

Terms and conditions of business for a NemID administrator of commercial NemID

1	Background	2
2	Scope and object	3
3	Administrator and Certificates.....	3
3.1	General obligations of the Customer	3
3.2	General obligations of the Administrator	5
3.3	Issuing NemID employee digital signatures	5
3.4	Revoking NemID employee digital signatures	6
3.5	Issuing company digital signatures and function digital signatures	7
3.6	Revoking company or function digital signatures	7
3.7	Duty to inform	7
4	Delivery of digital signatures	8
4.1	Requesting NemID employee digital signatures.....	8
4.2	Requesting company or function digital signatures	8
4.3	Fee	9
5	Compensation and compensation amount limit	9
6	Force majeure.....	10
7	Assignment	10
8	Entry into force, changes and termination.....	11
9	Conflicts.....	12
10	Definitions.....	12

1 Background

These Terms and conditions of business, together with the associated order and Terms for commercial NemID from Nets DanID A/S, the combined terms of Customer registration as a NemID administrator and Nets DanID A/S' subsequent delivery of OCES company certificates (company digital signatures), OCES employee certificates (NemID employee digital signatures) and OCES function certificates (function digital signatures) to Users associated with the Customer. The terms and conditions of business are approved by the Danish Agency for Digitisation.

The first person at the Customer's business to receive the NemID employee digital signature automatically becomes the NemID administrator (Administrator). It is possible to have more than one Administrator at the same time. The Customer must at all times have at least one designated NemID administrator. The Administrator can do the following:

- Request NemID employee digital signatures from Nets DanID A/S, which issues these to individuals associated with the Customer. The NemID employee digital signature will include the Customer's CVR number and may also be associated with the employee's civil registration number, and the owner of the NemID employee digital signature will subsequently be able to undertake secure electronic communications and securely document his/her association with the Customer.
- Request company digital signatures from Nets DanID A/S. Nets DanID A/S issues these to the Customer. A company digital signature guarantees that the certificate owner is the company stated on the Certificate. A company digital signature represents the actual company, not individuals. Thus, no personal names are associated with the Certificate, which contains only the Customer's/company's name and one e-mail address.
- Request function digital signatures from Nets DanID A/S. Nets DanID A/S issues these to the Customer. A function digital signature ensures that the application, unit, process or service specified on the Certificate belongs to, is used by or is controlled by the company specified on the Certificate.
- Revoke and request the re-issuance of NemID employee digital signatures, company digital signatures and function digital signatures (Certificates).

- Associate rights (attributes) for NemID employee digital signatures via Nets rights management (Attribute Service) to give the employee special rights in relation to external service providers that use Nets rights management.
- Register other Administrators in the Customer's organisation.

2 Scope and object

- 2.1.1 The purpose of these Terms and conditions of business is to establish the conditions for the Customer's registration of an Administrator with Nets DanID A/S, including setting up an Administrator at the Customer, terms and conditions for the Administrator's request and Nets DanID A/S' delivery, etc., of Certificates.
- 2.1.2 The Customer registers an Administrator at the time of signing the Agreement. The more detailed requirements in relation to the Customer are set out in clause 3 of the Terms and conditions of business.
- 2.1.3 Nets DanID A/S delivers Certificates to the Customer in accordance with clause 4 of the Terms and conditions of business.
- 2.1.4 The Parties are obliged to treat all information about individuals in accordance with the rules set out in the Danish Processing of Personal Data Act (Lov om behandling af personoplysninger) from time to time in effect. Information covered by this Act, submitted in accordance with this Agreement, must only be used for the issuing and administration of Certificates.

3 Administrator and Certificates

3.1 General requirements, Customer

- 3.1.1 The Customer must at all times comply with the following requirements:
- a) The Customer must use prudent administrative and managerial procedures for instructing Users in the use of Certificates. The Customer has sole responsibility for such instruction.
 - b) The Customer must at all times use reliable systems and products in conformity with current recommendations from Nets DanID.
 - c) The Customer must ensure compliance with any current or future requirements issued by the Authorities concerning matters of significance to the Customer's

activities, the present Terms and conditions of business and as set out in "Terms for commercial NemID from Nets DanID A/S".

