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-06 for details.

6.2 TSA practice statement

[REQ 6.2-01] The TSA shall prepare a TSA practice statement addressing all requirements of this policy. This TSA practice statement shall include all external organizations supporting the TSA's services and shall conform to this policy. The TSA practice statement may be divided into a public and private part, with the public part of the TSA practice statement being published.

This TSA-practise addresses all TSA requirements; it takes advantage of Den Danske Stat being a qualified trust service provider issuing qualified certificates and as such, many of the requirement in the [TSA Policy] are already handled by the Den Danske Stat CPS [CPS].

This TSA practice statement includes all external organizations supporting the TSA's services namely subcontractor operating and administering the trust service on behalf of Den Danske Stat.

The CPS is a certification practise statement and follows the [RFC 3647] outline and includes all applicable requirements sections in the relevant CP's for all CA-hierarchies in the PKI System.

The CPS is communicated when approved by Den Danske Stat as suitable statements for the implemented CP's. New versions of TSA practice statement and CPS is edited when new trust service policies are published, or implementation is changed. All practise statements are published in English.

[REQ 6.2-01A] When the VA makes use of other parties, including trust service component providers through subcontracting, outsourcing or other third party arrangements, the CA shall maintain the overall responsibility for meeting the requirements of this policy.

See CPS REQ 1.5.4-01A

[REQ 6.2-01B] When the VA makes use of a trust service component provided by another party, the VA shall ensure that the use of the component interface meets the requirements as specified by the provider.

See CPS REQ 1.5.4-01B

[REQ 6.2-01C] When the VA makes use of a trust service component provided by another party, the VA shall ensure the necessary security and functionality required for compliance with this policy.

See CPS REQ 1.5.4-01C**[REQ 6.2-02] The management of the TSA shall be responsible for and approve the overall TSA practice statement and ensure correct implementation, including that the practice statement is conformant with this policy and is communicated to relevant employees and partners.**

Den Danske Stat management approves this practice and ensures correct implementation. After approval the practice statement is communicated to relevant employees and subcontractors.

[REQ 6.2-03] The TSA shall make the public part of the TSA's applicable practice statement available on the TSA's website on a 24/7 basis.

The TSA practice statement is published on https://ca1.gov.dk on a 24/7 basis.

[REQ 6.2-04] The TSA practice statement shall be reviewed and revised on a regular basis and at least once a year. The responsibility for maintaining the TSA practice statement must be determined and documented. Changes in the TSA practice statement must be documented.

This TSA practice statement is reviewed at least once every year. Den Danske Stat's management is responsible for the review. Any change is documented, and historic versions of the practice is archived for at least seven years after they are replaced.

The part of the TSA practise statement relevant for subcontractor is reviewed at least once a year by the subcontractor prior to the regular annual conformity assessment. The process for approval of changes to the documentation is following the Den Danske Stat procedures.

[REQ 6.2-05] In the TSA practice statement, the TSA shall specify provisions upon termination of the service. These must at a minimum include information on who will be notified upon termination and who will take over customers and users, if these types of agreements exist.

In case the Den Danske Stat terminates the TSS a notice will be published on https://ca1.gov.dk least 6 months prior to the service ceases to issue timestamps.

Den Danske Stat do not have or plan to have agreements or contracts with other parties to continue trust service activities in case of a termination.

[REQ 6.2-06] The TSA practice statement shall at least specify

a) the hashing algorithm (or algorithms) used to represent the datum being time-stamped;

b) the accuracy of the time in the time-stamps with respect to UTC;

c) synchronization source or sources;

d) any limitations on the use of the time-stamping service;

e) the subscriber's obligations, if any;

f) the relying party's obligations;

g) 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

h) any claim to meet the requirements on time-stamping services under national or European law. Ad a) The hashing algorithm SHA512 is calculated over the data, and hash value is used as reference to represent the data that is time stamped.

Ad b) The time-stamps has an accuracy of 500 ms.

Ad c) The time is synchronized with the GNSS based reliable time source using antennas located in Denmark and Norway.

Ad d) There are no limitations on the use of TSS.

Ad e) Since the TSS is only used from Den Danske Stat's Signing Service, the subscriber has no additional obligations than those accepted for the issuing of a certificate during the signature session.

Ad f) Obligations for relying parties are available in REQ 6.6-01.

Ad g) Information on good practice on how to verify a time stamp issued by the TSS can be found in REQ 6.6-01.

Ad h) The Qualified Trust Service Provider Den Danske Stat provides the TSS under the regulation [eIDAS].

[REQ 6.2-07] The TSA practice statement should specify information on availability of the TSA's service.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-06 for details.

6.3 Terms and conditions

[REQ 6.3-01] The TSA shall make the terms and conditions regarding its services available to all subscribers and relying parties.

The timestamping service is only used internally by the signing service, thus no need for internal terms and conditions.

[REQ 6.3-02] The terms and conditions shall include:

- **a) a description of the service, including what policies are covered by the service;**
- **b) any limitations on the use of the service;**
- **c) the subscriber's obligations;**
- **d) information for parties relying on the trust service;**
- **e) the period of time during which event logs are retained;**
- **f) limitations of liability;**
- **g) limitations on the use of service, including the TSA's limitation of liability in terms of wrong use of the service;**
- **h) the applicable legal system;**
- **i) dispute procedures;**
- **j) that the TSA is a qualified trust service, cf. the eIDAS Regulation;**

k) the TSA's contact information; and
l) any undertaking regarding availability.

