

DANISH AGENCY FOR DIGITAL GOVERNMENT



Terms and conditions for user organisations in MitID Erhverv

The terms and conditions are written in Danish and English.

The Danish language version of terms and conditions shall be controlling in all respects and shall prevail in case of any inconsistencies with the English version, if any.

Content

Annexes	3
1 Introduction.....	4
2 Contact information	4
3 Definitions	4
4 Connection and acceptance of terms and conditions.....	7
4.1 Acceptance of terms and conditions.....	7
4.2 Registration in the Central Business Register.....	8
4.3 Appointment of Organisation Administrator by the Authorised Person	8
4.4 Connection based on migration from Nets DanID	8
5 User Organisation administrators	8
5.1 Creating administrators.....	8
5.2 Organisation Administrator.....	9
5.3 Rights Administrator.....	9
5.4 User Administrator	9
6 Connection and use of Local IdP	9
7 Services for User Organisations.....	9
7.1 Services.....	9
7.2 Creation of User Identities and acquisition of authenticators	9
7.3 Creation of user identities via Local IDM Service	10
7.4 Identity assurance on User Identity creation	10
7.5 Certificates for electronic signature	10
7.6 User rights administration.....	10
7.6.1 Rights of the User Organisation's Users	10
7.6.2 Digital Power of Attorney for businesses	10
8 Dedicated MitID Authenticators	10
8.1 Purchase of dedicated MitID Authenticators	10
8.2 Special rules for acquisition of MitID Authenticators	11
9 Certificates for electronic signature	11
9.1 Access to certificates via MitID Erhverv	11
9.2 Terms and conditions for the use of certificates.....	13
9.3 General information about Certificates	13
9.4 OCES certificates (Persistent)	13
9.5 Qualified certificates (Persistent).....	13
9.6 Qualified signatures (based on Short-term certificates)	14
9.7 Certificate policies	14
9.8 Validation of qualified electronic signatures and seals.....	14

10	Obligations of the User Organisation	14
10.1	Correct and updated information	14
10.2	Consistency with the Danish Central Business Register (CVR).....	15
10.3	Use of procedures and systems.....	15
10.4	Ensuring correct association between User Organisation and Business Users.....	15
10.5	Business Users' compliance with terms and conditions.....	15
10.6	Use of powers of attorney.....	15
10.7	Management of Authenticators	15
10.8	Reporting of security events	16
11	Processing of personal data	16
12	Service levels and availability	16
13	Support	16
14	System management.....	16
14.1	The Danish Agency for Digital Government's management unit.....	16
14.2	Suspension and revocation of the User Organisation.....	17
15	Fees.....	17
15.1	General	17
15.2	Fees for migration from Nets DanID	17
15.3	Invoicing and payment terms.....	17
16	Erasure and logging	17
17	Changes to rights regimes	18
18	Breach and remedies for breach	18
18.1	Remedial action.....	18
18.2	General information about termination	18
18.3	Termination by the Danish Agency for Digital Government	18
18.4	Suspension of the User Organisation's access to Services	19
19	General suspension of access to Services	19
20	Liability and limitation of liability	19
20.1	General information about liability.....	19
20.2	Liability for issuance of Separate MitID.....	19
20.3	Limitation of liability.....	20
20.4	Liability related to qualified certificates.....	20
21	Duty of confidentiality.....	20
22	Term and expiry.....	20
22.1	Term and termination	20
22.2	Changes	20
22.3	Expiry	21

23	Disputes	21
23.1	Governing law	21
23.2	Disputes, mediation and arbitration	21
23.3	Disputes relating to certificates issued by the Danish Agency for Digital Government.....	21

Annexes

Annex 1 Terms and conditions for dedicated MitID for Business Users

Annex 2 Terms and conditions for OCES User Certificates

Annex 3 Terms and conditions for OCES Organisation Certificates

Annex 4 Terms and conditions for qualified user signatures

Annex 5 Terms and conditions for qualified seals

Annex 6 Terms and conditions for physical MitID authenticators

Annex 7 Terms and conditions for use of Local IdP

1 Introduction

These terms and conditions regulate Legal Entities' connection to MitID Erhverv as a User Organisation. Legal Entities' connection to and use of MitID Erhverv is also regulated by the Danish Executive Order on MitID Erhverv and MitID Privat til Erhverv (MitID Private for Business) (Executive Order No. 1778 of 1 September 2021).

In MitID Erhverv, Legal Entities, in the role as User Organisation, can create, administer and use digital Business Identities and link and administer Authenticators to Business Users. Moreover, user rights can be assigned and administered for the Business Identities created.

MitID Erhverv is the national identity guarantee for Business Identities.

The creation of Business Identities in MitID Erhverv by a User Organisation allows Service Providers to receive information on when a Business Identity has been linked to the Authenticator used for authentication towards a Service Provider.

Information that Business Identities are available must be given to Service Providers connected to NemLog and brokers that entered into a separate agreement with Digitaliseringsstyrelsen for receipt of Business Identities via NemLog-in.

For further information about MitID Erhverv, reference is made to information on the MitID Erhverv Portal.

These terms and conditions replace the "Terms and conditions for using NemLog-in/User Administration".

