DANISH AGENCY FOR DIGITAL GOVERNMENT

Erhverv

Annex 5
Terms and conditions for qualified seals in the Signing Solution

Content

1 Qualified seals in the Signing Solution

These terms and conditions regulate the User Organisation's provision of a qualified electronic seal (seal) when using a qualified organisation certificate issued by Den Danske Stat Tillidstjenester via the Signing Solution for use in public and private Self-Service Solutions.

Unless otherwise stated, these terms and conditions also apply to the issuing of qualified time stamps linked to the electronic seal. A qualified time stamp documents the time when the electronic seal was provided, including that the certificate and the signed data were available at the time of signing.

In the following, the User Organisation is referred to as the Subscriber and the entity associated with the Subscriber who is registered and to whom a certificate is issued is named the Subject.

These terms and conditions have been prepared in accordance with the Public Certificate Policy for Qualified organizational certificates, version 1.1, which forms the basis for the Danish Agency for Digital Government's issuing of the qualified organisation certificate. The terms and conditions also cover the certificate policy.

These terms and conditions use the term organisation certificate for the type of certificate that is referred to as a organizational certificate in the certificate policy. The certificate policy's regulation of organizational certificates thus applies to the organisation certificates in these terms and conditions and the electronic seals issued on this basis.

The qualified time stamps linked with the electronic seal are issued based on the Danish Agency for Digital Government's Public Policy for Qualified Time-Stamping, version 1.0, which is also covered by these terms and conditions.

The certificate policy, policy for time-stamping and the Danish Agency for Digital Government's description of the Signing Solution (Certificate Practice Statement) are available at certifikat.gov.dk.

Den Danske Stat Tillidstjenester issues various other certificate types for commercial use. These certificates are subject to separate terms and conditions.

2 Contact information

Den Danske Stat Tillidstjenester can be contacted at:

Danish Agency for Digital Government
Attn. Den Danske Stat Tillidstjenester
Landgreven 4
DK-1301 Copenhagen K

Further contact information is available at www.ca1.gov.dk/

3 The legal validity of the organisation certificate

The qualified electronic seal is recognised by the EU. Accordingly, Den Danske Stat Tillidstjenester acts as qualified trust service provider as specified in 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 (the eIDAS regulation).

In terms of a qualified electronic seal provided based on a qualified organisation certificate, there is a presumption of the integrity of the data and the accuracy of the origin of the data to which the qualified electronic seal is related. Qualified seals are recognised by all members of the European Economic Area.

When linking the signed data with a qualified electronic time stamp, all Member States have a presumption of the accuracy of the date and time it states and the integrity of the data to which the date and time indication relates.

4 Applications – qualified seals

4.1 General application

A qualified organisation certificate for providing a qualified seal can be used when an organisational unit related to the Subscriber is to sign data in order to document the integrity and accuracy of data.

The Signing Solution can only be used to provide a qualified electronic seal online via service providers who have joined the solution. Accordingly, the certificate for the seal cannot e.g. be used to sign emails via an email client or for encryption.

Seals in the Signing Solution are based on cryptographic keys that are created for the specific occasion in a central qualified signature creation device (QSCD) and the private key is deleted immediately after each electronic seal has been created.

Seals and organisation certificates should not be used for authentication. The authentication to a service provider is managed by the User's eID authenticator.

Electronic seals are issued in LTV format.

No restrictions have been set for the type of agreements and obligations that can be made when using organisation certificates issued by Den Danske Stat Tillidstjenester.

4.2 Naming the Subject in the certificate

The Subscriber's User Administrator determines the Subject's naming in the certificate.

5 Availability

5.1 Signing solution

All the Danish Agency for Digital Government's Services related to issuing and validation of certificates are available 24/7/365.

The Danish Agency for Digital Government cannot be held liable for the above availability being provided.

5.2 Certificate revocation list

A list of revoked certificates can be accessed at any time via Den Danske Stat Tillidstjenester's (CA 1) certificate revocation list at www.ca1.gov.dk/tilbagekald-certifikater/.

6 Obligations on using qualified organisation certificates

6.1 Publication of the certificate

Certificates issued via the Signing Solution will not be made public. The individual certificate is only embedded in the electronic seal.

6.2 Validity period of the certificate

The certificate is valid for 10 days. However, the technical solution ensures that it is not possible to create multiple seals based on the same certificate.