See REQ 6.3-01.

[REQ 6.3-03] 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.

See REQ 6.3-01.

[REQ 6.3-04] Terms and conditions shall be made available through a durable means of communication.

See REQ 6.3-01.

[REQ 6.3-05] Terms and conditions shall be available in a readily understandable language.

See REQ 6.3-01.

[REQ 6.3-06] Terms and conditions may be transmitted electronically.

See REQ 6.3-01.

6.4 Information security policy

[REQ 6.4-01] The TSA shall live up to the requirements in the information security standard ISO 27001 and be able to document compliance through e.g. certification.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-01 for details.

[REQ 6.4-02] The TSA shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-02 for details.

[REQ 6.4-03] Changes to the information security policy shall be communicated to third parties, where applicable. This may include subscribers, conformity assessment body, supervisory body and other authorities.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-03 for details.

[REQ 6.4-04] A TSA's information security policy shall be documented, implemented and maintained, including the security controls and operating procedures for the TSA's facilities, systems and information assets providing the services.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-04 for details.

[REQ 6.4-05] The TSA shall publish and communicate the information security policy to all employees who are impacted by it, including employees at subcontractors performing work for the TSA.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-05 for details.

[REQ 6.4-06] The TSA shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSA's functionality is undertaken by outsourcers.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.2.2-04 for details.

[REQ 6.4-07] The TSA shall set out and ensure efficient implementation of relevant controls at the subcontractors.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-06, 5.3.1-01, 5.3.3-01, 5.3.7-01, 5.8-07, 6.6.2-03, 6.6.2-05 and 9.6.1-01 for requirements on subcontractors.

[REQ 6.4-08] The TSA's information security policy and inventory of assets for information security shall be reviewed at annually and if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-06 for details.

[REQ 6.4-09] Any changes that may impact on the level of security provided shall be approved by the TSA's management.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] 6.6.2-07 for details.

[REQ 6.4-10] The configuration of the TSA's systems shall be checked at fixed intervals and at least once a year for changes which violate the TSA's information security policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-08 for details.

[REQ 6.4-11] The maximum interval between two of the above checks shall be documented in the TSA practice statement.

See REQ 6.4.10.

6.5 TSA obligations

6.5.1 General obligations

[REQ 6.5.1.01] The TSA shall adhere to any additional obligations indicated in the timestamp either directly or incorporated by reference.

The timestamp service is only used internally by the signing service, there are no additional obligations than the accuracy referenced in the time-stamp tokens.

6.5.2 TSA obligations towards subscribers

[REQ 6.5.2-01] The present document places no specific obligations on the subscriber. All TSA specific requirements for the subscriber shall be stated in the TSA's terms and conditions.

This practice statement does not place any obligations on the subscriber, as the timestamp service is only used internally by the signing service.

6.6 Information for relying parties

[REQ 6.6-01] The terms and conditions for relying parties shall at least include the following obligations on the relying party, before a time-stamp is accepted:

- **a) the relying party shall verify that the time-stamp is correctly signed and that the private key used to sign the time-stamp has not been marked as compromised until the time of the verification;**
- **b) the relying party shall take into account any limitations on the usage of the time-stamp indicated by the time-stamp policy; and**
- **c) the relying party shall take into account any other precautions prescribed in agreements or elsewhere.**

Before trusting a timestamp from the Den Danske Stat TSA the timestamp authenticity, integrity and validity of the timestamp shall be checked by the relying party. This includes:

1) That the timestamp was signed correctly using a private key corresponding to the public key in the TSA's certificate.
2) Verify that the TSA certificate is valid.
    a. The TSA certificate is signed by the Den Danske Stat qualified root CA
    b. The TSA is not expired.
    c. The TSA is not revoked.

The validation of a TST may be prolonged beyond the validity of the TSA certificate, if another non-repudiation proof is available, typically another TST, that was created before the expiry of the TSA certificate.

These requirements are listed in the terms and conditions for trusting a timestamp issued by the Den Danske Stat TSA.

7 TSA management and operation

7.1 Introduction

[REQ 7.1-01] The TSA shall have a system or systems for quality and information security management appropriate for the time-stamping services it is providing, cf. REQ 6.4-01.

Den Danske Stat has processes, procedures and infrastructure in place to offer TSS.

7.2 Internal organization

[REQ 7.2-01] The TSA shall be a legal entity.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 1.3.1-02.

[REQ 7.2-02] The TSA organization shall be reliable and non-discriminatory.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9-01 for details.

The subcontractor operates under their company social responsibility policy and CSR framework ensuring trustworthy and non-discriminating conduct.

[REQ 7.2-03] The TSA 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 TSA's terms and conditions.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9-02 for details.

[REQ 7.2-04] The TSA shall maintain sufficient financial resources and/or obtain appropriate liability insurance in accordance with applicable law, including eIDAS, to cover liabilities arising from its operations and/or activities.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9.2.1-01 for details.