All Services described in the terms and conditions are not necessarily available at the time of the User Organisation's acceptance of the terms and conditions. On the MitID Erhverv Portal, the User Organisation is required to check the descriptions of which Services are available and any time schedules for introducing new Services.

The terms and conditions include seven annexes. The annexes form an integral part thereof.

2 Contact information

The contact information of the Danish Agency for Digital Government is as follows:

Danish Agency for Digital Government
Landgreven 4
DK-1301 Copenhagen K
Tel. +45 3392 5200
mitiderhverv@digst.dk
CVR: 34051178

3 Definitions

Term	Definition
------	------------

Administrator	<p>Administrator is a generic term for the administrator roles (Organisation Administrator, User Administrator and Rights Administrator) that can be created in MitID Erhverv.</p> <p>An administrator role is always filled by a User.</p>
Authorised Person	<p>A representative from the Legal Entity (typically a management representative) that formally connects the entity as User Organisation in MitID Erhverv.</p> <p>The group of persons/entities that can act in the role as Authorised Person depends on the business type of the Legal Entity. Reference is made to the MitID Erhverv Portal for further information.</p>
Authenticator	<p>An Authenticator is a unit for online authentication by a user. The Authenticator must be under the control of the natural person or Legal Entity to which it was issued.</p>
Business User	<p>A natural person associated with a User Organisation and who is created with a User Identity in MitID Erhverv.</p>
Business Identity	<p>Business Identity is a collective term for User Identity and Organisation Identity. An Organisation Identity always has a CVR and RID attribute which together allow for unique identification of the Business Identity across organisations connected as User Organisations in MitID Erhverv.</p>
Certification Authority	<p>A natural person or legal entity generating, issuing and administering certificates in its capacity as trust service provider. The eIDAS Regulation uses the term trust service provider for this entity.</p> <p>On behalf of the Danish State, the Danish Agency for Digital Government is Certification Authority for the certificates issued via MitID Erhverv.</p>
Dedicated MitID Authenticator	<p>See Separate MitID.</p>
Digital Self-Service Solution	<p>An IT system through which private persons or Business Users may access digital self-service after having been authenticated.</p>
Legal Entity	<p>A Legal Entity means a legal entity with a business registration (CVR) number as set out in Section 3 of the Danish Act on the Central Business Register.</p>
Local IdP	<p>A local NSIS-notified authentication solution connected to NemLog-in that can authenticate Business Users from a User Organisation and convey the authentication response through NemLog-in to a Service Provider connected to NemLog-in.</p>
MitID Private for Business	<p>A private MitID used to represent a Legal Entity without a Business Identity being created in MitID Erhverv.</p> <p>MitID Private for Business can only be used by persons who are authorised to sign individually for a business.</p>

MitID Erhverv Portal	<p>The Danish Agency for Digital Government’s product site about MitID Erhverv aimed at User Organisations at www.mitid-erhverv.dk</p> <p>The MitID Erhverv Portal contains a description of the technical requirements for User Organisations' use of MitID Erhverv and a number of underlying policies. Any reference to the portal is also a reference to the technical requirements and underlying policies available on the portal.</p>
NemLog-in	The Danish Agency for Digital Government’s Identity Broker, from which authentication of digital identities is conveyed, including by using authenticators from NemID, MitID and Local IdPs.
Organisation Administrator	The top administrator in the User Organisation. The Organisation Administrator can conclude agreements on behalf of the User Organisation in NemLog-in.
Organisation Identity	<p>A Business Identity (organisation profile) under which OCES organisation certificates and qualified organisation certificates can be issued.</p> <p>No natural person is linked to an Organisation Identity.</p>
Persistent	A type of certificate issued in the Signing Solution via MitID Erhverv. A distinctive feature of the certificate is that it is valid for 36 months. An unlimited number of signatures and seals can be provided on the basis of the certificate which also offers a variety of uses.
Rights Administrator	A Rights Administrator is in charge of administering user roles, rights and Power of Attorney for businesses for Users in a User Organisation in MitID Erhverv.
Services	Services from the Danish Agency for Digital Government to be used by the User Organisation, including Business Identities, certificates, authenticators, rights management and the further obligations set out in the terms and conditions by which the Danish Agency for Digital Government is governed.
Signing solution	<p>The Danish Agency for Digital Government's signing solution, which enables for signatures and seals to be submitted via service providers.</p> <p>Signatures and seals in the Signing Solution are based on Short-term certificates.</p>
Separate MitID	A separate MitID Authenticator issued to a Business User in the User Organisation for the exclusive use by the Business User as a representative of the User Organisation. Also called Dedicated MitID
Subscriber	A natural or legal person who concludes an agreement with the Certification Authority (CA) on issuing of certificates to one or more Subjects.
Subject	A natural person or entity with a Subscriber who is identified in the certificate as the proper user of the private key belonging to the public key granted in the certificate, and to whom a certificate is either being issued or has already been issued.

