DANISH AGENCY FOR DIGITAL GOVERNMENT

Erhverv

Annex 2
Terms and conditions for OCES user certificates

Content

1 Description of certificates in MitID Erhverv

These terms and conditions regulate the use of OCES user certificates issued by Den Danske Stat Tillidstjenester (The Danish State's Trust Services) (CA1) under the Danish Agency for Digital Government to User Organisations and their Users created in the MitID Erhverv solution to be used by the User Organisation's Users.

After the issuing of a user certificate, it will be linked to the user identity in MitID Erhverv.

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

OCES user certificates are issued based on the Danish Agency for Digital Government's Certificate Policy for OCES employee certificates (Public Certificates for Electronic Service), v.7.1. The certificate policy supplements these terms and conditions and therefore also applies to the relationship between the Subscriber and the Danish Agency for Digital Government. The certificate policy is available at https://certifikat.gov.dk/

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.

The terms and conditions for issuing and using OCES 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 the Users in the role as Subject are covered by 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.

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/

Part 1 Terms and conditions for the Subscriber

3 Legal validity of user certificates

An electronic signature provided with an OCES user certificate in Denmark has the same legal validity as an ordinary physical signature.

OCES certificates and signatures provided on the basis thereof are not acknowledged by members of the European Economic Area, but cannot be denied having legal effect in the member states and acknowledgement as proof in litigation, on the grounds that they are in an electronic form or that they do not meet the requirements for qualified electronic signatures.

OCES certificates are not qualified certificates and they must therefore not be used in situations where qualified certificates are required.

4 Applications – OCES user certificates

4.1 General application

OCES user certificates in MitID Erhverv are based on persistent certificates and are used when a physical person linked to a Legal Entity is to sign data using an electronic signature that is comparable to a physical signature.

The certificates offer a high degree of functionality and flexibility, and they can be used for authentication (towards services that specifically allow it), signing of emails and for encryption.

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

4.2 Use of pseudonym

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

5 Availability

5.1 General Services

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

However, 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 OCES user certificates

6.1 Publication of the certificate

The Subscriber's User Administrator decides whether certificates from MitID Erhverv should be published in Den Danske Stat Tillidstjenester's public certificate database (LDAP search engine) where it can be retrieved by third parties.

6.2 The Subject's acceptance of terms and conditions

In connection with the issuing of certificates to the Subject, the Subscriber must:

- ensure that the Subject accepts part 2 of these terms and conditions prior to the issuing of the certificate
- establish and document fixed processes for issuing certificates and ensure that the Subject's acceptance of the terms and conditions can be proven.

Processes and the documentation for the Subject's acceptance of the terms and conditions must be provided to the Danish Agency for Digital Government on demand.

The terms and conditions for Subjects stated in part 2 are available on MitID-Erhverv in a version that can be distributed in the User Organisation.

6.3 Protection of private key on creation

The Subscriber is obligated to provide the required technical basis and administrative checks to ensure that the private key is created securely and under the control of the Subject.

The Subject's keys must be created using an algorithm that observes the profile requirements specified in Certificate Profiles at https://www.ca1.gov.dk/efterlevelseserklaeringer/

As part of the technical basis and the administrative checks, the Subscriber must make sure that the Subject remains in control of its own key at all times.

6.4 Validity period of the certificate

The certificate is valid for 36 months. The certificate may no longer be used after expiry.

6.5 Revocation of certificate

The Subscriber must immediately revoke the certificate if the following situations occur before the expiry of the validity period of the certificate:

i. Access to the private key has been lost, including if it has been stolen or potentially compromised.
ii. Control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.
iii. Known or suspected compromise of the Subject's private key.
iv. Inconsistencies or changes are detected in data included in the certificate.
v. The Subject no longer has an association with the Subscriber.
vi. The Subscriber's bankruptcy or closing of its business

Use of the private key must cease if it is found to be compromised or is suspected to be compromised following a request for revocation, revocation notification or after expiry of the certificate except where use relates to decryption of data. However, the private key may always be used as the basis for authentication for the purpose of revocation.

Certificates are revoked in the MitID Erhverv solution.

Revocation of a previously used certificate does not prevent the issuing of a new certificate to the Subject.

7 The Danish Agency for Digital Government's right to revoke certificates

The Danish Agency for Digital Government is entitled to unilaterally revoke a certificate if the agency discovers or suspects that the Subscriber or Subject acts contrary to defined obligations or if the agency otherwise discovers or suspects that the private key has been compromised or destroyed.

In some cases, the revocation will take place according to defined processes, including if the Subscriber changes its name or closes its business.

The Danish Agency for Digital Government is also entitled to revoke certificates for security reasons or if technical errors are found related to the issuing of the certificate, which affects the proper use of the certificate.