[REQ 7.2-05] If the TSA is a private enterprise, the TSA shall obtain and maintain liability insurance, cf. REQ 7.2-04. Such insurance shall as a minimum provide a coverage of DKK 25 million per year.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9.2.1-02 for details.

[REQ 7.2-06] The TSA shall have the financial stability and resources required to operate in conformity with this policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9.2.2-01 for details.

[REQ 7.2-07] The TSA 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9.13-01 for details.

[REQ 7.2-08] The TSA shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] 9.17-01 for details.

[REQ 7.2-09] Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSA's assets.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.1-05 for details.

7.3 Personnel controls

[REQ 7.3-01] The TSA shall ensure that employees and contractors support the trustworthiness of the TSA's operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3-01 for details.

[REQ 7.3-02] The TSA 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.1-01 and 5.3.3-01 for details.

[REQ 7.3-03] The TSA's personnel, including personnel of any subcontractors, 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.3-01 for details.

[REQ 7.3-04] The TSA shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding information security and personal data protection rules as appropriate for the offered services and the job function.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.1-01 for details.

[REQ 7.3-05] The above training requirements should encompass regular (at least every 12 months) updates concerning new threats and current security practices.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.4-01 for details.

[REQ 7.3-06] Appropriate disciplinary sanctions shall be used for personnel who violate the TSA’s policies or procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.6-02 for details.

[REQ 7.3-07] Security roles and responsibilities, as specified in the TSA's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.1-03 for details.

[REQ 7.3-08] Trusted roles, on which the security of the TSA's operation is dependent, shall be clearly identified and approved by the management.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.1-01 for details.

[REQ 7.3-09] Trusted roles shall be approved by the management and accepted by the person to fulfil the role.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.3-02 for details.

[REQ 7.3-10] The TSA'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, the sensitivity of data that can be accessed, background screening and employee training and awareness.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.3-03 for details.

[REQ 7.3-11] Where appropriate, job descriptions shall differentiate between general functions and the TSA's specific functions. These should include skills and experience requirements.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.3-04 for details.

[REQ 7.3-12] Personnel shall exercise administrative and management procedures and processes that are in line with the TSA's information security management procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.6-01 for details.

[REQ 7.3-13] Managerial personnel shall have experience or training in relation to operation of the TSA, knowledge of compliance controls for personnel with security responsibility and experience with information security and risk assessment that is sufficient to be able to perform management functions for the TSA.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.3.1-02 for details.

[REQ 7.3-14] All TSA's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSA's operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.1-03 for details.

[REQ 7.3-15] 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 TSA's critical systems for service management, including system restoration.**

c) **System Operators: Responsible for operating the TSA's critical systems on a day-to-day basis. Authorized to perform system backup.**
d) **System Auditors: Authorized to view archives and audit logs of the TSA's critical systems.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.1-04 for details.

[REQ 7.3-16] Personnel that are to access or configure privileges for trusted roles shall be for-mally approved by a security manager at the senior management level.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.3-01 for details.

7.4 Asset management

7.4.1 General requirements

[REQ 7.4.1-01] The TSA shall maintain an inventory of its assets, including information assets. All information assets shall be classified according to the TSA's risk assessment, and the TSA shall ensure adequate protection of all assets.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.2-06 for details.

7.4.2 Media handling

[REQ 7.4.2-01] All media in the TSA’s operating system shall be handled securely in accordance with its classification, and

- **media containing sensitive data shall be securely disposed of when no longer required;**
- **media shall be protected from damage, theft, unauthorized access and obsolescence; and**
- **sensitive data shall be protected against unauthorized access through re-used storage objects.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.6-02 and 5.1.7-01 for details.

7.5 Access control

[REQ 7.5-01] The TSA shall implement effective access control that protects against unauthorized physical or logical access to the TSA's systems. In particular: see req 7.5-02 to 7.5-09

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-08 for details.

[REQ 7.5-02] The TSA shall implement controls (e.g. firewalls) to protect the TSA's internal network from unauthorized access, including access by subscribers and relying parties.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-13 for details.

[REQ 7.5-03] Firewalls shall also be configured to prevent all protocols and accesses not required for the operation of the TSA.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7.13 for details.

[REQ 7.5-04] The TSA shall implement an efficient user administration, including administer user access of operators, administrators and system auditors applying the principle of "least privileges".

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-01 for details.

[REQ 7.5-05] User accounts shall be checked regularly to ensure that the users at all times only have the necessary rights, cf. access control policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-02 for details.

[REQ 7.5-06] Access to information and application system functions shall be restricted in accordance with the access control policy.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-03 for details.

[REQ 7.5-07] The TSA's operating systems shall provide sufficient computer security controls for the separation of trusted roles identified in the TSA practice statement, including the separation of security administration and operational roles. Particularly, use of system utility programs shall be restricted and controlled to what is necessary.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] 6.5.1-01 for details.

[REQ 7.5-08] The TSA's personnel shall be identified and authenticated before using critical systems and applications.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-04 for details.

[REQ 7.5-09] The TSA's personnel shall be accountable for their activities., e.g. through efficient event logging.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-05 for details.