Short-term	<p>A type of certificate issued in the Signing Solution where the private key is deleted immediately after the signature is provided and where the certificate expires after 10 days.</p> <p>Short-term certificates can only be used to provide an electronic signature and not for encryption and secure email.</p>
System Administrator	<p>A System Administrator is an employee of the Danish Agency for Digital Government or the service provider of the Agency who on the basis of administrative privileges can perform the certain actions on behalf of a User Organisation as the other administrators of the organisation.</p> <p>All actions performed by a System Administrator on behalf of a User Organisation are logged so that they may be related to the Employee who executed them.</p>
User	<p>Business User associated with a User Organisation. A formal employment relationship between the User and User Organisation is not a requirement.</p>
User Organisation	<p>A Legal Entity connected to MitID Erhverv.</p>
User Data	<p>User data is information about the Business Users in the User Organisation and includes name, civil registration number (CPR), email and telephone number and the rights assigned to the Business Users.</p> <p>User data is added and administered in MitID Erhverv by a User Administrator.</p>
User Identity	<p>Electronic identity issued to a natural person associated with a User Organisation.</p>
User Administrator	<p>A User Administrator in MitID Erhverv is in charge of creating and administering the Business Users of a company and any linked Authenticators.</p>
Qualified Certificate	<p>A certificate that is a 'Qualified Certificate for Electronic Signature' or a 'Qualified Certificate for Electronic Seal' as defined in Article 3(15) and (30) of the eIDAS Regulation.</p>

4 Connection and acceptance of terms and conditions

4.1 Acceptance of terms and conditions

The terms and conditions must be accepted by the Authorised Person on behalf of the Legal Entity. On acceptance of the terms and conditions, the Authorised Person declares that the Legal Entity will comply with the terms and conditions. The obligations of the Danish Agency for Digital Government towards the User Organisation start when the User Organisation accepts the terms and conditions.

The Authorised Person must undertake such a role in the User Organisation that allows representation of the User Organisation towards the Danish Agency for Digital Government, including in relation to acceptance of terms and conditions.

4.2 Registration in the Central Business Register

It is a precondition for creating a User Organisation in MitID Erhverv that the Legal Entity is registered in the Danish Central Business Register (CVR).

4.3 Appointment of Organisation Administrator by the Authorised Person

As part of the connection process, the Authorised Person must appoint at least one Organisation Administrator, cf. clause 5.2. On appointment, the Authorised Person accepts and agrees that the Organisation Administrator, on behalf of the User Organisation, is authorised to perform the tasks set out for the Organisation Administrator, including to serve as the point of contact for the Danish Agency for Digital Government in relation to notification of updates to terms and conditions and otherwise entering into agreements with binding effect for the Danish Agency for Digital Government in MitID Erhverv on behalf of the User Organisation, cf. clause 5.2 and clause 22.2.

The Authorised Person is allowed to appoint herself as Organisation Administrator.

4.4 Connection based on migration from Nets DanID

If the User Organisation is connected as part of a migration from the NemID Employee Signature solution with Nets DanID, then all or selected employees can be transferred to MitID Erhverv after acceptance of these terms and conditions and acceptance of migration.

As part of the migration, registered employees in the NemID Employee Signature solution are created as User Identities in MitID Erhverv and on transfer, they will be in a temporarily suspended state.

It is the responsibility of the Organisation Administrator to check that all transfers have been done correctly, after which the Organisation Administrator will select the user registrations to be created as User Identities. The formal creation of a User Identity is based on an acceptance from the individual User who is at the same time notified of the transfer of personal data from Nets DanID to MitID Erhverv.

Reference is made to clause 15 for a detailed description of the prices of creating the User Organisation on migration from the NemID Employee Signature solution.

5 User Organisation administrators

5.1 Creating administrators

The day-to-day administration of the User Organisation is undertaken by three administrators:

- Organisation Administrator
- Rights Administrator
- User Administrator

The administrators appointed by the User Organisation must not have been convicted of a crime that makes them unsuitable for performing the job as administrator.

In order to be appointed as administrator, it is a prerequisite that the User in question is registered as a Business User with the User Organisation.

It is the responsibility of the User Organisation to make sure that the appointment of administrators is in accordance with the internal signing authority of the User Organisation.

5.2 Organisation Administrator

After being appointed, the Organisation Administrator is the top representative of the User Organisation in MitID Erhverv. The User Organisation must ensure that it is always represented by at least one Organisation Administrator associated with the Legal Entity. If, for instance due to termination of employment, the Legal Entity is no longer represented by an Organisation Administrator, an Authorised Person will have to appoint a new Organisation Administrator.

The requirements for verification of an Authorised Person when it comes to appointing a new Organisation Administrator are the same as the requirements when the Legal Entity was initially connected.

The Organisation Administrator is responsible for appointing other administrators and for configuring business data and administration preferences in MitID Erhverv.

The Organisation Administrator can appoint itself in the role as rights administrator and User Administrator, and the other administrators may be one and the same person.

5.3 Rights Administrator

The Rights Administrator may assign and administer rights for the registered Business Identities and may also appoint other Rights Administrators with similar rights.

5.4 User Administrator

The User Administrator creates Business Identities in the form of User Identities and Organisation Identities which are linked to the business registration (CVR) number of the Legal Entity.

On creation of a Business Identity, the User Administrator specifies whether the creation concerns a User Identity or an Organisation Identity and whether a certificate or Authenticator should be linked to the identity.

When creating User Identities, the User Administrator must consider which Authenticator to link, cf. clause 7.2.

