Agency for Digital Government

TERMS AND CONDITIONS FOR SIGNATURES BASED ON QUALIFIED PERSONAL CERTIFICATES

Version: 1.3

Author: Agency for Digital Government, Den Danske Stat Trust Services

Publication Date: March 2026

Den Danske Stat Trust Services

Table of Contents

1. Introduction and Purpose 4
2. Description of the Signing Solution 4
3. Contact Information 5
4. The Legal Validity of an Electronic Signature 5
5. Use Cases 6
   5.1. General Use 6
   5.2. Validity Period of the Certificate 6
   5.3. Revocation List 6
6. Availability of the Signature Solution 6
   6.1. The Signing Solution 6
7. Your Obligations When Making an Electronic Signature 7
   7.1. Up-to-date and Correct Information About You 7
   7.2. Use of Signature Creation Data 7
   7.3. Protection of Authenticator 7
   7.4. Notification of the Agency for Digital Government and Revocation of Certificate 7
   7.5. Protection on a Qualified Electronic Signature Creation Device (QSCD) 8
8. Obligations as a Recipient of a Signature 9
9. Support 9
10. Registration of Information by the Agency for Digital Government 10
   10.1. Registration of Information When Making a Signature 10
   10.2. Storage of Data 10
   10.3. Information Not Registered 10
   10.4. Publication of the Certificate 10
11. Processing of Personal Data 11
   11.1. Privacy Policy 11
   11.2. Controllership 11
12. Electronic Communication 11
13. Liability in Connection with Making and Receiving an Electronic Signature 11
   13.1. Liability for the Holder of a Certificate 11
   13.2. Liability for the Recipient of Digitally Signed Data 11
   13.3. Liability in Connection with Issuing a Time Stamp 12
14. Amendment of Terms and Conditions 12

15. Governing Law and Disputes 12
16. Termination and Transfer of Den Danske Stat Trust Services 12

The terms and conditions are written in Danish and translated into English. The Danish-language version shall be authoritative in all respects and shall prevail in the event of any inconsistency with the English translation.

1.Introduction and Purpose

These terms and conditions regulate private users' making of an electronic signature (hereinafter 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 made.

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

Making a signature in the signature solution requires that you, as a private user, can authenticate yourself with your private MitID.

You must handle your MitID in accordance with the rules and terms and conditions (MitID End User Terms and Conditions, also known as terms and conditions for MitID) applicable thereto, and which are accepted in connection with the issuance of a MitID.

Signatures and time stamps in the signing solution are issued by Den Danske Stat Trust Services (CA1) at the Agency for Digital Government.

2.Description of the Signing Solution

The signing solution supports the making of a signature on documents and other data.

The signature is a qualified electronic signature recognised in the EU and the EEA. Den Danske Stat thus acts as a qualified trust service provider as further described 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, as amended by Regulation (EU) No 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. Electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (the eIDAS Regulation). The signature made therefore has legal effect throughout Europe in the same way as a handwritten signature.

When you use the solution, a certificate is issued which is subsequently included in the signature. In addition to a number of technical details, the certificate contains your name and a unique serial number and ensures that it can subsequently be ascertained that it was you who made the signature.

The certificate may only be used for making one signature. The next time you need to make a signature, a new certificate will be issued.

The time stamp used is qualified and is recognised in the EU and the EEA. The time-stamping documents the time of the making of the signature, including that a certificate and the signed data were present at the time of signing. The qualified time stamp combined with the electronic signature is issued on the basis of the Agency for Digital Government's Public Policy for Qualified Time-Stamping, version 1.2.

These terms and conditions have been prepared in accordance with the Combined Public Certificate Policy for OCES and Qualified Certificates version 8.0, which forms the basis for the Agency for Digital

Government's issuance of qualified personal certificates. Den Danske Stat Trust Services is approved by the Agency for Digital Government as an issuer of qualified certificates, cf. the eIDAS Regulation.

The certificate policy and the time-stamping policy can be read at:

https://certifikat.gov.dk/

Den Danske Stat Trust Services issues other types of certificates for use in a business context, which are subject to separate terms and conditions.

A detailed description of the trust services can be read at:

https://www.ca1.gov.dk/

3.Contact Information

Agency for Digital Government
Att. Den Danske Stat Trust Services
Landgreven 4
1301 Copenhagen K

Tel. (+45) 3392 5200

E-mail: **info@ca1.gov.dk**

CVR: 34051178

4.The Legal Validity of an Electronic Signature

A qualified electronic signature from the signature solution made by you as a natural person is binding in the same way as your handwritten signature. It is therefore essential that you pay attention to what you are signing when you make the signature.