7.6 Cryptographic controls

7.6.1 General controls

[REQ 7.6.1-01] The TSA shall implement secure handling of cryptographic keys and cryptographic devices. The handling shall cover the full lifecycle of keys and devices.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.1.1-02 for details.

7.6.2 TSU key generation

[REQ 7.6.2-01] a) The generation of the TSU's private signing keys shall be undertaken in a physically secured environment (as per clause 7.8) by personnel in trusted roles (as per clause 7.3) under dual control. The personnel authorized to carry out this function shall be limited to those required to do so under the TSA's practice statement.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.1.1-05 for details.

[REQ 7.6.2-02] The generation of the TSU's private signing key shall be carried out with-in a cryptographic module which either:

i) is a trustworthy system which is assured to EAL 4 or higher in ac-cordance with [ISO/IEC 15408] or equivalent national or interna-tionally recognized IT security evaluation criteria. This shall be to a security target or protection profile which meets the require-ments of the present document, based on a risk analysis and tak-ing into account physical and other non-technical security measures; or

ii) meets the requirements of [ISO/IEC 19790], [FIPS PUB 140-2] level 3 or [FIPS 140-3] level 3.

The cryptographic device should be as specified in i) above. This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.2.1-01 and REQ 6.2.2-02 for details.

[REQ 7.6.2-03] The TSU key generation algorithm, the signing key length and signature algorithm used for signing time-stamps shall be as specified in [ETSI TS 119 312]. The recommendation for choice of cryptographic algorithms and key lengths defined in [ETSI TS 119 312] may be superseded by national recommendations.

The Time Stamp Unit provides time stamp tokens, which are signed using ECDSA using SHA256 as hash algorithm.

[REQ 7.6.2-04] A TSU's signing key should not be imported into different cryptographic modules.

The TSA uses two TSU's each with their own dedicated cryptographic module and TSU signing key.

[REQ 7.6.2-05] If the same signing key is used in different cryptographic modules, the key shall be associated with the same public key certificate into all the different cryptographic modules.

N/A. See REQ 7.6.2-04.

[REQ 7.6.2-06] A TSU shall have a single private time-stamp signing key active at a time.

The TSU's have been configured with one active private time-stamp signing key.

7.6.3 TSU private key protection

[REQ 7.6.3-01] The TSU private keys shall remain confidential and their integrity shall be maintained. In particular: see req 7.6.3-02 to 7.6.3-04

See 7.6.3-02 to 7.6.3-04

[REQ 7.6.3-02] The TSU private signing key shall be held and used within a cryptographic module which:

i) is a trustworthy system which is assured to EAL 4 or higher in ac-cordance with [ISO/IEC 15408] or equivalent national or interna-tionally recognized IT security evaluation criteria. This shall be to a security target or protection profile which meets the require-ments of the present document, based on a risk analysis and tak-ing into account physical and other non-technical security measures; or

ii) meets the requirements of [ISO/IEC 19790], [FIPS PUB 140-2] level 3 or [FIPS PUB 140-3] level 3.

The cryptographic device should be as specified in i).

See REQ 7.6.2-02.

[REQ 7.6.3-03] 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 this function shall be limited to those required to do so under the TSA's practice statement.

N/A. The TSUs private keys are not backed up. In case of a disaster recovery, new TSUs private keys are generated.

[REQ 7.6.3-04] c) Any backup copies of the TSU private keys shall at all times be protected to at least the same level as the cryptographic module on which the key is generated and used to ensure its integrity and confidentiality.

N/A. See REQ 7.6.3-03.

7.6.4 TSU certificate

[REQ 7.6.4-01] The TSA shall guarantee the integrity and authenticity of the TSU signature verification (public) keys with at least the following particular requirements: see req 7.6.4-02 to 7.6.4-04

See REQ 7.6.4-02 to 7.6.4-04

[REQ 7.6.4-02] TSU signature verification (public) keys shall be made available to relying parties in a certificate.

The public time stamp verification keys are available at https://ca1.gov.dk

[REQ 7.6.4-03] The TSU certificate shall be issued by a qualified CA operating under [ETSI EN 319 411-1] and [ETSI EN 319 411-2].

The certificates for the Time Stamp Units are issued by Den Danske Stat Qualified Trust Service Provider operated by Den Danske Stat. See [Profile], section 13 for certificate profile for TSUs.

[REQ 7.6.4-04] The TSU shall not issue time-stamp before its certificate is loaded into the TSU or its cryptographic device.

The TSU is only available for issuing time stamp token after a key signing ceremony, which includes that the TSU shall receive a certificate.

[REQ 7.6.4-05] When obtaining a TSU certificate, the TSA should verify that this certificate has been correctly signed by the CA (including verification of the certificate chain to a recognised qualified CA).

The TSUs certificates are issued during the initialization of the complete PKI System, which ensures that TSUs certificates are signed by the Den Danske Stat qualified root CA.

7.6.5 Rekeying TSU's key

[REQ 7.6.5-01] The validity period of the TSU's certificate must 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 of the TSU's certificates is 20 Years covering an ECC key on secp256r1. See 7.6.2-03 for details on algorithm.