6 Connection and use of Local IdP

The User Organisation can via MitID Erhverv connect a Local IdP to NemLog-in for the purpose of linking authenticators from the Local IdP to the User Identities created in MitID Erhverv so that such Authenticators can be used as authentication towards Service Providers.

The connection and use of a Local IdP is subject to terms and conditions set out in Annex 7.

7 Services for User Organisations

7.1 Services

Via MitID Erhverv, the User Organisation has access to a number of Services These are described in clause 7.2 to clause 7.3 below.

7.2 Creation of User Identities and acquisition of authenticators

The User Organisation can create User Identities for natural persons who, as Business Users, may represent the User Organisation towards third parties.

The User Organisation is to link one of the following Authenticators to the User Identity:

- The Business User's private MitID Authenticator

- A Separate MitID Authenticator
- An Authenticator from a Local IdP (requires the User Organisation to have a linked Local IdP from which it issues authenticators)

The Business User's private MitID Authenticator can only be linked to the User Identity if both the User Organisation and the Business User has agreed to this (the double principle of voluntariness). The acceptance from the Business User must be based on an individual consent obtained by the User Organisation.

As part of the issuance of a Separate MitID Authenticator, the Business User must accept the terms and conditions from MitID set out in Annex 1.

The purchase of MitID Authenticators by the User Organisation must be in accordance with clause 8.

7.3 Creation of user identities via Local IDM Service

The User Organisation can create Business Users and maintain related rights in MitID Erhverv via a Local IdM solution. Further requirements for integration of the IdM solution are set out on the MitID Erhverv Portal.

7.4 Identity assurance on User Identity creation

In order to create a User Identity, the relevant User must be identity assured and authenticated as a natural person with an NSIS-notified eID which can be received by MitID Erhverv. The eID used must as a minimum support an authentication at NSIS assurance level Substantial. MitID and NemID can be used as basis for identity assurance.

7.5 Certificates for electronic signature

In MitID Erhverv, the User Organisation can create and administer certificates for electronic signature.

Detailed provisions about certificates are described in clause 9.

7.6 User rights administration

7.6.1 Rights of the User Organisation's Users

A User Organisation can assign and administer rights to its own User Identities for the purpose of using Public Self-Service Solutions.

7.6.2 Digital Power of Attorney for businesses

A User Organisation can use MitID Erhverv to assign rights (also known as Power of Attorney for businesses) to a User Organisation or another Business User in another User Organisation with another business registration (CVR) number.

The Power of Attorney for businesses is assigned for specific public self-service solutions.

8 Dedicated MitID Authenticators

8.1 Purchase of dedicated MitID Authenticators

MitID Authenticators can be ordered by the User Organisation via MitID Erhverv. The User Organisation's purchase of MitID Authenticators is made with Nets DanID A/S as a party to the agreement in accordance with the terms and conditions set out in Annex 6. The Danish Agency for Digital Government is not a party to agreements on purchase of MitID Authenticators.

8.2 Special rules for acquisition of MitID Authenticators

MitID Authenticators may only be acquired for the User Organisation's own Users. MitID Authenticators may not be purchased for any third party. Reselling of Authenticators is not allowed.

9 Certificates for electronic signature

9.1 Access to certificates via MitID Erhverv

In MitID Erhverv, the User Organisation can create and administer certificates for electronic signature. Certificates in MitID Erhverv are Persistent certificates.

In addition, Business Users may use their User Identity to provide electronic signatures and electronic seals in the Danish Agency for Digital Government's Signing Solution. Certificates in the Signing Solution follow the Short-term model.

Certificates and time stamps to be used for electronic signature are issued by Den Danske Stat Tillidstjenester (CA1) provided by the Danish Agency for Digital Government.

Via MitID Erhverv, there is general access to the following certificates issued by Den Danske Stat Tillidstjenester (CA1):

ID	Certificates and signature types	Characteristics
A	<p>OCES organisation certificate (Persistent)</p> <p>Issued according to the certificate policy for OCES organizational certificates, cf. clause 9.7.</p>	<p>Certificate to be used for electronic signature for businesses. No personal names are linked to the certificate.</p> <p>An organisation certificate is used by machines and programs to communicate securely on behalf of a business. A business signature is a guarantee to the relying party that it is communicating with the business specified on the certificate. An OCES organisation certificate and the related private key can also be used to sign emails and encrypt data</p>
B	<p>OCES user certificate (Persistent)</p> <p>Issued according to the certificate policy for OCES employee certificates, cf. clause 9.7.</p>	<p>Certificate to be used for electronic signature for natural persons associated with Legal Entities.</p> <p>OCES user certificates can be used when natural persons are to sign electronically and authenticate themselves as associated with a given organisation.</p> <p>An OCES user certificate and the related private key can be used to sign emails and encrypt data</p>