- d) The Administrator designated by the Customer cannot have a criminal record in matters pertinent to fitness to serve as an administrator.

The Customer is in all cases deemed unsuitable to perform its obligations if the Customer or associated Users have made errors that they should have realised were of major importance in relation to the tasks to be performed by an Administrator.

Nets DanID is furthermore entitled to rescind the contractual relationship and revoke all digital signatures issued to the Company in the following instances:

- e) The Customer terminates his business or goes bankrupt.
- f) The Customer is sentenced by a court for a criminal act that raises relevant doubts about the Customer's integrity.

- 3.1.2 The Customer must have at least one Administrator to interface with Nets DanID A/S at any given time. The Customer may have more than one designated Administrator simultaneously.
- 3.1.3 The Administrator must be associated with the Customer's organisation, but the Administrator is not required to be employed by the Customer. If the Administrator ceases to be associated with the Customer's organisation, the Customer must revoke that Administrator's employee digital signature.
- 3.1.4 The Customer must vouch for the identity of the Administrator. If the Customer wants to link the Administrator's civil registration number with that person's employee digital signature, the Customer must verify the link between the Administrator's name and civil registration number, e.g. by asking the Administrator to present photo ID.
- 3.1.5 The Customer must ensure the Administrator has given unequivocal consent for his/her civil registration number to be passed on to Nets DanID A/S as well as for registration with the Danish Agency for Digitisation's RID service.
- 3.1.6 Upon the Administrator's subsequent installation/activation of the employee digital signature, Nets DanID A/S will obtain the Administrator's consent to allow Nets DanID A/S to process his/her civil registration number in conformity with the Certificate policies and the Danish Processing of Personal Data Act (Lov om behandling af

personoplysninger). Consent will also be obtained for the civil registration number to be passed on to and registered with the Danish Agency for Digitisation's RID service.

- 3.1.7 The Customer is responsible for ensuring that the Customer's Administrators and Users comply with the terms to which an Administrator/User is subject in accordance with these Terms and conditions of business and the Terms for commercial NemID. This applies irrespective of whether the Administrator was designated by the Customer or by another Administrator, cf. clause 3.2.1.
- 3.1.8 There is an option not to protect the private key with an activation password in the case of automated use of company and function digital signatures, provided that the installation is secured against unauthorised access. In such a case, the Customer must take responsibility for this and must be able to document the nature of the security.

3.2 *General requirements, Administrator*

- 3.2.1 The Customer has authorised the Administrator to undertake all dispositions and activities covered by the present terms and conditions of business. The Administrator's duties include requesting and revoking Certificates in self-service for commercial NemID, and the Administrator can designate other Administrators for the Customer.
- 3.2.2 The Administrator must at all times comply with Nets DanID A/S' Terms for commercial NemID.

3.3 *Issuing NemID employee digital signatures*

- 3.3.1 The Administrator requests NemID employee digital signatures from Nets DanID A/S, which subsequently issues the digital signatures in accordance with the request.
- 3.3.2 When requesting a NemID employee digital signature, the Administrator must give Nets DanID A/S the information concerning the future User which Nets DanID A/S requests via self-service for commercial NemID, including the User's name or pseudonym, and possibly the person's civil registration number, if this is to be associated with the employee digital signature.
- 3.3.3 Before requesting a NemID employee digital signature, the Administrator must ensure that the User is familiar with the Terms for commercial NemID from Nets DanID A/S, and that the User accepts these terms when the employee digital signature is issued.
- 3.3.4 Before requesting a NemID employee digital signature, the Administrator must make sure that the User's identity has been unequivocally established. The User must

produce the necessary documentation to enable unequivocal verification of the User's identity and information.

If the User's civil registration number is to be associated with the digital signature, the Administrator must, at the time of placing the request, provide the User's civil registration number and also verify that the civil registration number belongs to the User. This can be done by the User producing photo ID. The User's name in the employee digital signature must match the User's name in the CPR register. The Administrator must also verify the User's name and civil registration number in the CPR register via self-service for commercial NemID.

