SKJERN BANK

Rules for Skjern Bank's e-Banking - Private

Skjern Banks e-Banking is the general term used for the electronic self-service functions (eBanking functions) offered by Skjern Bank, for instance Skjern Banks Netbank and Skjern Banks Mobilbank.

The rules for Skjern Banks e-Banking are supplemented with special rules for individual functions, for which there are deviations from the rules for Skjern Banks e-Banking. The rules for Skjern Banks e-Banking and the special rules for the individual functions supplement Skjern Banks General terms and conditions.

Feel free, at any time, to contact Skjern Bank to obtain a copy of these rules, and also, you find the rules in your Netbank and on www.skjernbank.dk.

1. General

You can find answers to most questions, read instructions on the technical requirements for applying the functions and get information on the latest updates at www.skjernbank.dk.

2. Registration

You may have limited access to the functions in Skjern Bank's e-Banking. If you wish to have access to more functions, you can sign up in Skjern Bank's e-Banking or you can contact Skjern Bank.

Depending on the function you register for, you can use the function immediately after you have registered for it or once you receive a message from Skjern Bank.

The first time you use a function in Skjern Bank's e-Banking, you must electronically accept the rules for Skjern Bank's e-Banking and/or the special rules applying to the function.

Skjern Bank is not obliged to allow you access to the functions in Skjern Bank's e-Banking, and Skjern Bank may decide only to offer you specific functions or part of these.

Access to Skjern Bank's e-Banking in connection with accounts opened according to the Danish Payment Accounts Act (Lov om betalingskonti) is, however, subject to special rules.

3. Consent to processing of personal data according to the Danish Act on Payments (lov om betalinger)

When you accept Rules for Skjern Bank's eBanking - private, you also accept that Skjern Bank will process personal data, for instance, civil registration number (CPR) and account details, about you in connection with the use of the individual self-service functions.

Processing of data about you will solely take place for purposes that are necessary for you to use the self-service functions activated, for instance, execution of payments and preparation of payments overviews.

Skjern Bank gathers the relevant personal data from you shops, financial institutions and others.

By contacting your branch, you can at any time revoke your consent to the processing of your personal data.

However, please be aware that, if you revoke your consent, you can no longer use the self-service functions.

If you would like to learn more about how we process your personal data, we refer to our full personal data policy on www.skjernbank.dk.

4. Cookies

Skjern Bank uses cookies and similar technologies in its electronic self-service functions. Cookies are used for both technical and statistical purposes.

If you set your browser to block cookies, it is not possible to log in to Skjern Banks Netbank.

In Skjern Banks Netbank and Skjern Banks Mobilbank we prepare statistics anonymously to make our self-service solutions even better. Read more about Skjern Bank's use of cookies and similar technologies, and how to delete them at skjernbank.dk - under "Regler og betingelser".

5. Power of attorney

You may in writing authorise another person to access your accounts with Skjern Bank or part of them. The person must have signed up for Skjern Banks e-Banking.

You must execute a power of attorney via power of attorney forms for Skjern Banks e-Banking. A power of attorney is effective until you notify Skjern Bank in writing of the revocation.

Once you have signed up for Skjern Banks e-Banking, you may also be granted a power of attorney and get access to other clients' accounts or part of them.

If you are under the age of 18, you cannot be granted a power of attorney for other clients' account(s).

We automatically delete the access of an agent under a power of attorney to accounts of clients under 18 at the 18th birthday of the principal under the power of attorney.

An agent is generally allowed access to and can register for the same functions as the principal, but a few functions will not be available to the agent.

The access of custody account holders to trade various types of securities also applies to the agent, if any.

Transactions performed by an agent are binding as if the transaction had been performed by the principal. The power of attorney granted by the principal to the agent is of no concern to Skjern Bank.

If you have authorised another person to access your accounts, this person also has access to Netboks which contains both historical and future documents. You should be aware that an agent under the power of attorney may be authorised on your behalf to select and deselect hard-copy prints in your e-Banking.

6. Third party provider

You are entitled to make use of payment initiation services or account information services to access your payment accounts that are available online.

You can use a payment initiation service to initiate, on your behalf, payments from your payment accounts.

You can use an account information service to provide you with consolidated information on your payment accounts with Skjern Bank.

You must enter into a separate agreement with and give express consent to the third party provider before this can gain access to render its services.

7. Personal security solution

Certain functions in Skjern Banks e-Banking require that you apply a personal security solution.

Basically, NemID is used, which is provided by Nets DanID A/S.