ID	Certificates and signature types	Characteristics
C	<p>Qualified user signature (Short-term)</p> <p>Issued according to the certificate policy for qualified employee certificates, cf. clause 9.7</p>	<p>Certificate to be used for qualified electronic signatures for natural persons associated with Legal Entities.</p> <p>User certificates can be used when a natural person associated with a Legal Entity is to sign data with a qualified electronic signature that is comparable to a physical signature.</p> <p>A qualified electronic signature based on a Short-term certificate cannot be used to sign emails or encrypt data.</p> <p>The signatures provided are based on non-persistent private keys. This means that the underlying cryptographic keys are created for the specific occasion in a central qualified signature creation device (QSCD) and the private key is deleted immediately after each electronic signature has been created.</p>
D	<p>Qualified user certificate issued in a local qualified signature creation device (QSCD) (persistent)</p> <p>Issued according to the certificate policy for qualified employee certificates, cf. clause 9.7.</p>	<p>Certificate to be used for qualified electronic signatures for natural persons associated with Legal Entities.</p> <p>User certificates can be used when a natural person associated with a Legal Entity is to sign data with a qualified electronic signature that is comparable to a physical signature.</p> <p>A qualified user certificate issued on a local QSCD can be used to sign emails and encrypt data.</p> <p>Signatures are based on a private key which is protected by a local qualified signature creation device (QSCD).</p>
E	<p>Qualified seal (Short-term)</p> <p>Issued according to the certificate policy for qualified organizational certificates, cf. clause 9.7.</p>	<p>Certificate to be used for qualified electronic seals for Legal Entities. No personal names are linked to the certificate.</p> <p>Qualified seals can be used when a Legal Entity is to provide data with a qualified electronic seal that is comparable to a physical signature</p> <p>A qualified seal based on a Short-term certificate cannot be used to sign emails or encrypt data.</p> <p>The seals provided are based on non-persistent private keys. This means that the underlying cryptographic keys are created for the specific occasion in a central qualified signature creation device (QSCD) and the private key is deleted immediately after each electronic signature has been created.</p>

ID	Certificates and signature types	Characteristics
F	<p>Qualified organisation certificate issued in a local qualified seal creation device (QSCD) (Persistent)</p> <p>Issued according to the certificate policy for qualified organizational certificates, cf. clause 9.7.</p>	<p>Certificate to be used for qualified electronic seals for Legal Entities. No personal names are linked to the certificate.</p> <p>Qualified seals can be used when a Legal Entity is to provide data with a qualified electronic seal for the purpose of documenting the integrity and origin of such data.</p> <p>A qualified organisation certificate can be used to sign emails and encrypt data.</p> <p>Signatures are based on private keys which are protected by a local qualified signature creation device (QSCD).</p>

9.2 Terms and conditions for the use of certificates

Specific terms and conditions for each individual type of certificate and signature, cf. clause 9.1 above, are included as annexes to these terms and conditions. In the role as Subject, the Business User must separately accept certain parts of the terms and conditions prior to issuing persistent user certificates in MitID Erhverv and prior to providing qualified signatures and seals in the Signing Solution. The specific terms and conditions contain detailed provisions on the User Organisation's obtaining of acceptance from the Business User for issuing of certificates.

9.3 General information about Certificates

Qualified signature based on a qualified certificate is recognised by the EU. 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). An electronic signature based on a Qualified Certificates is enforceable throughout Europe in the same way as a physical signature. For an electronic seal based on a qualified organisation certificate, there is a presumption of the integrity of the data and the accuracy of the origin of the data to which the qualified electronic seal is linked. Qualified seals are recognised by all Member States.

Electronic signatures based on an OCES certificate are based on the government OCES standard. In Denmark, the signature provided is enforceable in the same way as a physical signature. In the rest of Europe, the signature is enforceable according to national provisions, but cannot be denied having legal effect solely on the grounds that it is in electronic form. Digital signatures based on an OCES certificate are advanced electronic signatures based on the eIDAS Regulation.

9.4 OCES certificates (Persistent)

OCES organisation certificate (ID A) and OCES user certificate (ID B) can be ordered and subsequently administered in MitID Erhverv.

As Subscriber, the User Organisation is responsible for processing the certificates in accordance with the terms and conditions and the related certificate policies, cf. clause 9.7.

9.5 Qualified certificates (Persistent)

Qualified certificates in the form of qualified user certificates (ID D) and qualified organisation certificates (ID F) in persistent form can be ordered and subsequently administered in MitID Erhverv.

The ordering of qualified certificates is subject to special requirements relating to the systems and processes that form the basis for managing qualified certificates, including creation and storing of private keys. These requirements are set out in separate terms and conditions.

Persistent qualified user certificates and persistent qualified organisation certificates are expected to be available in MitID Erhverv in late 2022. These terms and conditions will be updated accordingly.

9.6 Qualified signatures (based on Short-term certificates)

Electronic signatures and electronic seals based on qualified user certificates (ID D) and qualified organisation certificates (ID E) as Short-term certificates can be used in the Signing Solution, provided that a Digital Self-Service Solution demand a qualified electronic signature or a qualified electronic seal.

9.7 Certificate policies

The terms and conditions for certificates that can be assigned and administered in MitID Erhverv are based on the following certificate policies:

- Certificate policy for qualified organizational certificates, version 7.1 (ID A)
- Certificate policy for OCES employee certificates, version 7.1 (ID B)
- Certificate policy for qualified employee certificates, version 1.1 (ID C and ID D)
- Certificate policy for OCES organizational certificates, version 1.1 (ID E and ID F)

The certificate policy and the Danish Agency for Digital Government's description of the Signing Solution (Certificate Practice Statement) are available on certifikat.gov.dk and ca1.gov.dk, respectively.