- 3.3.5 In connection with this, the Administrator is responsible for ensuring that the User has given unequivocal consent for his/her civil registration number to be passed on to Nets DanID A/S and the Danish Agency for Digitisation so that it can be registered with the Danish Agency for Digitisation's RID service.
- 3.3.6 Upon the User's subsequent installation/activation of the employee digital signature, Nets DanID A/S will obtain the User's consent to allow Nets DanID A/S to process his/her civil registration number in conformity with the Certificate policies and the Danish Processing of Personal Data Act (Lov om behandling af personoplysninger). Consent will also be obtained for the civil registration number to be passed on to and registered with the Danish Agency for Digitisation's RID service.
- 3.3.7 The Customer is responsible to Nets DanID A/S for ensuring that the User's identity and association with the Customer are as set out in the registration undertaken by the Administrator with Nets DanID A/S.

The Administrator must ensure that the User's details are kept up to date at all times. Any changes to these details must be made via self-service for commercial NemID.

- 3.3.8 The Administrator is responsible for associating rights (attributes) with employee digital signatures wherever external service providers make these available to the Customer via Nets rights management. Rights in relation to external service providers who use Nets rights management are associated or removed via self-service for commercial NemID.

3.4 *Revoking NemID employee digital signatures*

- 3.4.1 The Administrator must revoke a NemID employee digital signature immediately upon receiving a request to this effect from the User. If circumstances so dictate, or if there

is any suspicion that an employee digital signature has been compromised or is no longer secure, the Administrator must revoke the employee digital signature on the Administrator's own initiative.

- 3.4.2 The Administrator must immediately revoke the User's employee digital signature if the User is no longer associated with the Customer, or if information in the employee digital signature no longer accords with the actual circumstances, whereupon a new employee digital signature may be issued in accordance with the new actual circumstances.

3.5 *Issuing company digital signatures and function digital signatures*

- 3.5.1 On behalf of the Company, the Administrator requests company and function digital signatures from Nets DanID A/S, which subsequently issues the digital signatures in accordance with the request.
- 3.5.2 When requesting a company or function digital signature, the Administrator must give Nets DanID A/S the information which Nets DanID A/S requests via self-service for commercial NemID, such as a technical contact for the digital signature.
- 3.5.3 On receipt of a company or function digital signature, the Customer must check that the content reflects the actual circumstances.

3.6 *Revoking company or function digital signatures*

- 3.6.1 If circumstances so dictate, or if there is any suspicion that an issued company or function digital signature has been compromised or is no longer secure, the Administrator must revoke the digital signature on the Administrator's own initiative.
- 3.6.2 The Administrator must immediately revoke the company or function digital signature if the information in the digital signature no longer corresponds to the actual circumstances.

3.7 *Duty to inform*

- 3.7.1 At the request of Nets DanID A/S, the Customer must provide documentation of compliance with the obligations under the Agreement. The Customer must provide Nets DanID A/S with any and all reasonable and relevant information relating to the Customer and the Administrator.

- 3.7.2 If circumstances arise that may have a bearing on the agreement, the Customer must immediately inform Nets DanID A/S in writing to this effect.

4 Delivery of digital signatures

4.1 *Requesting NemID employee digital signatures*

- 4.1.1 Once Nets DanID A/S has approved a request from the Customer to create the Customer's first Administrator, Nets DanID A/S will send an activation password to the individual the Customer has authorised as the Administrator. The Administrator will use the activation password to install/activate his/her NemID employee digital signature.
- 4.1.2 The Customer requests NemID employee digital signatures pursuant to this Agreement by the Administrator submitting requests via self-service for commercial NemID.
- 4.1.3 NemID employee digital signatures are issued by Nets DanID A/S to the User. Nets DanID A/S sends the activation password direct to the User by post, or the Administrator may deliver it direct to the User.
- 4.1.4 If the Administrator delivers the activation password direct to the User, the Customer must ensure proper delivery, and that the User acknowledges receipt of the activation password. The Customer must ensure that the User's acknowledgement of receipt is registered/logged, and that periodic audits of this are undertaken by the Customer's management or by an individual (not the Administrator) designated by the management. Nets DanID A/S reserves the right at any time to ask the Customer for documentation that this procedure has been followed, including evidence of audits undertaken.

