Agency for Digital Government

DEN DANSKE STAT

TSA Practice Statement

Version: 2.1

Author: Danish Agency for Digital Government, Den Danske Stat

Date: 13th February 2026

Den Danske Stat Trust Services

Table of contents

Changelog

Version	Dato	Change description
2.0	30-01-2026	Initial version of the validation practice statement using ETSI policy.
2.1	13-02-2026	Minor corrections.

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 [ETSI EN 319 421] and [ETSI EN 419 422]. As the Time Stamp Tokens (TST) issued by the Time Stamp Authority uses recognized and recommended 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.

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.

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.

Many of the general requirements from [ETSI EN 319 421] for the Time Stamp Authority are similar to general policy requirements for qualified trust service providers stated in [ETSI EN 319 401]. How the Den Danske Stat meets these requirements is described in [GRPS] and whenever relevant referenced to from this document.

2. Void

This section is added to have the same numbering as [ETSI EN 319 421].

3. Void

This section is added to have the same numbering as [ETSI EN 319 421].

4. General concepts

4.1. 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.

4.2. 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.

4.3. 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 with 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.

4.4. 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.

5. Introduction to time-stamp policies and general requirements

5.1. General requirements

The Agency for Digital Government has established a trust service provider Den Danske Stat, which provides time stamping services which meet 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 seals 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 TSA uses policy BSTP from [ETSI EN 319 421].

The profile of the public key certificates used by the Den Danske Stat in general and for the TSA are described in [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.

5.2. Policy name and identification

The best practices policy for time-stamp (BSTP) is identified by

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

This version of the TSA practice can be identified through the OID

iso(1) iso-member-body(2) denmark(208) stat(169) pki(1) practice-statements(2) timestamp(2) major-ver(2) minor-ver(1)

5.3. User community and applicability

The time stamp 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].

5.3.1. Best practices time-stamp policy

The TSS is used by Den Danske Stat’s Signing Service.

6. Policies and practices

6.1. Risk assessment

See [GRPS], clause 5 for general considerations on Risk Assessment.

6.2. Trust Service Practice Statement

See [GRPS], clause 6.1 for general considerations on Trust Service Practice Statement.

The hashing algorithm SHA512 is calculated over the data, and hash value is used as reference to represent the data that is time stamped.

The time-stamps has an accuracy of 500 ms. The time is synchronized with the GNSS based reliable time source using antennas located in Denmark and Norway.

There are no limitations on the use of TSS.

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.

Obligations for relying parties are available in section 6.5.

Information on good practice on how to verify a time stamp issued by the TSS can be found in section 6.6

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

The TSA disclosure agreement is published at the TSP repository.

6.3. Terms and conditions

See [GRPS], clause 6.2 for general conditions on Terms and conditions.

6.4. Information security policy

See [GRPS], clause 6.3 for general conditions on Information security policy.

6.5. TSA obligations

6.5.1. General

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

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

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 appears on EUTL.

    b. The TSA certificate has not expired.

    c. The TSA certificate has not been 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

7.2. Internal organization

See [GRPS], clause 7.1 for general considerations on Internal organization.

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

See [GRPS], clause 7.2 for general considerations on Human resources.

7.3. Personnel security

See [GRPS], clause 7.2 for general considerations on Human resources.

7.4. Asset management

See [GRPS], clause 7.3 for general considerations on Asset management.

7.5. Access control

See [GRPS], clause 7.4 for general considerations on Access control.

7.6. Cryptographic controls

7.6.1. General

See [GRPS], clause 7.5 for general considerations on Cryptographic controls.

7.6.2. TSU key generation

TSU signing key is generated in a physically secured environment under dual control by personnel in trusted roles following key signing ceremony scripts.

The TSU uses cryptographic modules which meet the requirements in FIBS PUB 140-2 level 3.

The Time Stamp Units provide time stamp tokens, which are signed using ECDSA on secp256r1, using SHA256 as hash algorithm. These algorithms are recommended by [ALGO].

The TSA uses two TSU's each with their own dedicated cryptographic module and TSU signing key. Each TSU has been configured with one active private time-stamp signing key.

7.6.3. TSU private key protection

See section 7.6.2 for remarks on TSU private key protection.

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

7.6.4. TSU public key certificate

The TSUs certificates are issued during a key signing ceremony in the secure facilities of the TSP by authorized personnel following scripted procedures. This ensures that the subject information in the certificate is correct, that the issuer of the certificate is Den Danske Stat qualified root CA and that the TSU certificates are signed by the Den Danske Stats qualified root CA.

