DANISH AGENCY FOR DIGITAL GOVERNMENT

Erhverv

Annex 3
Terms and conditions for OCES organisation certificates

Content

1 Description of certificates in MitID Erhverv

These terms and conditions regulate the use of OCES organizational certificates issued by Den Danske Stat Tillidstjenester (The Danish State's Trust Services) (CA1) under the Danish Agency for Digital Government for physical or logical entities in the User Organisation. An entity may comprise the entire User Organisation.

After the issuing of an organizational certificate, it will be linked to the organisation identity in MitID Erhverv.

In the following, the User Organisation is referred to as the Subscriber and the entity associated with the Subscriber who is registered and to whom a certificate is issued is named the Subject.

OCES organisation certificates are issued on the basis of the Danish Agency for Digital Government's Certificate Policy for OCES organizational certificates, 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 organisation certificate for the type of certificate that is referred to as organizational certificate in the certificate policy. The certificate policy's regulation of organizational certificates thus applies to the organisation certificates in these terms and conditions.

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/

3 Legal validity of organisation certificates

For an electronic seal based on an OCES organisation certificate, there is a presumption of the integrity of the data and the accuracy of the origin of the data to which the seal is linked.

OCES certificates and seals 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 comply with the requirements for qualified electronic seals.

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

4 Applications – OCES organisation certificate

4.1 General application

OCES organisation certificates in MitID Erhverv are issued with an associated and persistent certificate and are used when a Legal Entity needs to provide data with an electronic signature for the purpose of documenting the integrity and origin of such data.

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 organisation certificates issued by Den Danske Stat Tillidstjenester (CA1).

4.2 Naming the Subject in the certificate

The Subscriber's User Administrator determines the Subject's naming in the certificate.

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 certificates

6.1 Updated and correct information about you

The Subscriber must ensure that information that serves as basis for the issuing of a certificate is correct and complete at the time of issuing the certificate. The information is presented as part of the issuing process and is based on the information already registered in MitID Erhverv.

The Subscriber is required to revoke the certificate if the registered information changes during the lifetime of the certificate, cf. clause 6.7 below.

6.2 Obligations on provision of an electronic seal

Prior to providing an electronic seal, the Subscriber must check the content of the certificate and ensure that its use is within the limitations stated therein. The seal and its content are accepted on the seal generation in question.

6.3 Use of keys

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

The private key must be protected according to clause 6.5.

6.4 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.

6.5 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/practice/.

As part of the technical basis and the administrative checks, the Subscriber must make sure that the Subject always upholds self-control of its own key.

Please refer to clause 7 for further requirements for the documentation of the Subscriber's technical basis and administrative checks.

6.6 Validity period of the certificate

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

6.7 Notification of the Danish Agency for Digital Government and 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 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.

6.8 Limitations on naming the Subject

The specific naming of the Subject, cf. clause 4.2, may not be confusingly similar to a trademark. Moreover, the Danish Agency for Digital Government may order a Subscriber to stop using specific naming if the Danish Agency for Digital Government finds that such use may be offensive.

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 seal

Besides trusting a certificate, the relying party receiving an electronic seal 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 the certificate policy, cf. clause 1.

Unless warranted by other circumstances, an electronic seal 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 seal 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 organisation certificates, including general circumstances related to provision of an electronic seal and use of certificates can be made to MitID Erhverv Support on tel. +45 33980020 or via the contact form on www.mitid-erhverv.dk/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 the Subscriber and the subsequent use of certificates.

The following is registered:

- The Subscriber's basic company data as registered in the MitID Erhverv
- Contact information of administrators
- Subject's name, UUID and email
- 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 seven (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 electronic seals or encryption.

11 Processing of personal data

11.1 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 which 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 Dan ID 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 10.1.

12 Termination of Den Danske Stat Tillidstjenester

If Den Danske Stat Tillidstjenester stops issuing OCES organisation 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

The Danish Agency for Digital Government usually communicates electronically regarding the use of certificates to the Subscriber's Organisation Administrator and Identity Administrator.

In MitID Erhverv, the Subscriber can sign up for a special information service provided by the Danish Agency for Digital Government, allowing the Subscriber to receive information via mobile phone, including push notifications.

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 seal 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 of OCES organisation certificate

The Subscriber's use of OCES organisation certificates must be in accordance with what is stated below.

The key pair may only be used in accordance with the determined authorised use and not beyond any limitations notified to the Subscriber and Subject.

The Subscriber is required to protect the private key and prevent any authorised use. This must be done by observing the following:

a) that the choice of password ensures that they cannot be readily guessed through knowledge of the Subject,
b) that adequate measures are taken to protect the security mechanisms that protect the private key against compromise, change, loss and unauthorised use, and
c) that passwords are not disclosed to any other parties.

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

16 Use restrictions

The Danish Agency for Digital Government has set no restrictions for use of OCES organisation certificates, cf., however, clause 4 on limitations in the technical use of certificates.

17 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.

18 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 the Danish Agency for Digital Government must be brought before the City Court of Copenhagen.