4.2 *Requesting company or function digital signatures*

- 4.2.1 The Customer requests company and function digital signatures pursuant to this Agreement by the Administrator submitting requests via self-service for commercial NemID.
- 4.2.2 Company and function digital signatures are issued to the Customer by Nets DanID A/S. An activation password is presented to the Administrator directly in self-service for commercial NemID, and a welcome e-mail containing a link to download the digital signature is sent to the technical contact person specified by the Administrator at the time of the request.

4.2.3 The Terms for commercial NemID from Nets DanID A/S apply to the use of a company or function digital signature.

4.3 Fee

4.3.1 All prices are in Danish kroner. The prices include all fees applicable at the time of delivery excluding VAT. If there is any change in applicable Danish duties, Nets DanID is entitled to adjust the fee, with the attendant net consequences.

4.3.2 The fee is calculated on the basis of the list prices of Nets DanID A/S' deliveries from time to time in effect for the services covered by the terms and conditions of business, and as set out in Nets DanID A/S' price and product catalogue from time to time in effect. The prices from time to time in effect are established contractually between Nets DanID A/S and the Danish Agency for Digitisation as of 21 August 2008 and adjusted once a year only, in accordance with the net price index.

4.3.3 Nets DanID A/S' fee is due for payment 30 days after the Customer receives a satisfactory invoice.

Payment after the due date as set out on Nets DanID A/S' invoice attracts interest on the overdue amount in accordance with the Late Payment of Commercial Debts (Interest) Act (Renteloven) starting on the due payment date and until payment is made.

4.3.4 For services where the fee does not exceed DKK 1,000 excluding VAT per year, payable in advance of a set period, there will be no repayment of the fee paid if the service is cancelled prior to the end of the prepaid period.

5 Compensation and compensation amount limit

5.1.1 Each Party is liable to pay damages under the general rules of Danish law for any failure to comply with the terms and conditions of business.

5.1.2 Nets DanID is also liable to pay damages to the Customer and to verifiers pursuant to clause 6.4 of the CP in question unless Nets DanID A/S can prove that it has not acted negligently or with wilful intent.

5.1.3 Nets DanID is not responsible to the Customer for any operational losses, loss of profit or any other indirect losses, and the Customer may only claim compensation for one or more incidents giving rise to a claim within one year (1 January – 31 December) up to a combined amount of DKK 50,000.

- 5.1.4 The Customer shall indemnify Nets DanID A/S if Nets DanID A/S is required to pay compensation to a third party as a result of incidents giving rise to a claim where such incidents are attributable to the Customer, including the Administrator.

6 Force majeure

- 6.1.1 Neither Party shall be held liable to the other Party pursuant to the Agreement in regard to circumstances beyond the control of the Party and which, at the time of entering into the Agreement, that Party could not have taken into account and would not have been able to avoid or overcome. Circumstances concerning a subcontractor can only be regarded as force majeure where a hindrance covered by the first sentence above affects the external supplier and where Nets DanID A/S could not reasonably have foreseen, avoided or overcome such circumstances.
- 6.1.2 Force majeure in respect of a delay can only be cited for the number of Working Days during which the force majeure situation persists. Where a deadline for Nets DanID A/S is postponed because of force majeure, the associated payments will be postponed correspondingly.
- 6.1.3 Force majeure may only be cited where the affected Party has given written notification of the matter to the other Party without undue delay.