7.6.6 Life cycle management of signing cryptographic hardware

[REQ 7.6.6-01] Cryptographic hardware used in connection with time-stamping shall be protected throughout its life cycle. AS a minimum, the following requirements must be met: see req 7.6.6-02 to 7.6.6-05

See REQ 7.6.6-02 to 7.6.6-05

[REQ 7.6.6-02] a) Cryptographic hardware shall not be tampered with during shipment.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.2.7-02 for details.

[REQ 7.6.6-03] b) Cryptographic hardware shall not be tampered with shall not be tampered with when and while stored.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.2.7-03 for details.

[REQ 7.6.6-04] c) Installation, activation and duplication of the 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).

All handling of TSU is performed by trusted roles under dual control in highly secured facilities.

[REQ 7.6.6-05] d) TSU signing keys stored on TSU cryptographic hardware shall be erased in such a way that it is practically impossible to recover them when the cryptographic hardware is no longer to be used for signing using TSU signing keys.

The TSU signing key is stored within a cryptographic module. The module is FIPS 140-2 level 3 certified and uses a secure key deletion algorithm, which prevents the key to be used after deletion.

7.6.7 Termination of TSU private key

[REQ 7.6.7-01] The TSA shall define an expiration date for TSU's signing keys.

The TSUs private keys are replaced before the expiry of the TSUs certificates.

[REQ 7.6.7-02] The expiration date for TSU’s signing key shall not be longer than the end of validity of the associated certificate.

See REQ 7.6.7-01

[REQ 7.6.7-03] The expiration date should take into account the lifetime defined in 'recommended key sizes versus time' from ETSI [ETSI TS 119 312].

See REQ 7.6.1-03 for details

[REQ 7.6.7-04] 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 shorter than the certificate validity.

The TSU private keys are updated before the certificate expires.

[REQ 7.6.7-05] The expiration date for the TSU signing keys may be defined when the TSU cryptographic module is initialized or by setting a 'privateKeyUsagePeriod' extension within the TSU's certificate.

The expiry of TSU private keys are before the expiry of the corresponding certificate. The extension privateKeyUsagePeriod is not used.

[REQ 7.6.7-06] The TSU signing keys shall not be used beyond the end of their validity period.

In particular: see req 7.6.7-07 and 7.6.7-08

See REQ 7.6.6-07 and REQ 7.6.7-08

[REQ 7.6.7-07] a) Operational or technical procedures shall be in place to ensure that a new key is put in place when a TSU signing key expires.

A scheme has been configured to schedule notifications starting 90 days before expiry with a fixed deadline.

[REQ 7.6.7-08] b) The TSU signing keys, or any key part, including any copies, shall be destroyed such that the keys cannot be retrieved.

As part of key update, expired keys are deleted.

7.7 Time-stamping

7.7.1 Time-stamp issuance

[REQ 7.7.1-01] Time-stamps shall conform to the time-stamp profile as defined in ETSI EN 319 422.

The time stamp tokens are specified in [AdES], section 4, which meets the requirements specified in [ETSI EN 419 422], section 6.2 and 9.1.

[REQ 7.7.1-02] In particular, time-stamps shall be marked as qualified time-stamps by including one qcStatements extension with the value ""esi4-qtstStatement-1"", cf. [ETSI EN 319 422] clause 9.1.

See REQ 7.7.1-01

[REQ 7.7.1-03] The time-stamps shall be issued securely and shall include the correct time. In particular: see req 7.7.1-04 to 7.7.1-08

The TSU's use local computer time source when issuing tokens. The local time source is synchronized with a reliable GNSS based time source via NTP. NTP serves the UTC timescale by definition.

The TSU's thereby derive an accurate time directly from the atomic clocks aboard the GNSS satellites. To maintain reliable time synchronisation the back-end synchronisation server performs a time cross-check of GNSS against at least two other time servers.

[REQ 7.7.1-04] 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 GNSS based reliable time source uses UTC (k) lab. UTC (USNO)

[REQ 7.7.1-05] The time included in the time-stamp shall be synchronized with UTC within the accuracy defined in this policy and, if present, within the accuracy defined in the time-stamp itself.

The time-stamp tokens have an accuracy of 500 ms.

[REQ 7.7.1-06] If the TSA's clock is detected (see REQ 7.7.2-04) as being out of the stated accuracy (see clause 7.7.1-04) then time-stamps shall not be issued.

The accuracy of the calibration is periodically monitored. A time-stamp token will not be issued unless the monitoring reported the time to be synchronized and the report was made within the configured interval of 1 second or better.

[REQ 7.7.1-07] The time-stamp shall be signed using a key generated exclusively for this purpose.

TSUs private key are only used for signing time stamp tokens.

[REQ 7.7.1-08] The time-stamp generation system shall reject any attempt to issue time-stamps if the TSU's signing key has expired.

Expired TSU private keys are deleted and can't be used to issue time stamp tokens.

[REQ 7.7.1-09] TSUs issuing qualified time-stamps, cf. [eIDAS] under this policy, must not issue non-qualified time-stamps.

The TSA only provides qualified time stamp tokens.

[REQ 7.7.1-10] TSAs issuing qualified time-stamps, cf. [eIDAS], under this policy from a TSU while also issuing non-qualified time-stamps from other TSUs shall use another subject name (subject distinguishedName) in certificates for TSUs issuing non-qualified time-stamps than in the certificate for the TSU issuing qualified time-stamps under this policy.