The TSU certificates appear on the LoTL[1] (List of Trusted Lists) as well as on the TSPs repository:

https://ca1.gov.dk

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

7.6.5. Rekeying TSU's key Life cycle management of signing cryptographic hardware

The Time Stamp Units provide time stamp tokens, which are signed using ECDSA on secp256r1 using SHA256 as hash algorithm. These algorithms are recommended by [ALGO]. The validity of the TSU’s certificates are 20 Years and inline with [ALGO], which only provides limitations for legacy key sizes.

7.6.6. Life cycle management of signing cryptographic hardware

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

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. End of TSU key life cycle

The TSUs private keys are replaced before the expiry of the TSUs certificates. The TSP has created a notification schedule to ensure that new TSUs keys are created and used 90 days before the existing TSU certificates expires. As part of key update, expired keys are deleted.

The expiration date for TSU certificates is one day before the expiry of the corresponding TSU certificates.

7.7. Time-stamping

7.7.1. Time-stamp issuance

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

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, which serves the UTC timescale by definition.

[1] The LoTL is available at https://ec.europa.eu/tools/lotl/eu-lotl.xml

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.

The GNSS based reliable time source uses UTC (k) lab. UTC (USNO).

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.

TSUs private key is only used for signing time stamp tokens. If the TSU private key expires, the key is deleted and can't be used to issue time stamp tokens.

7.7.2. Clock synchronization with UTC

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.

The 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.

The TSA continuously monitors for time synchronisation and will automatically update the time whenever a leap second occurs. Whenever this happens, an entry is recorded in the audit log.

7.8. Physical and environmental security

See [GRPS], clause 7.6 for general considerations on Physical and environmental security.

7.9. Operation security

See [GRPS], clause 7.7 for general considerations on Operation security.

7.10. Network security

See [GRPS], clause 7.8 for general considerations on Network security.

7.11. Incident management

See [GRPS], clause 7.9 for general considerations on Incident management.

7.12. Collection of evidence

See [GRPS], clause 7.10 for general considerations on Collection of evidence.

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

7.13. Business continuity management

See [GRPS], clause 7.11 for general considerations on Business continuity management.

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

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.

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

See [GRPS], clause 7.12 for general considerations on termination and termination plans.

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

7.15. Compliance

See [GRPS], clause 7.13 for general consideration on Compliance.

7.16. Supply chain

See [GRPS], clause 7.14 for general considerations on Supply chain.

8. Additional requirements for qualified electronic time-stamps as per Regulation (EU) No 910/2014

8.1. TSU public key certificate

See section 7.6.4 for information on TSU public key certificate.

8.2. TSA issuing non-qualified and qualified electronic time-stamps as per Regulation (EU) No 910/2014

The TSA does not issue non-qualified time-stamps.

9. References

Term	Reference
[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.
[CIR 2025/1929]	COMMISSION IMPLEMENTING REGULATION (EU) 2025/1929 of 29 September 2025 laying down rules for the application of Regulation (EU) No 910/2014 of the European Parliament and of the Council as regards the binding of date and time to data and establishing the accuracy of the time sources for the provision of qualified electronic time stamps. https://eur-lex.europa.eu/eli/reg_impl/2025/1946/oj
[ETSI EN 319 401]	ETSI EN 319 401, Electronic Signatures and Trust Infrastructures (ESI) General Policy Requirements for Trust Service Providers. v3.2.0, June 2025, ETSI ESI. https://www.etsi.org/standards
[ETSI EN 319 421]	ETSI EN 319 421, Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps, v1.3.1, July 2025, ETSI ESI. https://www.etsi.org/standards
[ETSI EN 419 422]	ETSI EN 419 422, Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles, v1.1.1, March 2026, ETSI ESI. https://www.etsi.org/standards
[RFC 3161]	Network Working Group, Request for Comments: 3161, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP), August 2001. https://www.ietf.org/rfc/rfc3161.txt
[RFC 5816]	Internet Engineering Task Force (IETF), Request for Comments: 5816 , ESSCertIDv2 Update for RFC 3161, March 2010. https://www.ietf.org/rfc/rfc5816.txt
[GRPS]	Den Danske Stat Practice Statement on General Security Requirements for Trust Service Providers. https://www.ca1.gov.dk/
[Profile]	Den Danske Stat Certificate Profile. https://www.ca1.gov.dk/
[AdES]	Den Danske Stat AdES Signature Profile. https://www.ca1.gov.dk/
[ALGO]	European Cybersecurity Certification Group, Sub-group on Cryptography: ‘Agreed Cryptographic Mechanisms’ published by the European Union Agency for Cybersecurity. https://certification.enisa.europa.eu/publications/eucc-guidelines-cryptography_en