

Addendum to NemID conditions for online banking and public digital signature – NemID on hardware, v.1

1 Introduction

NemID on hardware is a digital signature that you can use to log on to private and public websites. You can also use NemID on hardware to provide your digital signature.

NemID on hardware differs from NemID with code card/code token in that your private key is stored in a cryptographic hardware module, such as a USB crypto token, which you yourself retain. For NemID with code card/code token, your private key is instead stored on a central server at Nets DanID.

When you order NemID on hardware, you receive an OCES certificate. OCES stands for Offentlige Certifikater til Elektronisk Service (public certificates for digital service).

This addendum includes the conditions that apply specifically to NemID on hardware. The general NemID conditions (NemID conditions for online banking and public digital signatures) also apply to NemID on hardware to the extent that they are applicable to digital signature.

You can also find the conditions at www.nemid.nu.

Nets DanID refers to Nets DanID A/S, CVR 30808460.

Hardware refers to the cryptographic hardware module (crypto token) where your private key and your OCES certificate are stored.

Device refers to the device on which the NemID is used e.g. computer, mobile or tablet.

2 NemID on hardware conditions

2.1 Generation and storage of your private key

The following conditions apply to NemID on hardware:

- you must use the hardware (crypto token) designated by Nets DanID at www.nemid.nu
- you must not generate, store or use your private key apart from for the designated hardware (crypto token). Thus, the key must not be generated in software on your device.

2.2 Storage of hardware and password

Please note that:

- you must store your hardware securely and responsibly so that no one else is able to use it
- you must not disclose your password to anyone
- you are not allowed to write down your password
- you must not store your password together with your hardware.

2.3 Security when using NemID

You must make sure that:

- your hardware is used only by you and in accordance with the conditions
- others cannot read your password when you enter it
- you use NemID on a device where the operating system, Internet browser and other programs are regularly updated with the latest security updates.

You must regularly check that you have not lost your hardware, and that NemID has not been misused.

3 Revoking your NemID on hardware

3.1 Revoking your OCES certificate

3.1.1 Your duty to revoke immediately

You must immediately revoke your OCES certificate:

- if you lose your hardware
- if you suspect that others have or could have gained knowledge of your password or access to your hardware.

3.1.2 Revoking

When you revoke your OCES certificate, you must give your name, and possibly your address and/or civil registration number.

Once your certificate is revoked, Nets DanID will send you a confirmation, stating the time and reason for revoking.

You can revoke your OCES certificate by:

- calling +45 72 24 70 10 (24 hours a day)
- visiting www.nemid.nu (24 hours a day)

You can use the activity log at www.nemid.nu at any time to check the time that your OCES certificate was revoked and the reason why.

3.1.3 Revoking by Nets DanID

Nets DanID will revoke your OCES certificate if:

- you ask Nets DanID to do so
- Nets DanID suspects or finds out that others have gained access to your password or your hardware.
- Nets DanID becomes aware that you have failed to comply with the NemID conditions.

4 Amendment of the conditions for NemID on hardware

Nets DanID may amend the Addendum to NemID conditions for online banking and public digital signature without prior notice if the amendment is due to a change of the NemID security requirements. Amendments will enter into force once published at www.nemid.nu. If you have registered your e-mail address with Nets DanID, you will also be notified of amendments by e-mail. Other amendments will be announced at www.nemid.nu no later than three months before becoming effective.