Den Danske Stat Tillidstjenester

The Danish State Trust Services

Terms and conditions for signatures based on qualified person certificates

Version 1.2
October 11 / 2022

AGENCY FOR DIGITAL GOVERNMENT
MINISTRY OF FINANCE

Content

1 Introduction and purpose

These terms and conditions regulate private individuals' creation of electronic signature (in the following 'signature') on documents and other data at self-service solutions connected to the signing solution in NemLog-in.

The terms and conditions must be accepted in the signing solution before a signature can be created.

Unless otherwise stated, these terms and conditions also apply to the issuance of time stamps linked to the signature.

Creation of a signature in the signing solution requires that you as a private individual is able to authenticate yourself via your private MitID.

You must treat your MitID is accordance with the applicable rules and terms and condition (End-User Terms and Conditions for MitID) and that can be accepted in connection with the issuance of an MitID.

Signatures and time stamps in signing solutions are issued by the Danish State Trust Services represented by the Danish Agency for Digital Government.

2 Description of the signing solution

The signing solution supports signing documents and other data.

The signature is a qualified electronic signature that is recognised in the EU and the EEA. Accordingly, the Danish State 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 signature provided is therefore enforceable throughout Europe in the same way as a physical signature.

A certificate is issued when you use the solution, which then forms part of the signature. Besides various technical information, the certificate contains your name and a unique serial number and ensures that it can subsequently be verified that it is you who has provided the signature.

The certificate can only be used for providing one signature. A new certificate will be issued the next time you provide a signature.

The time stamps used are qualified and are recognised in the EU and the EEA. The time stamp documents the time of the signature, including that the certificate and the signed data were available at the time of signing. 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 1.1.

These terms and conditions have been prepared in accordance with the Public Certificate Policy for Qualified Person Certificates, version 1.1, which forms the basis for the Danish Agency for Digital Government's issuance of qualified person certificates.

The certificate policy and the policy for time-stamping is available at certifikat.gov.dk.

A detailed description of the trust services (Practice) is available at www.CA1.gov.dk.

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

3 Contact information

Danish Agency for Digital Government
Attn. Den Danske Stat Tillidstjenester
Landgreven 4
DK-1301 Copenhagen K
Tel. (+45) 3392 5200
info@ca1.gov.dk
CVR: 34051178

4 The legal validity of an electronic signature

A qualified electronic signature from the signing solution provided by you as a natural person is binding in the same way as your physical signature. It is therefore important that you are aware of what you are signing when you provide your signature.

The signature is universally recognised in the EU and the EEA and has equal status with physical signatures.

The time stamp ensures that it can be documented when the signature was provided as well as which document or other data that was signed at that given time. An electronic time stamp shall not be denied legal effect and admissibility as evidence in legal proceedings solely on the grounds that it is in an electronic form.

5 Applications

5.1 General application

Signatures with accompanying certificates from the signing solution can be used for statements of intent and entering into agreements with both natural and legal persons including public authorities and public law bodies.

It is only possible to sign documents and other data online at service providers who are part of the signing solution. It is not possible to use the signing solution to sign emails or for encryption.

No limitations have been made for the type of agreements or obligations you can enter into by using a signature from the signing solution.

5.2 Validity period of the certificate

The certificate is valid for 10 days. However, the technical solution ensures that it is not possible to generate multiple signatures based on the same certificate. The 10 day validity period after the signature has been created is solely based on technical concerns for the systems that will subsequently be reading the signature.

5.3 Certificate revocation list

Information about the status of issued certificates can be accessed from time to time via the signing solution's certificate revocation list at https://www.ca1.gov.dk/crls/

6 Availability of the signing solution

6.1 Signing solution

The signing solution and related services are available all day, all year.

However, the Danish Agency for Digital Government cannot be held liable for the above accessibility being provided.

7 Your obligations on provision of an electronic signature

7.1 Updated and correct information about you

Before you provide the signature, the signing solution will display you your name. The signing solution retrieves this information from your MitID.

You must make sure that your name is correct as it is included in the signature and the related certificate to document that you have provided the signature.

When you approve the signing in question, you also accept the certificate and that the information stated about your name is correct.

If the information is not correct, you must terminate the signing process and update your MitID in accordance with the relevant rules.

7.2 Use of signature generating data

You cannot use signature generating data (the private key) to sign other certificates.

7.3 Protection of authenticator

You must protect your MitID and related security mechanisms (e.g. password and MitID App) that you use for providing the signature in accordance with the applicable terms and conditions to ensure that reasonable measures have been taken to prevent a signature being given in your name by other entities than yourself.

If you suspect that your MitID has been compromised, you must suspend or revoke it in accordance with the End-User Terms and Conditions for MitID (terms and conditions for MitID) and terms for private individuals' possession of MitID, cf. § 8 of the executive order on MitID for private individuals to prevent any unauthorised use of your MitID by other entities that yourself for providing a signature in your name.

7.4 Notification of the Danish Agency for Digital Government and revocation of certificate

Generally, you never need to revoke a certificate from the signing solution.

