NemID conditions for online banking and public digital signatures

1 Introduction

NemID is a security solution that you can use for accessing your online banking service, public authority websites and private websites. You can also use NemID for providing your digital signature.

NemID comprises a user ID, a password and a code card that indicates the one-time passwords (called codes) you must use together with your user ID and your password.

For the IVR (Interactive Voice Response) solution, you receive your codes via your telephone.

You also have the option of having an electronic code token to indicate your codes. However, you will still need to retain your code card, as there are some situations in which you will need to use it.

If you wish to use NemID as a public digital signature, you also need a linked OCES certificate for NemID. OCES stands for Offentlige Certifikater til Elektronisk Service (Public certificates for digital service).

The conditions below apply to the use of NemID. If you only want to use NemID for your online banking service, you only need to read through Sections 2 and 3. The use of NemID for your online banking service is otherwise regulated by your online banking agreement. This will also make clear to what extent the rules on liability in the Danish Payment Services Directive (Betalingstjenesteloven) apply.

If you also wish to use NemID as a public digital signature, please read through Sections 2, 3 and 4.

You can also find the conditions at www.nemid.nu or www.nets-danid.dk.

DanID refers to Nets DanID A/S, CVR 30838460.

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

2 Obligation

When you use NemID to carry out actions, e.g. to provide your digital signature, you obligate yourself towards the recipient in the same way as you do when you sign a document physically.

3 Conditions for the use of NemID

3.1 Registration for NemID

When you register for NemID you are obligated to provide sufficient and correct information.

3.2 Storing user ID, password and code card/code token

Please note that:

- your user ID, password and code card/code token must be stored securely to prevent others from using them
- you may not disclose your password or your codes, and you may not hand over your code card/code token to others
- you may not scan your code card, enter the codes on external media or in any other way copy the codes or store them digitally
- you are not allowed to write down your password
- you may not store the password together with your code card/code token or write the password on your code card/code token.

3.3 Security when using NemID

You must make sure that:

- your user ID, password and code card/code token are only used by you and only 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 code card/code token and that NemID has not been misused. You can, for example, choose to record where you use NemID in the activity log by using the self-service function at www.nemid.nu. This will enable you to check that NemID has only been used for the websites of service providers you have visited.

3.4 Activation password

If you have just registered for your online banking service, you will receive an activation password that you can use to log in and register for NemID. This also applies if you have blocked your password; see Section 3.5 on blocking.

If you suspect that others have knowledge of your activation password, e.g. if the letter with the activation password has been tampered with, you should immediately request a new activation password from DanID or your bank.

3.5 Blocking

3.5.1 Your duty to block immediately

You must immediately block:

- your code card if you suspect others have or might have gained knowledge of the codes on your code card, e.g. if the letter containing the code card has been tampered with when you receive it
- your code token if the letter containing the code token has been tampered with when you receive it
- your code card/code token if you have lost it. If you find a lost code card/code token, it must be destroyed
- your password if you suspect that others have or might have gained knowledge of it, unless you are immediately able to change the password via www.nemid.nu.

3.5.2 Blocking

When you block your password and/or code card/code token, you must provide your name, address and CPR number as required, or your user ID, code card number or code token number.

You must also indicate whether you want to block your password or code card/code token. When you have blocked your password, DanID will send you a confirmation, stating the time and cause of the blocking.

You can block your password and/or code card/code token by

- dialling +45 80 30 70 10 (24 hours a day)
- visiting www.nemid.nu (24 hours a day)
- contacting your bank or local citizen service centre (if your NemID is associated with a public digital signature).

You can use the activity log at www.nemid.nu at any time to check the time that your password and/or code card/code token was blocked and the reason why.

3.5.3 Blocking by DanID

DanID will block your:

- password if DanID suspects or finds out that others have gained access to your password
- password if the password has been entered incorrectly a certain number of times
- code card/code token if DanID suspects or finds out that others have gained access to codes from your code card/code token
- NemID if DanID finds out you have not complied with the conditions in Section 3
- NemID if the information you provided when registering for NemID is incorrect, or
- NemID if DanID is informed that you have passed away.

3.5.4 Using NemID after blocking

You cannot use NemID when your NemID or password has been blocked. If only your code card/code token has been blocked, some banks may allow you limited access to online banking, for instance to check your account information.

3.6 Terminating your access to NemID

If you no longer wish to use NemID, you may terminate your access at any time. See Section 3.5.2 on blocking. Please note that you will no longer be able to use the services that make use of NemID.

3.7 Processing of personal data

If you have registered for NemID via your bank, DanID will process your personal data on behalf of the bank. DanID will process your data, i.e. name, address and CPR no., to be able to identify you. DanID will also use your e-mail address, if you have provided one, to notify you of any blocking, for example.

If you have registered your mobile phone number with DanID, DanID will use your mobile phone number to send you text messages concerning activation passwords etc.

Log files may be created on the user's device whenever NemID is used. The user may delete these if desired. As part of security, DanID registers the times when you use NemID, the IP address and other information about the device on which you use your NemID.

The NemID solution uses a so-called "Java applet", which runs on the user's computer. In order to ensure that the system is working securely and efficiently, the applet stores the code locally (cache) on the user's computer.

To read more about the log files and security, visit: www.nemid.nu/om_nemid/sikkerhed/logning/

If you use the self-service function at www.nemid.nu and choose to record where you have used NemID in the activity log, DanID will also log the service providers with which you have used NemID. You can always unsubscribe from this recording function, in which case DanID will no longer log where you have used NemID. DanID will keep the data for the current year + five years, after which it will be deleted.