The signature has uniform recognition in the EU and the EEA and is treated as equivalent to a handwritten signature.

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

5.Use Cases

5.1.General Use

Signatures with associated certificates from the signing solution may be used for making declarations of intent and for entering into agreements with both natural and legal persons, including public authorities and public organisations.

It is only possible to sign documents and other data online at Service Providers connected to the signing solution. It is not possible to use the signing solution to sign emails or for confidentiality purposes (encryption).

There are no limitations on the types of agreements and obligations you may enter into by using a signature from the signing solution.

5.2.Validity Period of the Certificate

The certificate has a validity period of either 12 hours or 10 days. However, the technical solution ensures that it is not possible to generate multiple signatures on the basis of the same certificate. The validity period of 10 days following the making of the signature is solely due to technical considerations relating to the systems that subsequently need to read the signature.

5.3.Revocation List

Information on the status of issued certificates may be accessed at any time via the signature solution's revocation list at:

https://www.ca1.gov.dk/tilbagekald-certifikater

6.Availability of the Signature Solution

6.1.The Signing Solution

The signing solution and associated services are available around the clock every day of the year. However, the Agency for Digital Government is not responsible for ensuring that the above availability is delivered.

In the event of operational disruptions, the Agency for Digital Government provides information at:

https://www.digitaliser.dk/nemlog-in

7. Your Obligations When Making an Electronic Signature

7.1. Up-to-date and Correct Information About You

Prior to making the signature, your name is presented to you in the signature solution. The signing solution obtains this information from your MitID.

You must ensure that your name appears correctly, as it is included in the signature and the associated certificate for the purpose of documenting that the signature was made by you.

By approving the signing in question, you simultaneously accept the certificate and that the stated information about your name is correct.

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

7.2. Use of Signature Creation Data

You may not use signature creation data (the private key) for signing other certificates.

7.3. Protection of Authenticator

You must protect your MitID and associated security mechanisms (e.g. passcode and MitID app) that you use for the purpose of making the signature, in accordance with the terms and conditions applicable thereto, so that reasonable precautions have been taken to ensure that a signature is not made in your name by anyone other than yourself.

If you suspect that your MitID has been compromised, you must suspend or block it in accordance with the MitID End User Terms and Conditions (terms and conditions for MitID) and the conditions for private users' possession of MitID, cf. clause 8 of the Executive Order on MitID for private users, so as to prevent your MitID from being used without authorisation by anyone other than yourself to make a signature in your name.

7.4. Notification of the Agency for Digital Government and Revocation of Certificate

As a general rule, you will never need to revoke a certificate from the signing solution.

However, you are obliged to immediately notify the Agency for Digital Government and revoke your certificate if you discover inaccuracies or changes to data included in the certificate before expiry of the certificate's validity period, cf. clause 5.2.

Revocation of a certificate must be done via:

https://spaer.ca1.gov.dk/

Revocation can be done around the clock. You may also send a request for revocation by physical post to the address of the 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 the purpose of making a new signature.

7.5. Protection on a Qualified Electronic Signature Creation Device (QSCD)

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

For this purpose, the Agency for Digital Government uses a so-called cryptographic module (QSCD), whereby the signature creation data remains under your control during the signing process.

8.Obligations as a Recipient of a Signature

Before relying on a certificate, the recipient of a signature from the signing solution must ensure the following:

- That the certificate is valid and not revoked – i.e. not listed on Den Danske Stat Trust Services' revocation list,
- that the purpose for which the certificate is sought to be used is appropriate in relation to any use restrictions in the certificate, and
- that the use of the certificate is otherwise appropriate in relation to the level of security described in the certificate policy, cf. clause 2.

Before a time stamp is accepted, the recipient of a signature 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 verification,
- that the use is within any limitations on the use of the time stamp specified in the time-stamping policy, and
- that other precautions specified in agreements or similar are fulfilled.

Unless other circumstances dictate otherwise, a signature from the signing solution will be valid, whereby the recipient may rely thereon, even if the certificate has expired or been revoked after the making of the signature.

