Terms for commercial NemID from Nets DanID A/S

February 2014

1. General terms

The following terms apply to the use of OCES commercial certificates from Nets DanID A/S (hereinafter referred to as Nets DanID).
These terms apply to certificate owners (the physical person who or legal entity that has entered into an agreement with Nets DanID on the issuing of certificates to one or more certificate holders), certificate holders, and to verifiers (recipients of signed data).

These terms have been prepared in accordance with the applicable certificate policies, respectively for OCES employee certificates (NemID employee digital signatures), OCES company certificates (company digital signatures) and OCES function certificates (function digital signatures) established by the Danish Agency for Digitisation as well as applicable Certification Practice Statement (CPS) prepared by Nets DanID, which describes the procedures followed by Nets DanID in handling certificates from Nets DanID.

These documents are available from www.trust2408.com/repository.

2. Obligations and responsibilities of the certificate owner

Unless otherwise stated, both the certificate owner and the actual user of the certificate (the certificate holder) associated with the certificate owner are obliged to abide by the rules in clauses 2.1–2.6 when using the OCES certificate from Nets DanID.

The certificate owner is responsible for handling OCES employee certificates, OCES company certificates and OCES function certificates internally at the certificate owner and for providing information to employees regarding the use and storage of private keys, including the certificate owner's option to read encrypted e-mails.

The certificate owner is responsible to third parties and to Nets DanID for ensuring certificate holder compliance with these terms.

2.1. Information

The certificate owner/certificate holder must provide accurate information to use for the application for issuing an OCES certificate from Nets DanID.

The certificate owner/certificate holder must, on receipt of his/her OCES certificate, check that the content of the OCES certificate reflects the actual circumstances.

If the information in the certificate differs from information given in connection with the application, Nets DanID must be notified immediately. The same applies if the content of the certificate no longer reflects the actual circumstances.

When a certificate is applied for, Nets DanID will issue an activation password to use when generating the certificate. The activation password must be stored confidentially.

2.2. Key file and hardware solution

Where the key pair is generated and stored at the certificate owner/certificate holder, the certificate owner/certificate holder must generate and store his/her private key and associated activation password in a secure IT environment and in accordance with the guidelines specified by Nets DanID in connection with the issuing of certificates. The certificate owner must ensure that the IT environment is kept up to date at all times with the latest security updates and antivirus software.

The certificate owner/certificate holder must immediately ask Nets DanID for a new activation password if an unauthorised person may have had access to it.

The certificate owner/certificate holder is obliged to protect the private key against loss, disclosure, modification and unauthorised use.

The private key must be stored encrypted and protected by a self-chosen password. The password must contain at least eight characters and must contain at least one upper-case character, one lower-case character and one number (e.g. *G2uw3KMs*). If a different password is used (e.g. a biometric password), it must be at least 2048-bit key strength. In solutions capable of blocking exhaustive searches, however, the password must be a minimum of four digits.

The certificate owner/certificate holder must ensure that no-one else finds out the password.

The password used to protect the private key must under no circumstances be stored at the same place as the private key and must always be kept confidential.

The certificate owner/certificate holder may not leave the private key in an unlocked state without supervision (e.g. a computer on which the password has been entered). Transferring the private key, activation password or self-chosen password to anyone else is prohibited.

If the certificate owner/certificate holder makes a back-up of the private key, the back-up must also be stored encrypted and protected by a password, cf. above.

The certificate owner/certificate holder must immediately stop using the certificate if the certificate owner/certificate holder is informed that Nets DanID has been compromised.

Data encrypted with a public key from the certificate may only be decrypted with an associated private key. This means for example that the certificate owner/certificate holder cannot read e-mails encrypted using the certificate if the certificate owner/certificate

holder no longer has access to the password and the private key.

2.3. Code card solution

Where key pairs are generated and stored centrally at Nets DanID, the certificate owner/certificate holder must immediately ask Nets DanID for a new activation password if it is possible that an unauthorised person may have had access to it.

The certificate owner/certificate holder must choose a personal password. The password must be between 6 and 40 characters, must contain both letters and numbers, must not contain special characters and must not have the same character four times in a row. Furthermore, the password must not contain the civil registration number or NemID number of the certificate owner/certificate holder.

The certificate owner is responsible for ensuring that the user ID, password and one-time codes from the code card/voice response are used in a secure and reliable IT environment. The certificate owner must therefore always ensure that the IT environment is kept up to date with the latest security updates and antivirus software. The certificate owner must furthermore ensure that the certificate holder does not use the user ID, password and one-time passwords from a device that does not have the latest security updates installed. "Device" refers to the device on which the NemID certificate is used e.g. computer, mobile phone or tablet.

The certificate owner must ensure that the certificate holder stores his/her user ID, password and code card securely and responsibly, and ensure that no one else gets to know this and thus gains access to using them.

The certificate owner/certificate holder must not: disclose the password, one-time passwords or hand over the code card to anyone else, scan, input or in any other way copy one-time passwords as a means of storing them, write down the password or keep the password together with the code card.

The private key stored at Nets DanID will be accessible to the certificate owner/certificate holder even after revocation to enable the certificate owner to decrypt data using the private key. Access to the private key is contingent on use of the personal password, however.

2.4. Associating a civil registration number

When an OCES employee certificate is issued with an associated civil registration number, the certificate holder simultaneously consents that:

- Nets DanID may retrieve the certificate holder's name and address from the CPR register.
- Nets DanID passes on the association between the certificate and the certificate holder's civil registration number to the Danish Agency for Digitisation's public RID service.
- Nets DanID may use the public RID service to retrieve the RID number of a previous certificate.