3.8 Claims related to NemID

Any claims that arise as a result of your use of NemID through your online banking service must be made to your bank in accordance with your online banking agreement. Any claims that arise as a result of your

use of NemID at other websites must be made to the service provider or to DanID.

3.9 IVR solution – special note

The IVR solution is primarily designed for the blind and people with impaired vision. If you receive codes via the IVR solution, you must take the proper precautions for the telephone on which you receive codes. The precautions for code cards/code tokens are specified in these conditions.

This means that:

- you must ensure that the telephone on which you receive codes is independent of the computer/telephone you subsequently use to type in the code
- you must immediately block your password if you lose the telephone on which you receive the codes, or if you discover that your telephone line is being misused.

3.10 Amendment of the conditions for using NemID

DanID may amend the conditions for NemID 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 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.

4 Special conditions applying to public digital signatures

- If you use NemID as a public digital signature, the following conditions will apply in addition to the conditions stated in Sections 2 and 3.
- If you wish, you may request different NemIDs, and thus also different code cards/code tokens and user IDs for use with your online banking service and your public digital signature respectively.

4.1 Processing of personal data

When your OCES certificate has been issued and associated with NemID, you confirm that:

- DanID may retrieve your name and address from the CPR register
- DanID may pass on the link between your public digital signature and your CPR number to the public PID (Personal Identification) service at the National IT and Tele Agency (IT- og Telestyrelsen). The PID service is used by public service providers for identification purposes. A private service provider may only retrieve your CPR number with your consent when you log onto the service provider's site
- DanID may use the public PID service to retrieve the PID number of a previous digital signature.

If you received your NemID through your online banking service and you also wish to use NemID as a public digital signature, you consent that the bank can pass on – and DanID can use – your personal data (name, address, CPR number and, if provided, e-mail address and mobile phone number) to DanID to issue and manage your public digital signature.

If you received your NemID in connection with the issuing of a public digital signature, and you also wish to use the NemID for your online banking service, you must accept your bank's request to let DanID pass on NemID data to your bank so that you may use NemID for your online banking service.

If you no longer wish your personal data and/or information about your NemID to be processed as indicated above, you can either block your public digital signature by contacting DanID or a citizen service centre, and/or you can terminate access to your online banking service by contacting your bank. If you block your public digital signature, you can only use NemID with your online banking service; if you terminate your access for your online banking service, you can only use NemID as a public digital signature.

4.2 Your obligations and responsibility as the holder of a public digital signature with associated OCES certificate

You must ensure that the name and any e-mail address details provided in the OCES certificate are correct.

In case of changes to the information provided on the OCES certificate – e.g. if you change your name – you must renew your OCES certificate within 30 days. If you do not renew the OCES certificate within 30 days, and DanID becomes aware that the information is incorrect, DanID will block your OCES certificate.

You may not use your OCES certificate to issue certificates to others.

4.3 Blocking your OCES certificate

DanID will block your OCES certificate if:

- you ask DanID to do so
- DanID becomes aware that you have failed to comply with the NemID conditions.

If the OCES certificate is blocked by you, DanID will send you a confirmation that the certificate has been blocked, either by sending a signed e-mail or by a letter to your address listed in the National Register of Persons (Folkeregisteret), if DanID has access to this address. If DanID does not have access to the address listed in the National Register of Persons, DanID will send the confirmation to the address provided to DanID by you. If DanID blocks your OCES certificate, and the blocking was not requested by you, DanID will inform you of the reason for the blocking by signed e-mail and by letter if this is possible.

4.4 Renewing your OCES certificate

The period of validity of your OCES certificate will be shown on the certificate. An OCES certificate is valid for up to four years. DanID will inform you no later than four weeks before the expiry of your OCES certificate by sending either an e-mail or a letter to the address listed in the National Register of Persons, if DanID has access to this address. You can renew your OCES certificate before it expires by using your old OCES certificate. If your OCES certificate has expired or has been blocked, you must order a new certificate.

4.5 Obligations and responsibility when you receive digitally signed data

If you receive digitally signed data, for example because you exchange digitally signed e-mails or documents, you must, before you rely on the OCES certificate, check that the sender's OCES certificate

- is valid, i.e. that the validity period shown on the OCES certificate has not expired
- is not blocked, i.e. it is not on DanID's certificate revocation list posted on DanID's website
- its use complies with any restrictions shown on the OCES certificate.

4.6 DanID's liability towards you as the holder of an OCES certificate

DanID's liability for misuse shall be subject to the general rules of Danish law. However, DanID shall not be liable for losses caused by your non-compliance with the conditions for NemID.

Any claim for damages relating to your OCES certificate shall be made to DanID.

The conditions for NemID shall be governed by Danish law. Any disputes arising between you and DanID that cannot be resolved by negotiation shall be brought before the City Court of Copenhagen.

4.7 DanID's liability to you when you receive digitally signed data

DanID shall be liable for losses sustained by you if you have proper trust in a sender's OCES certificate, if such loss is caused by an error on DanID's part in connection with registering, issuing or blocking the certificate. DanID shall not be liable for any loss if DanID can prove that DanID has not acted negligently or with wilful intent.

5 Further information

If you would like to know more about NemID and the public digital signature, please contact your bank, local citizen service centre or DanID. You can also find out more about our key terminology and certificate technology at www.nemid.nu.