However, you are obligated to notify the Danish Agency for Digital Government immediately and revoke your certificate if you identify inaccuracies or changes to data that is included in the certificate before the expiry of the validity period of the certificate, cf. clause 5.2.

You can revoke a certificate via https://spaer.ca1.gov.dk. You can revoke a certificate at any time of the day. You can also send a request for revocation by physical mail to the address of the Danish Agency for Digital Government as stated in clause 3.

Revocation of a previously used certificate does not prevent you from having a new certificate issued for providing a new signature.

If you suspect that your MitID has been compromised, you must revoke it in accordance with the relevant terms and conditions to prevent any unauthorised use for providing a signature in your name, cf. clause 7.3 above.

7.5 Protection on a qualified electronic signature generation device (QSCD)

The signature solution ensures that the signature you provide is generated with a high degree of security and is linked to the document or other data you are being shown in the self-service solution.

For this purpose, the Danish Agency for Digital Government uses a cryptographic module (QSCD), which means that the signature generating data remains at your control during the signing process.

8 Obligations as relying party

Besides trusting a certificate, the relying party receiving a signature from the signing solution must ensure the following:

- that the certificate is valid and has not been revoked – i.e. is not listed on the Danish State Trust Services' certification revocation list;
- 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 the certificate policy, cf. clause 2.

Before a time stamp is accepted, the relying party 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;
- That use is within any limitations on the use of the time stamp indicated by the time-stamp policy; and
- That any other precautions prescribed in agreements or elsewhere are observed.

Unless warranted by other circumstances, a signature from the signing solution will be valid allowing the relying party to rely on it even though the certificate after the provision of the signature has expired or been revoked.

Detailed information about the relying party's obligations is stated in 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.

9 Support

Questions regarding the document or data being signed shall be directed to the service provider responsible therefor. Similarly, questions related to the digital self-service solution used shall be addressed to the service provider.

Support for the process in the signing client can be addressed to NemLog-in support (https://www.nemlog-in.dk/support/).

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

10.1 Registration of data on provision of signature

When you provide a signature and a certificate is created, the Danish Agency for Digital Government registers various data about you, the certificate and the service provider where the signature has been used.

The following is registered:

- Time of signing
- Your name (first and last name)
- Your age
- The NSIS Level of Assurance you are authorised at towards the service
- CPR/session UUID
- Reference text
- Technical information related to the authentication (SAML assertion)

10.2 Data storage

The Danish Agency for Digital Government stores data about you and your use of Signatures and certificates from the signing solution for 7 years from the time of signing. Data about the accepted terms and conditions on use of the signature is also stored.

Storage is done to uphold a high level of privacy, investigation and for use as evidence in any legal proceedings. All data related to a signature is erased continuously as the seven-year expiry date of a certificate is reached.

10.3 Data that is not registered

The Danish Agency for Digital Government does not register which document or which data you have signed in the signing solution.

10.4 Publication of the certificate

Certificates from the Danish State Trust Services are not published in a public register. The certificate is only embedded in the signature.

11 Processing of personal data

11.1 Privacy policy

Read the Danish Agency for Digital Government's privacy policy for NemLog-in (https://digst.dk/it-loesninger/nemlog-in/om-loesningen/persondata/) for more information about which data the Danish Agency for Digital Government collects, stores and processes about you in connection with issuance of certificates and provision of signatures.

11.2 Data control

The Danish Agency for Digital Government is the controller of the personal data being processed by the signing solution. Nets Dan ID A/S is the processor for the Danish Agency for Digital Government.

The processing of your 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 7 years.

12 Electronic communication

By accepting these terms and conditions, you also allow the Danish Agency for Digital Government to contact you by email in connection with the operation of the signing solution. Enquiries may concern operation-related information, security-related matters, changes and termination.

13 Liability on provision and receipt of an electronic signature

13.1 Subscriber's liability

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, issuance and revocation of the certificate.

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

13.2 Liability of the recipient of electronically signed data

The Danish Agency for Digital Government is liable to anyone who reasonably rely on a qualified electronic signature from the signing solution under the general rules of Danish law unless the Danish Agency for Digitisation 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 Digitisation's liability comprises any loss due to the Danish Agency for Digitisation having made errors in connection with registration, issuance and revocation of the certificate.

The Danish Agency for Digital Government's liability to legal persons, including public authorities and public law bodies 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 all matters that arise from the same continued or repeated actionable matter.

13.3 Liability for provision of time stamp

The provisions stated under clauses 13.1 and 13.2 also apply to the Danish Agency for Digital Government's provision of time stamps.

14 Amendment of terms and conditions

The Danish Agency for Digital Government is entitled to amend these terms and conditions for signatures created after the am amendmend without notice. In the event of amendments, you will be asked to accept the updated terms and conditions the next time you want to provide a signature.

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 signatures and certificates issued by the Danish Agency for Digital Government must be brought before the City Court of Copenhagen.

16 Termination of Den Danske Stat Tillidstjenester

The Danish Agency for Digital Government is entitled to transfer all information and obligations under these Terms to another legal entity, including a public authority or a body governed by public law, which is entrusted with the continued management or termination of the Danish State Trust Services.