Detailed information on the recipient's obligations is set out in the PKI Disclosure Statement, which is available at:

https://www.ca1.gov.dk/pds

The Agency for Digital Government has also included further information in the certificate on the use thereof, including a reference to the PKI Disclosure Statement.

Den Danske Stat describes matters relating to revocation information, including the period of availability, information in the event of compromise of the issuer's keys, and access to revocation information upon termination of the service in clauses 4.9 and 4.10 of the applicable Certification Practice Statement, which is available at:

https://www.ca1.gov.dk/efterlevelseserklaeringer/

9.Support

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

Support regarding the process in the signing client may be directed to NemLog-in support:

https://www.nemlog-in.dk/support/kontakt/

10. Registration of Information by the Agency for Digital Government

10.1. Registration of Information When Making a Signature

When you make a signature and a certificate is created, the Agency for Digital Government registers a number of items of information about you, the certificate and which Service Provider the signature has been used at.

The following is registered:

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

10.2.Storage of Data

The Agency for Digital Government retains data about you and your use of signatures and certificates from the signature solution for seven (7) years from the time of making a signature. Information on the accepted terms and conditions at the time of use of the signature is also retained.

Retention is carried out for the purpose of maintaining a high level of privacy protection, investigation and use as evidence, e.g. in legal proceedings. All data related to a signature is deleted on an ongoing basis when the seven-year deadline from the certificate's expiry date is reached.

10.3.Information Not Registered

The Agency for Digital Government does not register the data or documents that you have signed in the signature solution.

10.4.Publication of the Certificate

Certificates from Den Danske Stat Trust Services are not published in a publicly accessible register. The certificate exists solely embedded in the signature.

11.Processing of Personal Data

11.1.Privacy Policy

In the Agency for Digital Government's privacy policy for NemLog-in, you can read about what information the Agency for Digital Government collects, retains and processes about you in connection with the issuance of certificates and the making of signatures.

www.digst.dk/nemlog-in-privatlivspolitik

11.2.Controllership

The Agency for Digital Government is the controller for your personal data processed in the signing solution. IN Groupe Denmark A/S is the processor for the Agency for Digital Government.

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

Personal data is deleted after 7 years.

12.Electronic Communication

By accepting these terms and conditions, you simultaneously consent to the Agency for Digital Government contacting you by email in connection with the operation of the signing solution. Communications may, for example, concern operational information, security-related matters, amendments and termination.

13. Liability in Connection with Making and Receiving an Electronic Signature

13.1.Liability for the Holder of a Certificate

The Agency for Digital Government is liable under the general rules of Danish law for failure to fulfil these terms and conditions, including for losses caused by errors made by the Agency for Digital Government in connection with the registration, issuance and revocation of the certificate.

The Agency for Digital Government is obliged to bear the burden of proof for not having acted intentionally or negligently.

13.2.Liability for the Recipient of Digitally Signed Data

The Agency for Digital Government is liable for losses under the general rules of Danish law towards anyone who reasonably relies on a qualified electronic signature from the signature solution.

For the matters specified in the Certificate Policy requirement [REQ 9.6.1-02], the Agency for Digital Government is liable for losses unless the Agency for Digital Government can demonstrate that it has not acted intentionally or negligently.

The Agency for Digital Government's liability towards legal persons, including public authorities and public organisations, is in all cases limited to DKK 100,000 for each loss-causing event, and is in all cases capped at DKK 100,000 annually. A loss-causing event is deemed to include all circumstances arising from the same continued or repeated liability-incurring circumstances.

13.3.Liability in Connection with Issuing a Time Stamp

The above under clause 13.1 and clause 13.2 stated also applies to the Agency for Digital Government's issuance of time stamps.

14.Amendment of Terms and Conditions

The Agency for Digital Government is entitled to amend these terms and conditions without notice for signatures made after the amendment. If amendments are made, you will be asked to accept updated terms and conditions the next time you wish to make a signature.

15.Governing Law and Disputes

The legal relationship pursuant to these terms and conditions and the interpretation thereof shall be determined in accordance with Danish law.

Any dispute arising from the use of signatures and certificates issued by the Agency for Digital Government shall be brought before the Copenhagen City Court.

16.Termination and Transfer of Den Danske Stat Trust Services

The Agency for Digital Government is entitled to transfer all information and obligations under these terms and conditions to another legal entity, including a public authority or a body governed by public law, which is tasked with the continued administration of or the termination of Den Danske Stat Trust Services.