DIGITALISERINGSSTYRELSEN

PKI Disclosure Statement for Den Danske Stat CA

Version 1.0

The CA is issuing qualified 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 (eIDAS).

The qualified certificates are issued using a certificate policy owned and administered by DIGST which require the private keys to be protected by a qualified signature creation device (QSCD). The certificate policy is compliant with the European standards ETSI EN 319 401 and ETSI EN 319 441-1 and is used for issuing certificates to physical persons.

Revision history

Version	Changes
Version 1.0	Initial version

TSP Contact Information

The CA is operated by the Agency for Digitisation on behalf of the Danish State. CA can be contacted via

Digitaliseringsstyrelsen
Landgreven 4
DK-1301 København K
Denmark

Phone: +45 3392 5200

E-mail: digst@digst.dk

Certificate type, validation procedures and usage

The CA issues certificates to

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

For physical persons, all certificates are issue are qualified according to the eIDAS.

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

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

Reliance limits

End user qualified and OCES certificates issued by CA are designed as general-purpose certificates with any reliance limits included as content of the certificate.

Logs and registration information are 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 limitation listed in terms and conditions.
- ensure misuse of keys.
- ensure that key generated by subscriber or subject is in accordance with requirement 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 are protected by 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

- Verify the CA certificates (integrity and revocation status) in the trust chain.
- Verify the issuers 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.
- Check if the certificates include limitation which is not compatible with the use for which the certificate is verified.

Limited warranty and disclaimer/Limitation of liability

CA is liable to anyone who reasonably relies on a valid certificate according to the general rules of Danish law, unless the CA 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.

Covered by the CA responsibility is losses due to CA's errors in connection with registration, issuance and revocation of the certificate.

CA's liability towards relying parties to the extent that these parties are businesses or public authorities is in all cases limited to DKK 500,000.

Applicable agreements, CPS, CP

End user terms and conditions can be found at https://ca1.gov.dk

Supported certificate policy:

- Public Certificate Policy for qualified person certificates Version 1.1 (OID 1.2.208.169.1.1.2.1.1.1)

The certificate policy can be found on https://certifikat.gov.dk/politikker-for-tillidstjenester/

CPS can be found on https://www.ca1.gov.dk/

Privacy policy

DIGST privacy policy can be found on

https://digst.dk/om-os/privatlivspolitik/ (in Danish)

https://en.digst.dk/about-us/about-endigstdk/privacy-policy/ (in 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

Qualified certificates are regulated via eIDAS.

Any complaints shall be sent to DIGST. 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

CA is a qualified certificate issuer according to eIDAS and is included as a qualified CA in the EU trust service provider list at https://webgate.ec.europa.eu/tl-browser/#/