If you do not already have NemID, you will get NemID which is to be applied as Skjern Banks security solution in connection with registration for certain functions in Skjern Banks e-Banking.

The NemID conditions 1-3 form part of the rules on the use of Skjern Banks e-Banking. You may view the existing NemID conditions at nemid.nu at any time. The NemID conditions 1-5 can be seen below.

If you state your mobile phone number in connection with registration for or use of the functions in Skjern Banks e-Banking,

D00PDFXEBREGLP/6.1

Skjern Bank will save your mobile phone number for administrative purposes and Skjern Bank will pass on the mobile phone number to Nets DanID A/S, which manages NemID.

If you get a new mobile phone number, it is your responsibility to change your mobile phone number in Skjern Banks Netbank and Nets DanID A/S' website nemid.nu.

If, at a later point in time, you wish to use NemID to provide your digital signature or you would like support in connection with this function, please contact Nets DanID A/S via the website nemid.nu or your local citizen service centre.

If for this function you need another type of personal security solution, this will appear from the special rules applying to the function.

8. Transactions under your commitment

In Skjern Banks e-Banking you can have access to your present and future account(s) with Skjern Bank.

If you have access, you can see and operate your account(s) in the same way as if you contact Skjern Bank. If you have chosen not to have access to operating your account(s), you will only be able to see but not operate your account(s).

If you are under 18, you can only view accounts in your name and operate accounts where the deposited amounts are generated by independent employment unless your guardian(s) has/have accepted in writing that you can operate other accounts.

Some of your accounts may be subject to limitations in authority.

Skjern Bank's e-Banking allows you to execute payments at a maximum amount of DKK 25.000 per banking day to a third party regardless of the payments being executed from your own accounts or from accounts that you are authorised to operate.

If you are under 18, your total maximum per day is DKK 10.000.

If you have registered a mobile phone number with the Bank, the Bank may use this in connection with executing certain transfers and payments. You can see the mobile phone number in one or more of Skjern Banks e-Banking functions. You are responsible for updating your mobile phone number in the individual e-Banking function if it changes.

The Bank may, for instance, use your mobile phone number to send you an SMS if a payment or transfer cannot be executed.

You may also experience that you need to approve certain transfers or payments more than once. This may be prompted by enquiry from the Bank or by an SMS code sent to you If you receive an SMS code, this must be entered in the individuel e-Banking function to execute the transaction.

In the event of other limitations to the application of the individual functions, the limitations appear from the special rules applying to the function.

9. Payment execution

In Skjern Banks e-Banking a payment order has been received when you receive an acknowledgement of this in the individual e-Banking function. You can find information om the maximum time it takes to execute a payment on the "Deadlines" page in the Netbank.

On the "Deadlines" page you can also see when to confirm your payments at the latest in order for these to be executed on the same day.

Information on cross-border transfers as well as transfers in another currency than DKK can be found in Terms and conditions - International Payments which is available on www.skjernbank.dk.

10. Stop payment

You can stop payments as long as the stop function of the individual payment is active.

You can also stop recurring payments and payments from Betalingsservice (Payment Service). The deadlines for revoking the different payments and transfers appear from the page "Deadlines" in the Netbank. Revocation is made by activating the stop function in the screen with details of the individual payment.

You find information on cancellation of payments and payment agreements in Betalingsservice (Payment Service) in "General conditions for Betalingsservice debtors" at www.betalingsservice.dk. The conditions are also available at www.skjernbank.dk and in your Netboks.

11. Coverage requirements

Skjern Bank is not obliged to execute your payments from accounts for which there are insufficient funds to cover the amount. Skjern Bank may therefore refuse to receive payment orders from your if there are insufficient funds in the account from where the payment is to be executed.

12. Spending overview

Through some of the functions in Skjern Banks e-Banking you can see a spending overview of your expenses broken down into different categories. Skjern Bank uses a number of standard categories, but you can re-categorise your expenses as you like. The Bank uses uses payment details about recipients of your payments or transfers and in which places you have used your payment cards to generate the spending overview. The spending overview is solely available to you. You can at any time deactivate the spending overview in the functions in Skjern Banks e-Banking where spending overview is available.

13. Budget

In Skjern Bank's Budget you can make different calculations for budgeting purposes.

You can, among other things, prepare a budget on the basis of you payment agreements, create manual budget items and perform budgetary follow-up.

The calculations in Skjern Bank's Budget only serve as an indicative calculation for your budget preparation.

Your budget can only be seen by you. You may, however, choose to give Skjern Bank access to your budget.

Skjern Bank has no responsibility for all relevant debt items and amounts being included in the budget or for the correctness of these.