As specified in clause 9.1, another naming of certificates is used in MitID Erhverv than specified in the certificate policies.

9.8 Validation of qualified electronic signatures and seals

The Danish Agency for Digital Government makes available a qualified validation service for validation of qualified electronic signatures and electronic seals.

The validation service can be used for validation of qualified signatures and seals provided based on certificates issued by the Certification Authority of the Danish Agency for Digital Government.

The use of the validation service is subject to specific terms and conditions.

10 Obligations of the User Organisation

10.1 Correct and updated information

The User Organisation is responsible for ensuring that the data registered about the User Organisation and its employees are correct and up to date. Moreover, the User Organisation is responsible for ensuring that user rights for Employees and administrators are in accordance with the actual circumstances, including the User Organisation's internal rules for responsibility and authorisation.

The User Organisation is also responsible for rectifying any incorrect registrations and for informing Employees about the registration, including in accordance with the obligation to provide information specified in Article 13 of the General Data Protection Regulation.

As part of the above, the User Organisation is also required to register contact information and make sure that it is updated on an ongoing basis.

If a Business User's affiliation with the User Organisation ends, the User Organisation must immediately close the relevant Business User's User Identity and revoke any associated certificates.

When a User Identity is closed, any dedicated Authenticators belonging to the User Identity are automatically revoked and any associations between a user identity and a private authenticator is removed.

10.2 Consistency with the Danish Central Business Register (CVR)

The User Organisation is required to ensure consistency between the registration of the Legal Entity in the Danish Central Business Register (CVR) and the registration in MitID Erhverv. Certain changes in the User Organisation's registration in CVR will automatically be transferred to MitID Erhverv, including business status, cf. also clause 14.2 on consequences on change of business status.

10.3 Use of procedures and systems.

The User Organisation must use adequate administrative and management procedures that support the activities of the User Organisation and Employees and provide reasonable protection against unauthorised attacks and impacts.

In this connection, the User Organisation must ensure that Employees are instructed on the correct use of User Identities, Authenticators and Certificates.

At the request of a Business User, the User Organisation must revoke dedicated Authenticators and remove the association between a Business User and private Authenticators.

10.4 Ensuring correct association between User Organisation and Business Users

The User Organisation vouch for the association between the User Organisation and the associated Business Users, including Administrators. The User Organisation must maintain organisational and management procedures for this.

10.5 Business Users' compliance with terms and conditions

The User Organisation is responsible for ensuring that Business Users, including Administrators, comply with the rules and procedures to which they are subject under these terms and conditions and the terms and conditions for MitID, cf. clause 7.2.

10.6 Use of powers of attorney

If the User Organisation or a Business User represent a natural person or Legal Entity, it must be ensured that such representation is in accordance with the power of attorney. Powers of attorney obtained must be deregistered when the basis for the power of attorney no longer exists.

10.7 Management of Authenticators

The User Organisation must ensure that processes and systems that support the management of Business Identities and Authenticators create security and confidentiality as well as protection against misuse and attack.

The User Organisation is responsible for informing all Business Users that they are responsible for complying with any rules in force at all times on the storing and use of issued Authenticators, including MitID, and must provide a procedural or organisational framework that supports the compliance by the Business User.

The following are covered by the Business User's obligations:

- Devices and applications on which Authenticators are used must be kept updated and secure.
- Safe and secure storing of user ID, passwords and Authenticators to prevent unauthorised access.

- Strict confidentiality in terms of passwords, including prohibition against writing them down.
- A 'Password Manager' application (program for storing passwords) for storing information about user ID, passwords, etc. may only be used if the relevant application offers adequate protection against unauthorised access to the information stored.
- Authenticators are personal and may not be used by others.

It is the responsibility of the User Organisation to ensure that its own processes and systems support the obligations to which Business Users are subject when using specific Authenticators.

10.8 Reporting of security events

The User Organisation is required to immediately notify the Danish Agency for Digital Government in the event of any security events or attacks against MitID Erhverv or other services from The agency.

The User Organisation is specifically required to notify personal data breach to the Danish Data Protection Agency, pursuant to Article 33 of the General Data Protection Regulation and is also required to notify the Danish Agency for Digital Government if the breach relates to Services.

11 Processing of personal data

The Danish Agency for Digital Government is the data controller of MitID Erhverv and makes sure that the operation and control is in accordance with the rules for processing personal data.

The User Organisation is the controller of its own processing of Personal Data in MitID Erhverv and is responsible for having the required legal authority to disclose and process personal data about the User Organisation's Employees, including Administrators.

12 Service levels and availability

Unless otherwise specifically stated, all Services in MitID Erhverv covered by these terms and conditions are available 24/7/365.

The Danish Agency for Digital Government is not responsible for non-availability of Services due to service interruptions at the Danish Agency for Digital Government or any third party wanting to use the Services.

13 Support

The Danish Agency for Digital Government offers support to the User Organisation via the Central Support Service under the Danish Business Authority's Customer Centre.

The User Organisation may also request technical support from Nets DanID A/S at the rates specified on the MitID Erhverv Portal.

Please refer to the detailed description of support on the MitID Erhverv Portal.