8 Obligations as relying party receiving an electronic signature

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

- that the certificate is valid and has not been revoked – i.e. is not listed on the revocation list of Den Danske Stat Tillidstjenester
- 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, cf. clause 1.

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.

9 Support

9.1 General support

Support requests regarding issuing of 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.

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

10.1 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:

- The Subscriber's basic company data as registered in the MitID Erhverv solution
- Contact information of administrators
- Name, UUID, email and possibly civil registration number of the Subject
- Time of issuing the certificate
- All interactions with MitID Erhverv related to the certificate
- Data related to subsequent revocation and suspension of the certificate

If the Danish Agency for Digital Government closes down its CA service, the Danish Agency for Digital Government will be entitled to transfer registered data to a third party in accordance with the provisions stated in clause 12.

All data related to the Subscriber and Subject will be stored for 7 years from the expiry or revocation of the certificate.

10.2 Data that is not registered

The Danish Agency for Digital Government does not register data about the regular use of the certificate, including use of the certificate for providing signatures or encryption.

11 Processing of personal data

11.1 Privacy policy

Certificates from Den Danske Stat Tillidstjenester issued via MitID Erhverv 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/om/privatlivspolitik.dk.

11.2 Data control

The Danish Agency for Digital Government is the controller of the personal data being processed by 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.

11.3 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 22.

12 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.

13 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.

Den Danske Stat Tillidstjenester usually communicates matters electronically regarding the use of certificates to the Subscriber's Organisation Administrator and User Administrator.

14 Liability of the Danish Agency for Digital Government

14.1 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.

14.2 Liability to third parties

The Danish Agency for Digital Government is liable to anyone who reasonably relies on an electronic signature from the Danish Agency for Digital Government 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.

14.3 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 14.1 and 14.2, 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.

15 Use restrictions

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

16 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.

17 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

18 Introduction

18.1 General conditions

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

The terms and conditions must be accepted by the Subject prior to the issuing of an OCES user certificate via MitID Erhverv. The issuing takes place on behalf of the Subscriber to which the Subject is associated.

The terms and conditions have been approved by the Subscriber, which has also accepted the general terms and conditions for the use of OCES user certificates from the Danish Agency for Digital Government.

After the issuing of a user certificate, it will be linked to the User Identity of the Subject in MitID Erhverv.

18.2 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/

19 Use of OCES user certificate

The Subject's use of OCES user certificate is done on behalf of the Subscriber in accordance with the agreements entered into between the 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.

The Subject is obligated to protect the private key so as to prevent it being compromised, changed, lost or used by unauthorised parties. Accordingly, reasonable measures must be taken to protect security mechanisms, including choice of and protection of password. The Subject must always keep passwords secret to prevent them from being disclosed to other parties.

In connection with issuing and subsequent use of the private key, the Subject must ensure that it takes place in a manner that upholds self-control of the key.

The private key may not be used for signing other certificates.

20 Obligation on using OCES user certificates

20.1 Updated and correct information about you

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.

The Subject is obligated to revoke the certificate if the registered information changes during the lifetime of the certificate, cf. clause 20.3 below.

20.2 Obligations on provision of an electronic signature

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.

20.3 Revocation of certificate

The Subject must immediately ensure that the certificate is revoked if the following situations occur before the expiry of the validity period of the certificate:

i. Access to the private key has been lost, including if it has been stolen or potentially compromised.
ii. Control over the Subject's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons.

iii. Known or suspected compromise of the Subject's private key.
iv. Inconsistencies or changes are detected in data included in the certificate.

Use of the private key must cease if it is found to be compromised or is suspected to be compromised following a request for revocation, revocation notification or after expiry of the certificate except where use relates to decryption of data. However, the Subject may always use the private key as the basis for authentication for the purpose of revocation.

The Subject’s obligation under this provision to revoke the certificate can be observed immediately by contacting the Subscriber’s User Administrator, who will revoke the certificate in the MitID Erhverv solution.

21 The Danish Agency for Digital Government’s right to revoke certificates

The Danish Agency for Digital Government is entitled to unilaterally revoke a certificate if the agency discovers or suspects that the Subject acts contrary to its obligations or if the agency otherwise discovers or suspects that the private key has been compromised or destroyed.

22 The Danish Agency for Digital Government’s registration of data

22.1 Registration of data on creation and use of certificates

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

The following is registered:

- The Subscriber’s basic organisational data as registered in MitID Erhverv
- Contact information of administrators
- Name, UUID, email and possibly civil registration number of the Subject
- Time of issuing the certificate
- All interactions with MitID Erhverv related to the certificate
- Data related to subsequent revocation and suspension of the certificate

All data related to the Subscriber and Subject will be stored for seven (7) years from the expiry or revocation of the certificate.

22.2 Data that is not registered

The Danish Agency for Digital Government does not register data about the regular use of the certificate, including use of the certificate for providing signatures or encryption.

23 Termination of certificate service

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.