7 Assignment

- 7.1.1 Nets DanID A/S and the Customer are entitled to assign their rights and obligations under the Agreement within their respective groups (a public authority may assign to another public authority) as well as to a third party in connection with a business transfer or merger.
- 7.1.2 With the written approval of Nets, the Customer may assign its rights and obligations under the Agreement in circumstances other than those referred to in clause 7.1.1. Approval may not be refused without objective justification.
- 7.1.3 With the approval of the Danish Agency for Digitisation, Nets DanID A/S may assign its rights and obligations under the Agreement in circumstances other than those referred to in clause 7.1.1. If the Danish Agency for Digitisation approves assignment of an OCES solution, the Customer must respect such assignment or terminate the Agreement in accordance with clause 8.1.1.
- 7.1.4 If assignment involves changing or terminating the Customer's CVR number, the Customer shall revoke all digital signatures issued under the previous CVR number.

8 Entry into force, changes and termination

8.1.1 These terms and conditions of business enter into force at the time of their publication at www.trust2408.com/repository

8.1.2 The Customer may terminate the Agreement without giving notice. Any repayment of prepaid fees will be in accordance with clause 4.3.4.

Continuous services pursuant to this Agreement may be terminated by Nets DanID A/S if termination is objective and non-discriminatory. Termination may be at 12 months' notice to the end of a quarter.

The Agreement ceases without notice no later than at the time of the termination of the contract entered into by the Danish Agency for Digitisation and Nets DanID A/S on 21 August 2008 relating to digital signatures (the Main Contract). The Main Contract ceases automatically on 30 November 2015 unless the Danish Agency for Digitisation chooses to exercise a built-in option clause, whereupon the Main Contract continues in effect for two successive one-year periods, so that the Main Contract automatically ceases on 30 November 2016 or 30 November 2017.

8.1.3 By agreement with the Danish Agency for Digitisation, Nets DanID A/S may make general changes to these terms and conditions of business with an effect on the Customer on giving notice of at least six months. Any changes that do not put the Customer in a worse position may be effected immediately.

Nets DanID A/S is obliged to publish the amended terms and conditions of business in self-service for commercial NemID, and to elucidate all the significant changes.

8.1.4 If either Party is in material breach of its obligations pursuant to the present terms and conditions of business, the other Party may rescind the Agreement in part or in whole, just as Nets DanID A/S may unilaterally revoke the digital signatures issued pursuant to this Agreement.

The following is a non-exhaustive list of what constitutes material breach on the part of the Customer:

- The Customer or an associated User has made mistakes that they should have realised were of major importance in relation to the tasks to be performed by an Administrator, or is in any other respect deemed not to be a fit and proper person to perform the obligations of an Administrator, cf. clause 3.1.1

- If the Customer is not a public authority, and the Customer does not meet the requirements set out in clause 3.1.1 letter e) and f)
- If the Customer fails to comply with a request to submit specified documentation pursuant to clause 3.7.1
- If, upon handling the User's civil registration number, the Customer fails to unequivocally ensure identification and obtain consent from the User to submit the civil registration number, cf. clause 3.1.5 and 3.3.5
- If the Customer uses direct delivery of the activation password but fails to comply with the obligations as set out in clause 4.1.4

8.1.5 In the event of the cessation of the Agreement – for any reason whatsoever – Nets DanID A/S' obligations pursuant to the Agreement shall remain in force in respect of Users for as long as the employee digital signatures issued by Nets DanID A/S remain in use by the Users.

9 Conflicts

The legal relationship governed by this Agreement and these terms and conditions of business and their construction shall be in accordance with Danish law.

The Parties undertake to seek to resolve any disagreements relating to the Agreement by negotiation.

If a resolution cannot be obtained by negotiation, the dispute may be brought before Copenhagen City Court.

10 Definitions

The term

Administrator refers to the physical person(s) at the Customer's business registered with Nets DanID as a NemID administrator, and authorised by the Customer (1) to request NemID employee digital signatures, company digital signatures and function digital signatures from Nets DanID, (2) to revoke digital signatures created, or to change the details relating to these, and (3) to designate additional Administrators for

Nets DanID among Users (point 3 applies only if the Customer has opted for the self-service for commercial NemID functionality in question).

The Agreement refers to the agreement entered into by Nets DanID A/S and the Customer for the creation of a NemID Administrator to issue NemID employee digital signatures, company digital signatures and function digital signatures with the associated Terms and conditions of business and Terms for commercial NemID.