2.5. Use

The certificate may be restricted in terms of use (restriction of purpose) or in terms of the transaction amount (restriction of amount). The certificate owner/certificate holder must only use the OCES certificate in line with any restrictions stipulated on the OCES certificate.

The OCES certificates are not qualified certificates and they must not therefore be used in situations requiring qualified certificates. The certificates may not be used to sign other certificates.

The private key provided at the time of issuing the OCES certificate must not be used until the OCES certificate has been received, except for usage in connection with applying for the certificate.

The certificate owner/certificate holder must not use the private key after request for revocation, notification of revocation or expiry of the certificate for any purposes other than decryption of data encrypted using the associated public key.

2.6. Revocation

The certificate owner/certificate holder must immediately revoke the certificate if the content of the certificate no longer reflects the actual circumstances, for example (but not restricted to) instances where an employee is no longer associated with the certificate owner, or if the certificate owner goes bankrupt or is dissolved.

If key pairs are generated at the certificate owner/-certificate holder, the certificate owner/certificate holder must immediately revoke the certificate if the private key has been, or may have been, compromised. In this connection, the private key must only be used to revoke the certificate or to decrypt data encrypted using the associated public key.

Where key pairs are generated and stored centrally at Nets DanID, the private key shall be deemed to be compromised if an unauthorised person gains access to both the password and unused one-time passwords from the code card.

The certificate owner/certificate holder must immediately revoke the code card if others have or may have gained access to unused one-time passwords.

The certificate owner/certificate holder must also immediately revoke the code card if it is lost.

The certificate owner/certificate holder must immediately revoke or change the password if the certificate owner/certificate holder suspects that others may have knowledge of it.

Revocation is possible 24/7 on tel. +45 72 24 70 10.

3. Obligations and responsibilities of the verifier

The verifier who verifies the signed data from a certificate owner must check the following before relying on the certificate:

- that the certificate has not expired.
- that the certificate is valid, by checking the status of the certificate. The certificate is considered to be invalid if its validity cannot be verified positively by looking up the current certificate revocation list from Nets DanID.
- that the certificate is used in accordance with any restrictions of use stated on the certificate. The certificate may be restricted in terms of use (restriction of purpose) or in terms of the transaction amount (restriction of amount).
- that the level of security is considered suitable in relation to the purpose for which an attempt to use the certificate is being made.

4. Nets DanID's powers in the event of breach

Nets DanID is entitled to unilaterally revoke a certificate if Nets DanID finds out or suspects that the certificate holder's private key has been compromised or destroyed, that the employee is no longer associated with the certificate owner, that the actual circumstances no longer correspond to the content of the certificate, that the certificate owner has gone bankrupt or is no longer operating, or that the certificate owner is in any other way in breach of its obligations.

Where key pairs are generated and stored centrally at Nets DanID, Nets DanID may furthermore revoke:

- the password if Nets DanID suspects or finds out that others have gained access to it.
- the password if it has been entered incorrectly a certain number of times.
- the code card if Nets DanID suspects or finds out that others have gained access to one-time passwords from the code card.

5. Liability to pay damages

The Parties are liable to pay damages to one another under the general rules of Danish law.

Nets DanID is also responsible for losses incurred by a party that reasonably relies on the certificate (verifier), if the loss is caused by:

- the information specified on the certificate not being correct at the time the certificate was issued.
- the certificate not containing all the information required by clause 7.3.3 of the OCES CPs.
- Nets DanID not having revoked the certificate after having received a request to do so from the certificate owner or certificate holder, or if the circumstances in general support this, cf. clause 7.3.6 of the OCES CPs.
- Nets DanID having provided inadequate or incorrect information that the certificate was revoked, the certificate's expiry date or whether the certificate is subject to restrictions in terms of purpose or amount.
- Nets DanID has ignored OCES CPs clause 7.3.1.
- and Nets DanID is unable to prove that Nets DanID has not acted negligently or with wilful intent.

Nets DanID is not liable for the losses of the certificate owner or verifier, where the certificate owner or verifier is a business or public authority, and

- the loss has occurred as a result of circumstances beyond Nets DanID's control, including circumstances at a subcontractor, strike and lockout.
- the loss has occurred as a result of an OCES certificate being used without the restrictions of purpose or amount that apply to the certificate, and which are stated on the certificate.
- the loss is an indirect loss, including loss of profits, operating losses, losses as a consequence of loss of data, system failure or similar.
- the total loss for all incidences of damages for the injured party exceeds DKK 50,000 during the course of one year (a "year" means 1 January to 31 December).

6. Expiry of and reapplication for a certificate

An OCES certificate from Nets DanID has a validity period of up to four years. When the validity period expires, a new certificate needs to be applied for. A new certificate may be issued using the old certificate provided that renewal takes place prior to the expiry of the validity period of the old certificate, and provided that the private key has not been compromised. If an OCES certificate has expired or been revoked, or the private key has been compromised, the old certificate cannot be used to reapply for an OCES certificate.

7. Other terms

7.1. Conflict resolution

Any disputes arising from the use of OCES certificates issued by Nets DanID are subject to Danish law and shall be brought before Copenhagen City Court.

As far as possible, disputes between the parties must be resolved by means of negotiation between the parties.

7.2. Changes to terms and conditions

Nets DanID is entitled to change the terms and conditions without notice and the changes will come into effect on publication at www.trust2408.com/repository and on sending electronic notification to the certificate owner. Changes of a favourable nature or which do not result in a restriction of the certificate owner's rights may, however, be implemented without direct notification being provided to the certificate owner.