N/A. See REQ 7.7.1-09

[REQ 7.7.1-11] The above non-qualified TSUs shall be accessed via other service interfaces for TSUs operating under this policy.

N/A. See REQ 7.7.1-09.

7.7.2 Clock synchronization with UTC

[REQ 7.7.2-01] The TSU clock shall be synchronized with UTC as defined in Recommendation ITU-R TF.460-6 within the declared accuracy with at least the following particular requirements:

See REQ 7.7.1-06.

[REQ 7.7.2-02] a) The calibration of the TSU clocks shall be maintained such that the clocks do not drift outside the declared accuracy.

See REQ 7.7.1-06.

[REQ 7.7.2-03] b) The declared accuracy shall be of 1 second or better.

See REQ 7.7.1-06.

[REQ 7.7.2-04] 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 underlying time source is protected against known threats such as DoS. To maintain reliable time synchronization the back-end synchronization server performs a time cross-check of GNSS against at least two other time servers.

[REQ 7.7.2-05] d) The TSA shall detect if the time that would be indicated in a time-stamp drifts or jumps out of synchronization with UTC.

TSA logs whether the time was considered in sync or not when processing a request. A time-stamp token will not be issued unless the monitoring reported the time to be synchronized.

[REQ 7.7.2-06] e) If it is detected that the time indicated in a time-stamp drifts or jumps out of synchronization with UTC, the TSU shall stop time-stamp issuance.

See REQ 7.7.2-05.

[REQ 7.7.2-07] 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.

The Time Stamp Server is continuously monitored for time synchronisation and will automatically update the time whenever a leap second occurs. Whenever this happens, an entry is record in the audit log.

7.8 Physical and environmental security

[REQ 7.8-01] The TSA shall control physical access to components of the TSA's systems based on the classification policy. This includes minimizing risks related to physical security.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1-01 for details.

[REQ 7.8-02] The TSA shall ensure that access to facilities is limited to authorized individuals.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.1-02 for details.

[REQ 7.8-03] The TSA shall implement effective protection against

- **loss, damage or compromise of assets and interruption to business activities; and**
- **compromise or theft of information and information processing facilities.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1-02 for details.

[REQ 7.8-04] Components that are critical for the secure operation of the TSA 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.

The following must be observed: see req 7.8-05 to 7.8.10

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-02 for details.

a) [REQ 7.8-05] Access controls shall be applied to the cryptographic module to meet the requirements of security of cryptographic modules as identified in clause 7.6.

b) The following additional controls apply to time-stamping management: see req 7.8-06 to 7.8-10

a) Access control is implemented in support of REQ 7.6.

b) See REQ 7.8-06 - 7.8-10

[REQ 7.8-06] 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-04 for details.

[REQ 7.8-07] 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-11 for details.

[REQ 7.8-08] 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-03 for details.

[REQ 7.8-09] 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. Recovery plans shall be in place following operational disasters (disaster recovery).

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1-03 and 5.1-04 for details.

[REQ 7.8-10] Controls shall protect against equipment, information, media and software relating to the time-stamping services being taken off-site without authorization.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1-05 for details.

[REQ 7.8-11] Other functions may be supported within the same secured area provided that the access is limited to authorized personnel.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.2-07 for details.

7.9 Operation security

[REQ 7.9-01] The TSA shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.2.1-01 for details.

[REQ 7.9-02] The TSA shall ensure that, prior to any system development (e.g. undertaken by the TSA or on behalf of the TSA), a plan approved by management is provided to ensure that security is built into the systems. The plan shall include an analysis of security requirements being met in order to maintain an adequate level of security.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.1-02 for details.

[REQ 7.9-03] The TSA shall implement documented processes for release and change management of software, hardware and configuration changes. The TSA shall have documented processes for security update of proprietary and standard software and firmware. The processes shall include documentation of the changes.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.5.1-02 for details.

[REQ 7.9-04] The integrity of TSA's systems and information shall be protected against viruses, malicious and unauthorized software, and the TSA shall specify and apply procedures for ensuring that:

- **security patches are applied within a reasonable time after they come available;**
- **security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and**
- **the reasons for not applying any security patches are documented.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.5.1-03 for details.

[REQ 7.9-05] Media used within the TSA's systems shall be securely handled according to the classification and to protect media from damage, theft, unauthorized access and obsolescence.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.6-01 for details.

[REQ 7.9-06] The TSA shall have media management procedures in place to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.6-02 for details.

[REQ 7.9-07] The TSA shall establish and implement procedures for all trusted and administrative roles that may impact on the TSA's security and operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.2.1-02 for details.

[REQ 7.9-08] The TSA shall plan and monitor future capacity requirements made to ensure that adequate processing power and storage are available at all times.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.6.3-06 for details.

7.10 Network security

[REQ 7.10-01] The TSA shall protect its network and systems from attack and unauthorized access.

In particular: see req 7.10.-02 to 7.10.17

See 7.10-02 to 7.10-17

[REQ 7.10-02] The TSA shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between critical systems and services.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.1.1-03 for details.

