Agency for Digital Government

TERMS AND CONDITIONS FOR SHORT-TERM USER SIGNATURES

Version: 1.3

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

Publication Date: March 2026

This document also serves as Annex 4 to the Terms for User Organisations.

Den Danske Stat Trust Services

Table of Contents

These 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.User signatures in the Signing Solution

These terms and conditions regulate business users' provision of a qualified or OCESelectronic user signature (electronic signature) by using qualified user certificates or OCES user certificates issued by Den Danske Stat Tillidstjenester's signing solution for public and private Self-Service Solutions. Den Danske Stat Tillidstjenester is approved by the Agency for Digital Government as an issuer of qualified certificates pursuant to the eIDAS Regulation and OCES certificates.

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 Consolidated Public Certificate Policy for OCES and qualified certificates version 8.0, which forms the basis for the Agency for Digital Government's issuance of user certificates. The qualified time stamps linked with the electronic signature are issued based on the European standard, ETSI EN 319 421. Both the certificate policy and ETSI EN 319 421 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 is available at:

https://certifikat.gov.dk/

ETSI EN 319 421 is available at:

https://www.etsi.org/standards

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 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:

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

Further contact information is available at:

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

Part 1
Terms and conditions for the Subscriber

3.Legal validity of user certificates

Den Danske Stat Tillidstjenester acts as 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, 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). A qualified user signature that has been given has legal effect in the EU and EEA in the same manner as a physical signature. An OCES user signature that has been given has legal effect in Denmark in the same manner as a physical signature. OCES user signatures given on this basis are not necessarily recognised in the EU, but may not be denied legal effect and admissibility as evidence in legal proceedings in member states solely on the grounds that they are in electronic form, or that they do not meet the requirements for qualified user signatures.

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 – user signatures

4.1.General application

Auser certificate can be used when a natural person linked to a Legal Entity is to sign data with an electronic signature that is comparable to a physical signature and that must be universally recognised by all ember States, cf. clause 3.

The Signing Solution can only be used to provide a 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 Agency for Digital Government's Services related to issuing and validation of certificates are available 24/7/365.

The 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:

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

6.Obligations on using qualified user certificates

6.1.Updated and accurate information

The certificate holder must ensure that the information forming the basis for the issuance of a certificate is accurate and complete at the time of issuance. The information is based on the information already registered in MitID Erhverv.

6.2.Publication of the certificate

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

6.3.Validity period of the certificate

The certificate is valid for either 12 hours or 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.

6.4.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 respective revocation lists 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 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:

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

Moreover, the Agency for Digital Government has provided further information in the certificate on its use, 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 sections 4.9 and 4.10 of the applicable Certificate Practice Statement, which is available at:

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

8.Support

8.1.General support

Support requests regarding 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:

https://mitid-erhverv.dk/en/about-mitid-erhverv/contact-mitid-erhverv-support/

The 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 IN Groupe Denmark 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 Agency for Digital Government are covered by the Agency for Digital Government's Privacy Policy for MitID Erhverv. The Privacy Policy is available at:

https://mitid-erhverv.dk/en/about-mitid-erhverv/about-mitid-erhvervdk/privacy-policy-for-mitid-erhverv/

9.2.Data control

The 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. AEVEN A/S and IN Groupe Denmark A/S are the processor for the 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 + seven (7) years.

9.3.Registration of data

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

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

12.2.Liability to third parties

The Agency for Digital Government is liable to anyone who reasonably relies on a electronic signature from the Signing Solution under the general rules of Danish law

For the circumstances set out in Certificate Policy requirement 9.6.1-04, 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.

12.3.Limitations of liability

The 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 clause 12.1 to clause 12.3 also apply to the Agency for Digital Government's provision of time stamps.

13.Use restrictions

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

14.Changes to terms and conditions

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

If the 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 user certificates issued by Den Danske Stat Tillidstjenester under the 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 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 user certificates from Den Danske Stat Tillidstjenester.

For further information about the use of a business user for providing signatures, go to:

https://mitid-erhverv.dk/

16.2.Contact information

Den Danske Stat Tillidstjenester can be contacted at:

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

Further contact information is available at:

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

17. Obligations on using a user certificate

17.1. General conditions

The Subject's use of a user certificate for providing an electronic signature is done on behalf of the The Agency for Digital Government is not a party to such agreements and cannot be held liable for the actual use of user certificates.

The 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 an electronic 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 certificates

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 Agency for Digital Government's registration of data

18.1. Registration of data on creation and use of certificates

The 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
- Level of Identity Proofing (LoIP), cf. ETSI TS 119 461
- 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 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 seven(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.