The extended validity of the certificate after the seal has been provided is solely based on technical concerns for the systems that will subsequently be reading the seal. Revocation of certificate

6.3 Revocation of certificate

The Signing Solution deletes the private key belonging to the certificate immediately after providing the qualified electronic seal an therefor the certificate cannot be used as basis for a new seal. Accordingly, the Subscriber or the Subject is under no obligation to revoke the certificate even if a situation should arise that, had it occurred prior to the use of the certificate, would warrant a revocation.

6.4 Limitations on naming the Subject

The specific naming of the Subject, cf. clause 4.2, may not be of such nature that it is be confusingly similar to a trademark. Moreover, the Danish Agency for Digital Government may order a Subscriber to stop using specific naming if the Danish Agency for Digital Government finds that such use may be offensive.

7 Obligations as relying party receiving an electronic seal

Prior to trusting a certificate, the relying party receiving an electronic seal must ensure the following:

- that the certificate is valid and has not been revoked at the time of signing – i.e. is not listed on the revocation list of Den Danske Stat Tillidstjenester (CA 1)
- that the purpose for which the certificate is to be used is suitable in respect of any use limitations in the certificate and
- that the use of the certificate in general is suitable in terms of the level of security as described in these terms and conditions and the underlying certificate policy for the certificate, cf. clause 1.

Before a time stamp is accepted, the relying party receiving an electronic seal must ensure the following:

- that the time-stamp is correctly signed and that the private key used to sign the time-stamp has not been marked as compromised at the time of the verification,
- take into account any limitations on the use of the time-stamp indicated by the time-stamp policy and
- take into account any other precautions prescribed in agreements or elsewhere.

Unless warranted by other circumstances, an electronic seal issued based on these terms and conditions will be valid and the relying party can rely on it even though the certificate after the provision of the seal has expired or been revoked.

Signed documents can be validated in the Danish Agency for Digital Government's validation service at https://validering.ca1.gov.dk/

Detailed information about the relying party's obligations is stated in the PKI Disclosure Statement which is available at www.ca1.gov.dk/pds. Moreover, the Danish Agency for Digital Government has provided further information in the certificate on its use, including a reference to the PKI Disclosure Statement.

8 Support

8.1 General support

Support requests regarding qualified organisation certificates, including general circumstances related to provision of an electronic seal and use of certificates can be made to MitID Erhverv Support on tel. +45 33980020 or via the contact form at http://www.mitid-erhverv.dk/support/kontakt.

The Danish Agency for Digital Government does not provide support related to technical matters, including installation of software and establishment of controls and processes at the Subscriber.

The Subscriber may enter a support agreement with Nets DanID A/S, cf. the relevant descriptions in the terms and conditions for User Organisations. With a support agreement, it is possible to request technical support, including urgent support, against payment.

9 Processing of personal data

9.1 Privacy policy

Certificates from the Danish Agency for Digital Government are covered by the Danish Agency for Digital Government's Privacy Policy for MitID Erhverv. The Privacy Policy is available at www.mitid-erhverv.dk/info/losning/privatlivspolitik/.

9.2 Data control

The Danish Agency for Digital Government is the controller of the personal data being processed by the Signing Solution in connection with the certificate application. NNIT A/S and Nets DanID A/S are the processor for the Danish Agency for Digital Government.

The processing of personal data is subject to the data protection rules, including the General Data Protection Regulation and the Danish Data Protection Act.

Personal data is erased after the current year + 7 years.

9.3 Registration of data on creation and use of certificates

The Danish Agency for Digital Government stores various data on registration of the Subscribers and Subjects and the subsequent use of certificates.

The following is registered:

- Time of signing/issuing the certificate
- The Subscriber’s basic company data as registered in the MitID Erhverv
- The NSIS Level of Assurance the Subscriber is authorised at towards the service
- Session UUID
- Reference text
- Technical data related to the authentication (SAML assertion)
- Subject's name, UUID and email

All data related to the Subscriber and Subject will be stored for seven (7) years.

9.4 Data that is not registered

Den Danske Stat Tillidstjenester does not register data about which document or which data that are signed when the certificate is used.

9.5 Overview of the use of signature

MitID Erhverv makes it possible to access a log of all uses of the Signing Solution.

9.6 Data storage

All data related to the Subscriber and Subject, including use of the Signing Solution, will be stored for seven (7) years.

If the Signing Solution terminates within the 7-year period, data will continue to be stored and can be accessed by the competent authorities and other parties having a legitimate interest in such data.

10 Termination of Den Danske Stat Tillidstjenester

If Den Danske Stat Tillidstjenester stops issuing organisation certificates, Den Danske Stat Tillidstjenester is entitled to transfer all registered data to another legal entity, including a public authority or a public law body, which will be tasked with undertaking the continued administration of or termination of Den Danske Stat Tillidstjenester

11 Electronic communication

In connection with the operation of the service, Den Danske Stat Tillidstjenester may contact the Subscriber by email. Enquiries may concern operation-related information, security-related matters, changes and termination.