[REQ 7.10-03] The TSA shall apply the same security controls to all systems co-located in the same zone.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-07 for details.

[REQ 7.10-04] The TSA shall restrict access and communications between zones to those necessary for the operation of the TSA.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-13 for details.

[REQ 7.10-05] The TSA shall explicitly forbid or deactivate not needed connections and services.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7.13 for details.

[REQ 7.10-06] The TSA shall also configure all TSU systems by removing or disabling all accounts, applications, services, and ports that are not used in the TSU's operations.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-04 for details.

[REQ 7.10-07] The TSA shall review the established network and firewall rules set on a regular basis.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-15 for details.

[REQ 7.10-08] The TSA shall operate, maintain and protect all TSU systems in secure zones or high-security zones.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-03 for details.

[REQ 7.10-09] The TSA shall place particularly critical systems in high-security zones.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-08 for details.

[REQ 7.10-10] The TSA shall separate dedicated networks for administration of IT systems and the TSA's operational network.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-10 for details.

[REQ 7.10-11] The TSA shall not use systems used for administration of the security policy implementation for other purposes.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-11 for details.

[REQ 7.10-12] The TSA shall separate the production systems from systems used in development and testing.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-12 for details.

[REQ 7.10-13] The TSA shall establish communication between critical systems only through trusted channels that are physically or logically distinct from other communication channels and provide confidentiality, integrity and authenticity between the systems.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7.14 for details.

[REQ 7.10-14] If a high level of availability of external access to the trust service is required, the external network connection shall be redundant.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-16 for details.

[REQ 7.10-15] At least once every quarter the TSA shall perform a vulnerability scan from external and internal IP addresses. The vulnerability scans shall be performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report. Scans shall be documented.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-17 for details.

[REQ 7.10-16] At least once a year, after set up and in case of significant infrastructure or application upgrades or modifications the TSA shall perform a penetration test. The penetration test shall be performed by a person or entity with the skills, tools, code of ethics and independence necessary to provide a reliable report. The penetration test shall be documented.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-18 for details.

[REQ 7.10-17] The TSA shall ensure that only trusted roles are granted access to secure zones and high-security zones.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.7-09 for details.

7.11 Incident management

[REQ 7.11-01] System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored.

In particular: see req 7.11-02 to 7.11.12

See REQ 7.11-02 to 7.11-12

[REQ 7.11-02] Monitoring activities must take account of the sensitivity of any information collected or analysed.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-02 for details.

[REQ 7.11-03] Abnormal system activities that indicate a potential security violation, including intrusion into the TSA's network, shall be detected and reported as alarms.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-03 for details.

[REQ 7.11-04] The TSA shall monitor the following events:

- **a) start-up and shutdown of the log functions; and**
- **b) availability and utilization of needed services with the TSA's network.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-04 for details.

[REQ 7.11-05] The TSA shall act in a timely and co-ordinated manner in order to respond quickly to security events and to limit the impact of breaches of security.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-05 for details.

[REQ 7.11-06] The TSA 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 TSA's procedures.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-06 for details.

[REQ 7.11-07] The TSA shall have procedures and emergency preparedness that ensure notification of a security event or loss of integrity to relevant parties, cf. applicable regulations, for example the data protection authorities and/or the eIDAS supervisory body at the latest 24 hours after the event has been identified.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-07 for details.

[REQ 7.11-08] Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person, the TSA shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-08 for details.

[REQ 7.11-09] The TSA'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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-09 for details.

[REQ 7.11-10] The TSA shall address any critical vulnerability not previously addressed by the TSA within a period of 48 hours after its discovery.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-10 for details.

[REQ 7.11-11] For any vulnerability, given the potential impact, the TSA shall either:

- **a) create and implement a plan to mitigate the vulnerability; or**
- **b) document the factual basis for the TSA's determination that the vulnerability does not require remediation.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-11 for details.

[REQ 7.11-12] Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.1-12 for details.

7.12 Collection of evidence

[REQ 7.12-02] The TSA shall maintain the confidentiality and integrity of archived records concerning operation of its services.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.5.3-02 for details.

[REQ 7.12-03] The TSA shall ensure the completeness, confidentiality and integrity of archived records concerning the operation of its services in accordance with disclosed business practices.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.5.3-02 for details.

[REQ 7.12-04] Records, including audit log, shall be made available if required for the purposes of providing evidence in legal proceedings.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.5.7-01 for details.

[REQ 7.12-05] The precise time of significant environmental, key management and clock synchronization events shall be recorded.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.8-02 for details.

[REQ 7.12-06] The time used to record events as required in the audit log shall be synchronized with UTC at least once a day.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 6.8-01 for details.

[REQ 7.12-07] Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSA's terms and conditions.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 2.1-03 item e. for details.

[REQ 7.12-08] 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-06 for details.

[REQ 7.12-09] a) Records concerning all events relating to the life-cycle of TSU keys shall be logged.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.4.1-03 for details.

[REQ 7.12-10] b) Records concerning all events relating to the life-cycle of TSU certificates (if appropriate) shall be logged.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.4.1-04 for details.

[REQ 7.12-11] 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.

The Time Stamp Service time synchronization is monitored, and extensive logs are provided.

