

PKI DISCLOSURE STATEMENT FOR DEN DANSKE STAT TSP

Version: 1.4

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

Published: 17th April 2026





Table of content

- Preface 3
- Revision history 3
- CA Contact Information 4
- Certificate type, validation procedures and usage..... 4
- Reliance limits..... 4
- Obligations of subscribers 4
- Certificate status checking obligations of relying parties..... 5
- Limited warranty and disclaimer/Limitation of liability 5
- Applicable agreements, CPS, CP 6
- Privacy policy 6
- Refund policy 6
- Applicable law, complaints and dispute resolution 6
- TSP and repository licenses, trust marks, and audit 7



Preface

Den Danske Stat TSP (Trust Service Provider) is issuing certificates according to *Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework* (hereafter denoted eIDAS2).

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.
1.3	23-01-2026	Den Danske Stat TSP	Reference to eIDAS1 update to eIDAS2 Support of combined OCES and Qualified CP version 8.0
1.4	17-04-2026	Den Danske Stat TSP	Availability information added



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 eIDAS2 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.

All services related to Den Danske Stat CA including issuance, CRL download and OCSP service are available on a 24/7/365 basis. The CA cannot be held liable for the availability being provided.

Reliance limits

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 the 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 policy:

- Combined Public Certificate Policy for OCES and Qualified Certificates Version 8.0 (OID 1.2.208.169.1.1.3.8.0)

The certificate policy can be found on:

<https://certifikat.gov.dk> (website is in Danish but policy is in English)

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

<https://ca1.gov.dk> (website is in Danish but practice statement is in English)

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](#) (English)

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

Certificates are regulated via eIDAS2.

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 eIDAS2 assessed by an independent conformity assessment body and is included as a qualified CA in the EU trust service provider list at:

[European Commission website - eIDAS Dashboard: EU/EEA Trusted Lists](#)

