General conditions for NemID with access to online banking, public and other websites

1 INTRODUCTION
NemID is a security solution which 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 or another unit such as a telephone which indicates the codes you should use together with your user ID and your password.

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

The conditions below apply for the use of NemID. If you only wish 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 Act (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.dk or at www.danid.dk.

2 OBLIGATION
When you use NemID for different purposes, e.g. to provide your digital signature, you obligate yourself towards the recipient in the same way you do when you sign a paper document.

3 CONDITIONS FOR THE USE OF NEMID

3.1 Registering for NemID
When you register for NemID you become obligated to provide sufficient and correct information.

3.2 Storing user ID, password and code card
Please note that:
• your user ID, password and code card must be stored securely to prevent others from using them;
• you may not disclose your password, your codes, or hand over your code card to others;
• you may not scan your code card, enter the codes or in any other way digitalise or copy the codes;
• you are not allowed to write down your password;
• you may not store the password together with the code card or write the password on the code card.

3.3 Security when using NemID
You need to make sure that:
• your user ID, password and code card can only be used by you and in compliance with the conditions;
• others cannot read your password, when you enter it; and
• you regularly install security updates for your operating system, your Internet browser and other programs on your PC.

You must regularly check that you have not lost your code card and that NemID has not been misused. You can, for example, have where you use NemID recorded in the activity log by using the self-service function at www.nemid.dk. 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 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, immediately request a new activation password from your bank or DanID.

3.5 Blocking
3.5.1 Immediately block your code card, if
• you suspect that others 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;
• you have lost your code card. If you find a lost code card, the card must be destroyed;
• you suspect that someone has knowledge of your password.

3.5.2 How to block your code card
When you block your password and/or your code card, you must provide the following information: name, address, CPR no. or user ID, or code card number. You must also indicate if you want to block the password or the code card. 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 your code card by:
• dialling +45 80 30 70 10 (24 hours a day);
• visiting www.nemid.dk (24 hours a day), or
• contacting your bank or local citizen service centre (if your NemID is associated with an OCES certificate). You can also order a new code card.

You can use the self-service function at www.nemid.dk at any time to check the time that your password and/or your code card were 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 it has been entered incorrectly a certain number of times;
• code card, if DanID suspects or finds out that others have gained access to the codes on your code card;
• NemID, if DanID finds out that 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 when your password, code card or NemID has been blocked
When your NemID or password has been blocked, you are no longer able to use NemID. If only your code card has been blocked, your online banking service may allow you limited access. For instance, you may be able 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 services that have registered for NemID.

3.7 Processing 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 email address to notify you of any blocking if this has been provided.

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

To be able to investigate any fraud, DanID logs the time when you use NemID as well as the IP address and other data related to the computer used by you to log on.

If you use the self-service function at www.nemid.dk and select to have where you used NemID recorded in the activity log, DanID will also log the service providers with which you have used NemID.

You can always unsubscribe from the activity log, 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 this period, the data 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 solutions
Interactive voice response (IVR) is a solution 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 have been specified in these conditions.

This means that:
- you must ensure that the telephone on which you receive codes is not in any way connected to the computer/telephone you 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 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 email address with DanID, you will be notified of the amendments by email. Other amendments will be announced at www.nemid.nu no later than three months before becoming effective.

4 SPECIAL CONDITIONS APPLYING TO OCES CERTIFICATES
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.

You may request different NemIDs, code cards and user IDs for your online banking service and your public digital signature.

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 CPR number to the public PID (Personal Identification) service at the National IT and TeleAgency (IT-og Telesstyrelsen). The PID service is used by public service providers for identification purposes. A private service provider may retrieve your CPR number subject to your approval when you log onto the service provider’s site; and
- DanID may use the public PID service to retrieve the PID number of a previous digital signature.

When you use NemID through your online banking service and wish to use NemID as a public digital signature, you confirm that your bank can pass on – and DanID use – your personal data (name, address, CPR number and, if provided, email address and mobile phone number) to issue and manage your public digital signature.

If you have requested a NemID in connection with the issuing of a public digital signature, and you 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 for 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, or you can terminate the 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 and for any other online banking services.

4.2 Your obligations as the holder of an OCES certificate
You must ensure that the name and email address 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 certificate within 30 days. If you do not renew the OCES certificate within 30 days, and DanID becomes aware that the information is incorrect, your certificate will be blocked by DanID.

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 request that it be blocked; or
- DanID becomes aware that you have failed to comply with the 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 email or by a letter sent to the address listed in the National Register of Persons. If DanID has access to your public PID service, 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 cause of the blocking by signed email and by letter if this possible.

4.4 Renewing your OCES certificate
The period of validity will be shown on your OCES 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 email 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 DanID’s liability towards you when you receive digitally signed data
If you receive digitally signed data, for example because you exchange digitally signed emails or documents, you must, before you accept the OCES certificate, check that the sender’s 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; and
- its use complies with any restrictions shown on the OCES certificate.

4.6 DanID’s liability towards you when you receive digitally signed data
DanID’s liability for misuse shall be subject to Danish legislation. 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 solved by negotiation shall be brought before the City Court of Copenhagen.

4.7 DanID’s liability towards 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 and the losses are caused by an error on DanID’s part in connection with registering, issuing or blocking the certificate. DanID shall not liable for any loss, if DanID can prove that DanID’s has not acted negligently or intentionally.

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