Hence, Skjern Bank cannot be held liable for any transactions made on the basis of the calculations in Skjern Bank's Budget.

You can delete your budgets on the "Budget" page in Skjern Banks Netbank.

If you delete a budget, you must be aware that subsequently it cannot be restored and Skjern Bank cannot print it for you.

14. Electronic signatures on agreements

Your NemID is your electronic signature and it is legally binding in the same way as your signature on a physical agreement. Therefore your NemID is personal and must not be used by others.

There may a deadline by which an agreement must be signed in the Skjern Banks Netbank. If you do not sign the agreement by this date, the agreement will no longer be available in Netboks.

Electronically signed agreements will be saved in your Netboks.

15. Support

Skjern Banks Hotline is hosted by employees who can offer you advice and answer your questions relating to the use of functions in Skjern Bank's e-Banking.

You can contact Skjern Bank's Hotline by phone at +45 96 82 14 44 or by email at ebanking@skjernbank.dk.

You can see the opening hours of Skjern Bank's Hotline at www.skjernbank.dk.

16. Blocking

You are obliged without delay to block the functions of Skjern Bank's e-Banking, if you suspect or become aware of abuse or the possibility of unauthorised use or attemped abuse of the functions of Skjern Bank's e-Banking.

You can always block the functions of Skjern Bank's e-Banking by contacting one of Skjern Bank's branches or Skjern Bank's Hotline. Other possibilities of blocking the function(s) appear from the special rules for the relevant function(s).

You should be aware that blocking of functions in Skjern Bank's e-Banking will not at the same time block your NemID. You can read about blocking of NemID at nemid.nu.

17. Responsibility for private accounts

The responsibility of unauthorised use of Skjern Bank's e-Banking is governed by the rules in the Danish Act of Payments.

If you are under the age of 18, the responsibility for unauthorised use furthermore follows the rules pertaining to minors' liability to pay damages in the Danish Guardianship Act.

You are liable up to the sum of DKK 375 for losses arising from other people's unauthorised use of your access to the functions of Skjern Bank's e-Banking, where a personal security solution has been used.

You are liable up to DKK 8,000 for losses arising from other people's unauthorised use of the functions in Skjern Bank's e-Banking, if Skjern Bank documents that a personal security solution has been applied, and you

- failed to notify Skjern Bank as soon as possible after having become aware that a personal security solution has been lost or become known to an unauthorised person, or

- you intentionally disclosed the details about a personal security solution to the person who made the unauthorised use of the function where you did not realise or should have realised that there was a risk of unauthorised use, or

- by gross negligence have enabled unauthorised use.

You are liable without limit for losses arising from unauthorised use of Skjern Bank's e-Banking by others, where Skjern Bank documents that a personal security solution was used and you intentionally disclosed the details about your personal security solution to the person who made the unauthorised use of the function where you realised or should have realised that there was a risk of unauthorised use.

You are also liable without limit for losses where you acted fraudulently, intentionally or neglected your obligation to protect your personal security solution or failed to block the functions in Skjern Bank's e-Banking.

You not liable for unauthorised use of Skjern Bank's e-Banking, which takes place after Skjern Bank was informed that

- the personal security solution was lost, or

- an unauthorised person gained knowledge of your personal security solution, or

- for other reasons, you wish to have the function or functions in Skjern Bank's e-Banking blocked.

In addition, you will not be liable for any unauthorised use of Skjern Bank's e-Banking when such use was caused by acts carried out by employees of the Bank, agents or branches or a unit to which the Bank's activities have been outsourced, or due to the inactivity or non-action on the part of the above.

In addition, you will not be liable if the loss, the theft or the fraudulent appropriation of the personal security solution could not be detected by you prior to the unauthorised use.

Skjern Bank is, according to the Danish Act on Payments, liable for your losses if the payment recipient knew or should have known that Skjern Bank's e-Banking had been subject to unauthorised use.

Skjern Bank is also, according to the Danish Act on Payments, liable for your losses due unauthorised use where Skjern Bank does not require use of the personal security solution unless you acted fraudulently.

You are only responsible for losses arising from the unauthorised use of Skjern Bank's e-Banking by other people if the transaction has been correctly registered and booked with Skjern Bank.

After you have realised the unauthorised use, you must without delay submit your objection against the unauthorised use or your suspicion in this respect to Skjern Bank. This shall also apply if the unauthorised use took place in connection with the use of payment initiation services. 13 months after the debiting of the unauthorised use you can in no circumstances raise an objection.