[REQ 7.12-12] d) Records concerning all events relating to detection of loss of synchronization shall be logged.

See REQ 7.12-11.

7.13 Business Continuity Plan

[REQ 7.13-01] The TSA shall define, test and maintain a Business Continuity Plan (BCP) to enact in case of a disaster.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.4-01 for details.

[REQ 7.13-02] In the event of a disaster, including compromise of one of the TSA's private signing keys, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster with appropriate remediation measures.

In particular: see req 7.13-03 to 7.13-06

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.4-02 for details.

[REQ 7.13-03] The TSA's disaster recovery plan shall address the compromise or suspected compromise of the TSU's private signing keys or loss of calibration of a TSU clock, which may have affected time-stamps which have been issued.

This requirement is partly implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7-01 for details.

In case the TSU's private key is compromised or suspected compromised, a new TSU's is established. In case the TSU clock is not calibrated, the TSU will cease issuing of time stamps until the issue has been corrected.

[REQ 7.13-04] 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 the compromise that occurred.

In the case of a compromise, or suspected compromise or loss of calibration when issuing time-stamp, the TSA will make a description of the compromise that occurred available to relying parties via https://ca1.gov.dk.

[REQ 7.13-05] In the case of compromise to a TSU's operation, suspected compromise or loss of calibration, the TSU must not issue time-stamps until steps are taken to recover from the compromise.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.7.3-01 for details.

[REQ 7.13-06] 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 a description of the incident. Such description shall provide information that allows identifying the time-stamps 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 the TSA's operation or loss of calibration, the TSA will make a description of the compromise that occurred available to relying parties via https://ca1.gov.dk.

Subcontractor reports all critical incidents to the TSA and supports the TSA in retrieving needed information from the TSA operations.

7.14 TSA termination and termination plans

[REQ 7.14-01] Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSA's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided.

In particular: see req 7.14-02 to 7.14-08

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-05 for details.

[REQ 7.14-02] The TSA shall have an up-to-date termination plan.

Before the TSA terminates its services, at least the following procedures apply: see req 7.14-03 to 7.14-08

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-03 for details.

[REQ 7.14.03] a) Before the TSA terminates its services, the TSA 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.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-03 for details.

[REQ 7.14-04] b) Before the TSA terminates its services, the TSA shall make the information of the termination available to other relying parties.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-03 for details.

[REQ 7.14-05] c) Before the TSA terminates its services, the TSA shall terminate authorization of all subcontractors to act on behalf of the TSA in carrying out any functions relating to the process of issuing time-stamps.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-03 for details.

[REQ 7.14-06] d) Before the TSA terminates its services, the TSA shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSA for a reasonable period, unless it can be demonstrated that the TSA does not hold any such information.

Due to the nature of the Den Danske Stat TSA currently no other TSP are identified which can take over the delivery of Den Danske Stat’s services.

Den Danske Stat TSA has a termination plan which ensures that the required information is available for a reasonable period

[REQ 7.14-07] e) Before the TSA terminates its services, the TSA's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-08 for details.

[REQ 7.14-08] f) Where possible the TSA should make arrangements to transfer provision of trust services for its existing customers to another TSA.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-09 for details.

[REQ 7.14-09] When the TSA terminates its services, the TSA shall maintain its obligations to make available its public keys to relying parties for a reasonable period or transfer such obligations to another reliable party.

After termination of the TSS, Den Danske Stat will either make it’s TSA certificates publicly available on https://ca1.gov.dk for a reasonable time or transfer this obligation to another public authority.

[REQ 7.14-10] When the TSA terminates its services, the TSA shall revoke all non-expired TSU's certificates.

When the TSA terminates its services, the TSA revokes the TSU's certificates.

[REQ 7.14-11] Where the TSA is a privately held organization or a natural person, the TSA shall provide an irrevocable demand guarantee or the like with an approved institute to secure payment of its financial obligations in accordance with REQ 7.14-1 to REQ 7.14-10.

N/A – Den Danske Stat TSA is a public entity

[REQ 7.14-12] The TSA shall state in its practice statement the provisions made for termination of service. This shall include:

a) **information about the affected entities to be notified; and**
b) **who will take over customers and users, where such form of agreement is available.**

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5.8-02 for details.

7.15 Compliance

[REQ 7.15-01] The TSA shall ensure that it operates in a legal and trustworthy manner as a qualified trust service that issues time-stamps: In particular REQ 7.15-02, 7.15-03 and 7.15-04.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 5-01 for details.

See REQ 7.15-02 to 7.15-04.

[REQ 7.15-02] The TSA shall provide evidence on how it meets the applicable legal requirements. Including, in particular, eIDAS’ regulation of qualified trust services, including any standards specified by the Commission, cf. [eIDAS] article 19 4.a).

See REQ 5.1-01.

[REQ 7.15-03] Services and end user products provided by the TSA shall be made accessible for persons with disabilities, where feasible and applicable standards on accessibility such as ETSI EN 301 549 should be taken into account.

This requirement is implemented according to certificate policies by qualified trust service provider. See [CPS] REQ 9-03 for details.

[REQ 7.15-04] 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.

The TSA is not processing any personal information.