Working Day refers to Monday to Friday except for public holidays, the Friday after Ascension Day, Ascension Day, Constitution Day in Denmark (5 June), Christmas Eve and New Year's Eve.

User refers to the physical person to whom Nets DanID issues a NemID employee digital signature.

Certificate refers to an electronic certificate that specifies the certificate owner's/certificate holder's public key along with supplementary information and which unequivocally links the public key to the identity of the certificate owner/certificate holder. A Certificate must be signed by a certification authority (CA) which thereby confirms the validity of the Certificate. In this Agreement, a Certificate is an OCES employee certificate, an OCES company certificate or an OCES function certificate.

Certificate holder refers to the physical person identified in the Certificate as the correct User of the private key belonging to the public key which is provided in the Certificate. "Certificate holder" is used when the person using the Certificate is not identical to the company which has entered into an agreement with and has been issued the Certificate by Nets DanID. The certificate holder is designated the User in these Terms and conditions.

Certificate owner refers to a physical person or company that enters into an agreement with Nets DanID and to whom or which an OCES certificate is issued (either an OCES personal certificate, an OCES employee certificate, an OCES company certificate or an OCES function certificate). The certificate owner is designated the Customer in these terms and conditions.

Certificate policies (CP) refer to the versions of the Certificate Policies prepared by the Danish Agency for Digitisation from time to time in effect for OCES personal certificates, OCES employee certificates, OCES company certificates and OCES function certificates respectively. Certificate policies may comprise more than those mentioned,

and an overall summary of these can be found and downloaded at any time from www.certifikat.dk/repository.

DanID A/S refers to Nets DanID A/S (CVR no. 30808460).

The Customer refers to the physical person or legal entity with whom or which Nets DanID A/S has entered into the Agreement. The Customer is also the certificate owner.

Activation password refers to the one-time password which is used when first installing a Certificate.

NemID refers to Nets DanID's security solution, which a User who has an OCES certificate can use to log on to a Service Provider and to carry out actions, including signing data digitally.

OCES stands for Offentligt Certifikat til Elektronisk Service (Public Electronic Service Certificate).

OCES CP refers to the Certificate Policy owned and maintained by the Danish Agency for Digitisation in respect of OCES personal certificates, OCES employee certificates, OCES company certificates and OCES function certificates.

OCES function certificate refers to function digital signatures requested by the Administrator, and issued by Nets DanID.

OCES employee certificate refers to NemID employee digital signatures requested by the Administrator, and issued by Nets DanID.

OCES company certificate refers to company digital signatures requested by the Administrator, and issued by Nets DanID.

Public authority refers to the public authorities listed in Appendix 2 to Guidelines on publicly registered public authorities (Guideline 85 of 23 November 2006) with the exception of DR and DSB.

Public key refers to the unique key included in a Certificate and used for verifying the electronic signature.

Party or Parties refers to Nets DanID or the Customer or both.

Price and product catalogue refers to the list of products and associated prices from time to time in effect. The price and product catalogue is available at www.nets-danid.dk.

Private key refers to the unique key which is used to create an electronic signature and to decrypt electronic messages.

Private company refers to the private companies listed in Appendix 2 to the Guidelines on publicly registered private companies (Guideline 85 of 23 November 2006), with the exception of The Danish Regions, Local Government Denmark, independent schools and private primary and lower secondary schools, Niels Brock Copenhagen Business College as well as Sundhed.dk.

Self-service for commercial NemID refers to the Nets DanID website where the Administrator can create new Certificates or new Administrators and where the Administrator can revoke Certificates created or amend the information on these.

Verifier refers to a legal entity which or a physical person who receives a digital signature created by the signing of data using a Certificate from a certificate owner or a certificate holder.

Service provider refers to a private company or public authority which offers access to digital services, also referred to as "content service" or a "self-service solution."

The definitions in the OCES CPs shall apply to other terms which are not defined in this Agreement but defined in the OCES CPs.