The Danish Agency for Digital Government usually communicates matters regarding the use of certificates to the Subscriber's Organisation Administrator and Identity Administrator.

12 Liability of the Danish Agency for Digital Government

12.1 Liability to the Subscriber

Subject to the general rules of Danish law, the Danish Agency for Digital Government is liable for failure to comply with these terms and conditions, including for any loss resulting from the Danish Agency for Digital Government's errors in connection with registration, issuing and revocation of the certificate.

The Danish Agency for Digital Government must prove that it has not acted intentionally or negligently.

12.2 Liability to third parties

The Danish Agency for Digital Government is liable to anyone who reasonably relies on a qualified electronic seal from the Signing Solution under the general rules of Danish law unless the Danish Agency for Digital Government can prove that it did not act intentionally or negligently, including that the certificate has not been used in compliance with the guidelines contained in the certificate.

The Danish Agency for Digital Government's liability comprises any loss due to the Danish Agency for Digital Government having made errors in connection with registration, issuance and revocation of the certificate.

12.3 Limitations of liability

The Danish Agency for Digital Government's liability to both the Subscriber and third parties, to the extent that such parties are legal entities, including public authorities and public organisations, is limited to DKK 100,000 for each loss-making event, and is in any event maximised at DKK 100,000 per year. A loss-making event is considered as any matter arising from the same continued or repeated actionable matter.

12.4 Liability for provision of time stamp

The provisions stated under clauses 12.1 to clause 12.3 also apply to the Danish Agency for Digital Government's provision of time stamps.

13 Use restrictions

The Danish Agency for Digital Government has set no use restrictions for qualified organisation certificates, cf. however, clause 4 on limitations in the technical use of certificates.

14 Use of qualified organisation certificate

14.1 General conditions

The Subject's use of a qualified organisation certificate for providing a qualified seal is done on behalf of the Subscriber in accordance with the agreements entered into between these parties.

The Danish Agency for Digital Government is not a party to such agreements and cannot be held liable for the actual use of an organisation certificate.

14.2 Limitations on the use of certificate and keys

The key pair of the certificate may only be used in accordance with the determined authorised use and not beyond any limitations notified to the Subscriber and the Subject, and the private key must not be used to sign other certificates.

Prior to providing a seal, the Subscriber must check the content of the certificate, including with a view to checking whether its use takes place within the limitations stated therein. The certificate and its content are accepted on approval of the signing in question.

14.3 Protection of authenticator

The Subject must protect the authenticator (e.g. MitID) and related security mechanisms (e.g. password) that are used for providing an electronic seal in accordance with the applicable terms and conditions to ensure that reasonable measures have been taken to prevent an electronic seal from being given in the Subject's name.

If the authenticator used for authentication against the Signing Service is believed to be compromised, this authenticator must be revoked in accordance with the relevant terms and conditions to prevent unauthorised use for providing an electronic seal in the Subject's name.

14.4 Updated and correct information

The Subscriber must ensure that information that serves as basis for the issuing of a certificate is correct and complete at the time of issuing the certificate. The information is presented as part of the issuing process and is based on the information already registered in MitID Erhverv.

If the data are incorrect, the Subscriber is obligated to terminate the signing process.

14.5 Protection on a qualified electronic signature creation device (QSCD)

In terms of the Subscriber, the Signing Solution ensures that the private key being issued with the certificate is created and can only be used for cryptographic actions within the secured cryptographic device (QSCD) in the Signing Solution. Accordingly, only the Subscriber is in charge of the private key and the certificate when providing an electronic seal.

14.6 Revocation of certificate

The Signing Solution deletes the private key belonging to the certificate immediately after providing the qualified electronic seal where the certificate cannot be used as basis for a new seal. Accordingly, the Subject is under no obligation to revoke the certificate even if a situation should arise that, had it occurred prior to the use of the certificate, would warrant a revocation.

15 Changes to terms and conditions

The Danish Agency for Digital Government may change the terms and conditions at three months' notice.

If the Danish Agency for Digital Government finds that changes are material for operational purposes, including security, changes can be made at shorter notice, including with effect from the time of notification.

16 Governing law and disputes

Any matters subject to these terms and conditions and their interpretation must be settled according to Danish law.

Any dispute arising out of the use of certificates issued by the Danish Agency for Digital Government must be brought before the City Court of Copenhagen.