Agency for Digital Government

PKI DISCLOSURE STATEMENT FOR DEN DANSKE STAT TSP

Version: Version 1.2

By: The Danish Agency for Digital Government, Den Danske Stat TSP

Published: 24th September 2024

Den Danske Stat - Trust Services

Table of content

Preface

Den Danske Stat TSP (Trust Service Provider) is issuing certificates according to *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* (hereafter denoted eIDAS1).

The TSP is operated by the Agency for Digital Government on behalf of the Danish State.

The qualified certificates used to create qualified electronic signatures, and qualified electronic seals are issued using certificate policies owned and administered by Agency for Digital Government, which requires the private keys to be protected by a Qualified Signature Creation Device (QSCD). The certificate policies are compliant with the European standards ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2 and are used for issuing certificates to physical persons, physical persons associated with a legal person and legal persons.

The TSP also issues other public key certificates not in scope of this statement.

Revision history

Version	Date	Author	Changes
1.0	28-09-2021	Den Danske Stat TSP	Initial version
1.2	24-09-2024	Den Danske Stat TSP	Scope of the statement is further specified Reference to EU/EAA TRUSTED List added. Supporting version 1.2 of policies. Excepting short-term certificates for status check requirement. Change of Logo. Update of responsible authority/agency.

CA Contact Information

The TSP can be contacted via

Agency for Digital Government
Landgreven 4
DK-1301 København K
Denmark

Phone: +45 3392 5200

E-mail: digst@digst.dk

Certificate type, validation procedures and usage

The TSP issues certificates to

- Physical persons
- Physical persons associated with a legal person
- Legal persons

Qualified certificates are issued after a registration of the subject compliant with eIDAS1 article 24.1

None of the certificates issued to subscribers or subjects associated with subscribers shall be used for issuing certificates i.e. act as intermediate CA.

Reliance limits

OCES certificates issued by the CA are designed as general-purpose certificates without any reliance limits included as content of the certificate.

Logs and registration information is retained for at least seven years and can be used as evidence in legal disputes.

Obligations of subscribers

The subscriber and subject must

- provide accurate and complete information to CA.
- ensure that the certificates and corresponding keys are used in accordance with limitations listed in terms and conditions.
- ensure no misuse of keys.
- ensure that key generated by subscriber or subject is in accordance with requirements with respect to algorithms and key length.

- ensure and maintain the subject's sole control of private keys corresponding to the issued certificates and is obligated to request revocation if the keys are lost, compromised, suspected to be compromised, if data in the certificate is inaccurate or if the subject shall no longer use the certificate.
- ensure that all private keys corresponding to qualified certificates used to create qualified signatures are protected by qualified signature creation devices (QSCD).
- stop using a certificate and corresponding private key if certificates are revoked or requested revoked (except for key decipherment purposes).

Certificate status checking obligations of relying parties

Before trusting any certificates in the provided infrastructure, a relying party must:

- Ensure that for qualified certificates the trust anchor (the root certificate) shall be identified as a qualified TSP on the EU/EAA Trusted List.
- Verify the TSP certificates (integrity and revocation status) in the trust chain.
- Verify the issuer's signature in the certificate.
- Verify the revocation status of the certificate using either a valid and updated revocation list or an online certificate status check unless the certificate includes the extension *ext-etsi-valassured-ST-certs* indicating that the revocation status does not need to be validated due the short certificate validity period.
- Check if the certificates include limitations, which are not compatible with the use for which the certificate is verified.

Limited warranty and disclaimer/Limitation of liability

The TSP is liable to anyone who reasonably relies on a valid certificate according to the general rules of Danish law, unless the TSP can lift the burden of proof for not having acted intentionally or negligently, including that the certificate has not been used in accordance with the guidelines contained in the certificate.

Losses due to TSP's errors in connection with registration, issuance and revocation of the certificate are covered by TSP's responsibility.

CA's liability towards relying parties to the extent that these parties are businesses or public authorities is in all cases limited to DKK 100,000.

Applicable agreements, CPS, CP

End user terms and conditions can be found at:

Den Danske Stat - Trust Services: Terms (Den Danske Stat - Tillidstjenester: Vilkår) (in Danish)

Supported certificate policies:

- Public Certificate Policy for qualified person certificates Version 1.2 (OID 1.2.208.169.1.1.2.1.1.2)
- Public Certificate Policy for qualified employee certificates Version 1.2 (OID 1.2.208.169.1.1.2.2.1.2)
- Public Certificate Policy for qualified organizational certificates Version 1.2 (OID 1.2.208.169.1.1.2.3.1.2)
- Certificate Policy for OCES employee certificates (1.2.208.169.1.1.1.2.7.2)
- Certificate policy for OCES organizational certificates (1.2.208.169.1.1.1.3.7.2)

The certificate policy can be found on:

Den Danske Stat - Certificate Authority: Public Trust Services (Den Danske stat - Tilsynsorgan: Offentlige Tillidstjenester) (in Danish)

The Certificate Practice Statements (CPS) can be found on:

Dan Danske Stat - Trust Services: Declarations of compliance (Den Danske Stat - Tillidstjenester: Efterlevelseserklæringer) (in Danish)

Privacy policy

The Agency for Digital Government privacy policy can be found on:

Agency for Digital Government website: Privacy policy for the Agency for Digital Government (Digitaliseringsstyrelsen: Privatlivspolitik for Digitaliseringsstyrelsen) (in Danish)

Agency for Digital Government website: Privacy policy for the Agency for Digital Government

Based on requirements set forth in certificate policies data is generally retained for seven years.

Refund policy

N/A

Applicable law, complaints and dispute resolution

Qualified certificates are regulated via eIDAS1.

Any complaints shall be sent to the TSP. If a dispute is not settled by informal negotiation, disputes are solved applying Danish law in the district Court of Copenhagen

TSP and repository licenses, trust marks, and audit

The TSP is a qualified certificate issuer according to eIDAS1 and is included as a qualified CA in the EU trust service provider list at:

European Commission website - eIDAS Dashboard: EU/EEA Trusted Lists