DANISH AGENCY FOR DIGITAL GOVERNMENT

Erhverv

Annex 4
Terms and conditions for qualified user signatures

Content

1 Qualified user signatures in the Signing Solution

These terms and conditions regulate business users' provision of a qualified electronic user signature (electronic signature) by using qualified user certificates issued by Den Danske Stat Tillidstjenester's signing solution for 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 signature. A qualified time stamp documents the time when the electronic signature was provided, including that the certificate and the signed data were available at the time of signing.

In the following, the User Organisation will be referred to as Subscriber and the User as Subject.

These terms and conditions have been prepared in accordance with the certificate policy for qualified employee certificates, version 1.1, which forms the basis for the Danish Agency for Digital Government's issuing of qualified user certificates. The qualified time stamps linked with the electronic signature are issued based on the Danish Agency for Digital Government's Public Policy for Qualified Time-Stamping, version 1.0. Both the certificate policy for qualified employee certificates and policy for qualified time-stamping are covered by these terms and conditions.

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

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.

The terms and conditions for issuing and using qualified user certificates consist of two parts that address the Subscriber (part 1) and the Subject (part 2), respectively.

The User Organisation's acceptance of the terms and conditions comprises both parts and the User Organisation therefore also accepts that Users in the role as Subject become subject to the terms and conditions in part 2.

The User Organisation's Users only need to accept part 2 in connection with the issuing of the certificate to the individual User in the Signing Solution.

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/

Part 1 Terms and conditions for the Subscriber

3 Legal validity of user certificates

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). The user signature provided is therefore enforceable throughout all members of the European Economic Area in the same way as a physical signature.

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 stated by the time stamp and the integrity of the data to which the date and time indication relates.

4 Applications – qualified user signatures

4.1 General application

A qualified user certificate can be used when a natural person linked to a Legal Entity is to sign data with a qualified electronic signature that is comparable to a physical signature and that must be universally recognised by all members of the European Economic Area.

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

User signatures in the Signing Solution are based on cryptographic keys that are created for the specific occasion in a central qualified signature creation device (QSCD). The private key is deleted immediately after creation of each individual electronic signature.

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

Signatures are issued in LTV format

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

4.2 Pseudonym

The Subscriber's User Administrator determines the Subject's naming in the certificate. A Pseudonym may be used.

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 certificate revocation list at www.ca1.gov.dk/tilbagekald-certifikater/.

6 Obligations on using qualified user certificates

6.1 Publication of the certificate

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

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 signatures based on the same certificate.

The extended validity of the certificate after signing is based on technical concerns for the systems that will subsequently be reading the signature.

6.3 Revocation of certificate

Since the Signing Solution deletes the private key belonging to the certificate immediately after the electronic signature has been provided, and the certificate therefore cannot be used as basis for a new signature. Accordingly, the Subscriber or 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.

7 Obligations as relying party receiving an electronic signature

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

- that the time stamp is signed correctly with a valid certificate
- 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 signature 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 signature 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 user certificates, including general circumstances related to provision of an electronic signature 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 and MitID Erhverv 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

The Danish Agency for Digital Government’s registration and processing of data, including personal data in connection with registration of Subjects and the subsequent use of certificates, are described in clause 18.

10 Termination of Den Danske Stat Tillidstjenester

If Den Danske Stat Tillidstjenester stops issuing qualified user certificates, Den Danske Stat Tillidstjenester is entitled to transfer all registered data to a third party thus allowing such third party to assume the obligations of Den Danske Stat Tillidstjenester under these terms and conditions.

11 Electronic communication

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

Communication regarding the use of certificates to the Subscriber’s Organisation Administrator and User 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 signature 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, subject to clauses 12.1 and 12.2, 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 12.1-12.3 also apply to the Danish Agency for Digital Government's provision of time stamps.

13 Use restrictions

Den Danske Stat Tillidstjenester has set no restrictions for use of qualified user certificates, cf., however, clause 4 on limitations in the technical use of certificates.

14 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.

15 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 Den Danske Stat Tillidstjenester must be brought before the City Court of Copenhagen.

Part 2 Terms and conditions for the Subject

16 Introduction

16.1 General conditions

These terms and conditions regulate the use of qualified user certificates issued by Den Danske Stat Tillidstjenester under the Danish Agency for Digital Government.

The user certificates are issued to Business Users in the role as Subject, who has been given rights to provide user signatures via the Signing Solution by the Business User's User Organisation (referred to as Subscriber).

The terms and conditions must be accepted by the Subject prior to issuing a qualified user certificate for providing a qualified signature in the Signing Solution. The issuing takes place on behalf of the Subscriber to which the Subject is linked.

The terms and conditions have been approved by the Subscriber, which has also accepted the general terms and conditions for the use of qualified user certificates from Den Danske Stat Tillidstjenester.

For further information about the use of a business user for providing signatures, go to mitid-erhverv.dk.

16.2 Contact information

Den Danske Stat Tillidstjenester can be contacted at:

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

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

17 Obligations on using a qualified user certificate

17.1 General conditions

The Subject's use of a qualified user certificate for providing a qualified signature is done on behalf of the Subscriber in accordance with the agreements entered into between these parties, including any terms of employment.

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

17.2 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 Subject, and the private key must not be used to sign other certificates.

Prior to providing a signature, the Subject must check the content of the certificate and ensure that its use takes place within the limitations stated therein. The certificate and its content are accepted on approval of the signing in question.

17.3 Protection of authenticator

The Subject must protect the authenticator and related security mechanisms (e.g. passwords) used for providing an electronic signature in accordance with the relevant terms and conditions. On this background,

the Subject must take reasonable precautions to prevent an electronic signature being provided in the Subject's name.

If the authenticator used for authentication against the signing solution 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 signature in the Subject's name.

17.4 Updated and correct information

The Subject must ensure that information that serves as basis for the issuing a certificate are correct and complete at the time of the issuing of 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 Subject is obligated to terminate the signing process.

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

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

17.6 Revocation of certificate

The Signing Solution deletes the private key belonging to the certificate immediately after signing whereas the certificate cannot be used as basis for a new signature. 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.

18 The Danish Agency for Digital Government's registration of data

18.1 Registration of data on creation and use of certificates

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

The following is registered:

- Time of signing/issuing the certificate
- The Subscriber's company data as registered in 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)
- Name (alternatively synonym), UUID and email of the Subject

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

18.2 Data that is not registered

The Danish Agency for Digital Government does not register data about which document or which data that are signed when the certificate is used.

18.3 Overview of the use of signature

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

18.4 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.

19 Termination of Den Danske Stat Tillidstjenester

If Den Danske Stat Tillidstjenester stops issuing user 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.