14 System management

14.1 The Danish Agency for Digital Government's management unit

As the System Administrator of MitID Erhverv, the Danish Agency for Digital Government's management unit has a number of administrative privileges to act on behalf of the User Organisation in MitID Erhverv.

Unless special circumstances exist, including of a security nature, the Danish Agency for Digital Government will only act on the basis of a specific consent, including in connection with a support case.

14.2 Suspension and revocation of the User Organisation

The Danish Agency for Digital Government receives information about the business status of the Legal Entity from the Danish Central Business Register (CVR). Access to MitID Erhverv and use of Business Identities and separate MitID for Business will be suspended if the business status is changed to any of the following:

- Under compulsory dissolution
- Under bankruptcy proceedings
- Under reconstruction
- Under resumed proceedings

Suspension can be lifted if the User Organisation is reconnected by an Authorised Person appointed according to the applicable rules, and this will mean that the User Organisation can access MitID Erhverv again.

All certificates belonging to the User Organisation will be revoked in connection with the above change in business status. Once a certificate is revoked it cannot be reinstated. If, after ended suspension, the User Organisation still needs to use certificates, these must be acquired as usual via MitID Erhverv.

If the User Organisation is marked as terminated/dissolved in the Danish Central Business Register (CVR), the Danish Agency for Digital Government will immediately suspend all Business Identities, certificates and Separate MitID Authenticators for business use. Afterwards, it is not possible to reopen the User Organisation.

15 Fees

15.1 General

The User Organisation will pay the fees specified On the MitID Erhverv Portal, for using MitID Erhverv, including in relation to creation of User Identities, purchase of certificates and request of MitID Authenticators.

15.2 Fees for migration from Nets DanID

User Organisations created as part of a migration from NemID Erhverv to MitID Erhverv, cf. clause 4.4, may transfer their active NemID Business Users to MitID Erhverv and create these users as Business Identities without paying a fee.

15.3 Invoicing and payment terms

Invoicing is done on a monthly basis according to consumption.

Invoicing is carried out through Nets DanID A/S, which also handles the practical matters concerning payments and any adjustments.

The User Organisation must make payment no later than thirty (30) days after receiving an invoice. For payments received after the due date, the Danish Agency for Digital Government is entitled to default interest under the Danish Interest Act.

16 Erasure and logging

User data are stored in MitID Erhverv until they are erased by the User Organisation's administrators.

The actions performed by the User Organisation's Business Users and Administrators in MitID Erhverv are logged. The purpose of the log is to be able to document who have performed specific actions at a given

time, and who have been assigned specific rights. The log will only be disclosed to persons who can establish that they are entitled to receive log information.

Information in the log is erased annually after expiry of the relevant year + 5 years. Information related to certificates in MitID Erhverv is erased after 7 years of the date of signing.

17 Changes to rights regimes

The Danish Agency for Digital Government will notify the User Organisation when public authorities establish new rights, including to replace existing rights.

The assignment of new rights to Users will be based on approval from the Rights Administrator.

18 Breach and remedies for breach

18.1 Remedial action

The parties are required, without undue delay after the other party's written complaint, to make remedial action regarding errors and defects in the party's obligations.

18.2 General information about termination

Both the User Organisation and the Danish Agency for Digital Government may terminate the agreement that follows from these terms and conditions if the other party materially has breached its obligations, in particular in relation to security, and has not remedied the said matter(s) without undue delay.

The Danish Agency for Digital Government may also terminate the agreement if the User Organisation is declared bankrupt, files a petition in bankruptcy or initiates reconstruction proceedings to the extent that the rules of the Danish Bankruptcy Act do not prevent this.

The termination takes effect from the time when the notification about termination is received and applies to any Services thereafter.

The parties may terminate the agreement as described in more detail in clause 18.2 and clause 18.3. Moreover, the Danish Agency for Digital Government may, according to clause 18.4 and clause 19, suspend the User Organisations access to Services.

18.3 Termination by the Danish Agency for Digital Government

The Danish Agency for Digital Government is entitled to terminate the agreement if one or more of the following circumstances apply:

- The User Organisation breaches its reporting obligation in relation to security events.
- The Danish Agency for Digital Government can properly ascertain that the User Organisation's use of Services is of such a nature that it entails a risk of compromising MitID Erhverv or related infrastructures, including MitID.
- Non-compliance with applicable law, including the Danish Data Protection Act.
- The User Organisation acts in a way which has a substantial negative influence on or is suited to create mistrust or in any other way negatively influence the End-Users' perception of MitID Erhverv and/or related infrastructures, including the MitID solution.
- The User Organisation does not provide audit reports to document the User Organisation's compliance with the requirement of the NSIS standard (only applies if the User Organisation has connected a Local IdP).

Termination according to this clause may, however, not take place until the Danish Agency for Digital Government has pointed out the said matter in writing to the User Organisation giving a reasonable deadline for remedying the said matter and this has not taken place within the deadline.

18.4 Suspension of the User Organisation's access to Services

The Danish Agency for Digital Government may suspend the User Organisation's access to Services covered by these terms and conditions if the Danish Agency for Digital Government finds that the User Organisation does not materially perform the obligations set out in the terms and conditions or otherwise uses Services or MitID in such a way that it is harmful to the security and reputation of the infrastructure.

Notice according to clause 18.3 above may also be supplemented by suspension.

The Danish Agency for Digital Government must give the User Organisation reasonable and to the extent possible 14 days' notice allowing the User Organisation to resolve the said matter.

In extraordinary cases, suspension of access to MitID Erhverv can take place at shorter or without notice if the consideration for the integrity of the infrastructure, other User Organisations or Public Authorities so warrants, or if the said use constitutes a substantial security risk. In all cases, the Danish Agency for Digital Government must give an actual reason for the decision to suspend.

In case of suspension, the User Organisation will not be able to use its Business Identities until the Danish Agency for Digital Government reopens the connection or uses its other powers under these terms, including the right to cancellation or the Executive Order on MitID Erhverv and MitID Private for Business (Executive Order No. 1256 of 7 September 2022).

19 General suspension of access to Services

The Danish Agency for Digital Government may generally suspend the User Organisation's access to Services for operational reasons, including out of consideration for maintaining a high security level.

To the extent possible, the suspension will be notified to the User Organisation.

20 Liability and limitation of liability

20.1 General information about liability

The parties are liable according to the general rules of Danish law and according to what is stated in this clause.

In no event is the Danish Agency for Digital Government liable for business interruption, loss of profits, consequential damage or other indirect loss. Losses related to suspension and revocation under clauses 18 and 19 can be characterised as indirect losses.

The Danish Agency for Digital Government is not liable for any losses as a result of non-availability of Services, including the performance of the service levels on the MitID Erhverv Portal.

20.2 Liability for issuance of Separate MitID

The Danish Agency for Digital Government is liable for any incorrect registrations made in connection with the issuance of Separate MitID as a result of non-compliance with the procedures and precautions on registration and enrolment and support that apply to the administration and termination of the MitID solution, unless the Danish Agency for Digital Government can prove that the Agency has made no errors or omissions.

20.3 Limitation of liability

The parties' total liability 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.

The above limitation only applies if the breach cannot be attributed to gross negligence or intentional circumstances of the parties.

20.4 Liability related to qualified certificates

The above clause 20.1 does not regulate the liability of the Danish Agency for Digital Government as issuer of qualified certificates which are regulated by special terms and conditions.

21 Duty of confidentiality

The parties, including employees, subcontractors, consultants etc. must observe unconditional confidentiality with regard to information received from the other Party in connection with the receipt of Services and performance of requirements related to these terms and conditions, and on the condition that the information concerns the said party's trade secrets, concepts, relations and other confidential information. The parties must particularly ensure confidentiality about personal data, technical integrations and security-related issues.

The rules for employees in public administration apply to the staff of the Danish Agency for Digital Government. A similar obligation as regards information about the Provider's affairs that apply to the Provider regarding the affairs of the customer is imposed on consultants and others that assist the Agency.

The duty of confidentiality also applies after the termination of the terms and conditions, regardless of whether they have been terminated with or without notice or has otherwise lapsed.

22 Term and expiry

22.1 Term and termination

The terms and conditions take effect on acceptance by the Service Provider and will remain in force until terminated by either party.

Either party may terminate the terms and conditions at three months' notice.

22.2 Changes

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.

The Danish Agency for Digital Government may without notice change the terms and conditions for MitID for Business Users set out in Annex 1. If changes are made, the User Organisation will be notified thereof, and the Business User will be required to accept the changes when using the MitID Authenticator.

Any addition of new Services or functionalities in MitID Erhverv and separate terms and conditions attached thereto that do not impact the current functionality and operational circumstances of the User Organisation may be made without notice. The User Organization's use of any such Services or functionalities shall be deemed to constitute acceptance of any separate terms and conditions thereof.

Changes will be notified to the Organisation Administrator or via Digital Post. After expiry of the notice, the updated terms and conditions will apply.

22.3 Expiry

The entire agreement expires at the end of the period of notice, cf. clause 22.1. Some Services may also be closed sooner if the Danish Agency for Digital Government so decides. Such close-down of Services will be notified as a change.

At the time of expiry of the agreement, the User Organisation and all certificates issued via NemLog-in will be revoked.

23 Disputes

23.1 Governing law

Any matters subject to these terms and conditions and their interpretation must be settled according to Danish law.

23.2 Disputes, mediation and arbitration

In the event that any disputes should arise between the Parties, the Parties must first endeavour to solve such dispute by mutual and loyal settlement negotiations.

Any disputes and disagreements directly or indirectly arising out of these terms and conditions must be settled with final and binding effect by arbitration in accordance with the Rules of Procedure of the Danish Institute of Arbitration and according to Danish law. The place of arbitration is Copenhagen.

Each Party appoints an arbitrator while the umpire of the arbitration tribunal is appointed by the Institute, provided that the arbitrators appointed by the Parties fail to agree on an umpire within 14 days after their appointment.

In the event that a Party has not appointed its arbitrator within 30 days after having given or received notification of a request for arbitration, such arbitrator will be appointed by the Institute in accordance with the above rules.

However, this clause 23.2 does not prevent the Parties from bringing cases regarding breach of these terms and conditions before the courts of law with a view to taking preliminary legal action.

23.3 Disputes relating to certificates issued by the Danish Agency for Digital Government

Disputes relating to certificates and the purchase of physical MitID Authenticators are handled as set out in Annex 2 to Annex 6.