Skjern Bank considers your objection and meanwhile we will normally credit your account temporarily with the objected amount If it is not another person's unauthorised use of Skjern Bank's e-Banking, we will debit your account with the amount again. Skjern Bank may claim interest subject to the rate of interest applicable to the account over the period during which the amount was temporarily deposited to your account.

In Skjern Bank's assessment as to whether you should have been aware of the unauthorised use, we may take into account that the Bank issues monthly statements of account to your Netboks, and that you have access to transactions in Skjern Bank's e-Banking.

For further information on how to submit objections, please see www.skjernbank.dk.

18. Liability for business accounts

Skjern Bank is not liable for losses on corporate of Skjern Bank's e-Banking or the functions of Skjern Bank's e-Banking.

Linking business accounts in Skjern Bank's e-Banking is at your own risk. You may cover the risk by taking out insurance.

Personal accounts used for business purposes are considered corporate accounts and are consequently subject to the same liability provisions as corporate accounts.

Should Skjern Bank suffer any losses due to unauthorised use of corporate accounts in Skjern Bank's e-Banking, the account holder will be liable for this.

19. Changes to the rules

Skjern Bank will change the rules of the functions of Skjern Bank's e-Banking without notice provided that the changes are of no disadvantage to you.

For any other instances, Skjern Bank will change the rules of the functions in Skjern Bank's e-Banking subject to two months' notice. Unless the changes are for security reasons and unless the changes relate to the limits for payments per 24-hour period, which will be effective without notice.

You will be informed about any changes by letter or electronically, for instance in Netboks.

You may be asked to accept the changed rules when logging on or the first time you use the function after the change has come into effect. Any changes of the rules will be deemed accepted, unless you inform Skjern Bank before the date of the changes coming into force that you do not wish to be bound by the new rules. If you do not wish to be bound by the new rules, the agreement will be terminated with effect from the date when the new rules come into force.

20. Termination and cancellation

This agreement shall be in force until terminated by you or by Skjern Bank.

You can always cancel the functions of Skjern Bank's e-Banking or terminate the agreement in writing and without notice.

Skjern Bank may close your access to the functions in Skjern Bank's e-Banking or terminate the agreement with two months' notice.

In the event of the death of you or the principal under a power of attorney, or where you or the principal are/is administered in bankruptcy, file(s) for debt restructuring or debt rescheduling or initiate(s) some other form of insolvency proceedings, the access to Skjern Bank's e-Banking will immediately be closed and orders will not be executed.

In addition, your access to Skjern Bank's e-Banking will be terminated without delay and orders will not be executed if Skjern Bank suspects your or another person's unauthorised use of the

D00PDFXEBREGLP/6.1

functions in Skjern Bank's e-Banking, or other security threats, or if you default on your commitment or account(s) or part of them with Skjern Bank.

In the event of or actual instances of unauthorised use or security threats, the Bank may contact you by telephone or in another secure way.

21. Complaints against the Bank

If you want to file a complaint against the Bank, please contact Skjern Bank's complaints officer. If a complaint is not upheld, complainants may contact The Danish Financial Complaint Board(Det finansielle ankenævn).

You may also complain to the authorities that supervise the Bank's compliance with the Danish Act on Payments. The Danish Consumer Ombudsman supervises compliance with disclosure requirements in connection with the execution of payment services, rights and obligations when using payment services, the use of payment data and disclosure of fees. The Danish Competition and Consumer Authority supervises compliance with the rules governing fees in general.

22. Fees

Fees incurred on use of functions in Skjern Bank's e-Banking are stated in the price list available in Skjern Banks Netbank and at www.skjernbank.dk. Any fees are payable at the end of each month.

The fees will be stated in your Account entries and on your statements of account in the Netbank.

23. Right of cancellation

You may cancel this Agreement subject to the Danish Consumer Protection Act within 14 days after the Agreement was signed. You can read about this in Skjern Bank's "Information on the right of cancellation", which is available in your Netboks and at www.skjernbank.dk.

SKJERN BANK

Rules for Skjern Banks Netbank - private

Skjern Banks Netbank is your electronic branch of Skjern Bank.

In Netbank the functions are added and developed on an ongoing basis, and, among other things, you can:

- communicate with Skjern Bank
- see your documents from Skjern Bank in your Netboks.
- see account entries on your acounts
- monitor your balance of account and get an overview of your spending
- prepare a budget
- see your payment cards
- transfer money - also to other countries
- pay bills using 'indbetalingskort'/Giro payment
- follow the development of your custody accounts
- buy and sell securities
- sign up for Mobilbank
- use Beskedservice(text message)
- administer e-Banking - and see which functions you have used.

You may have limited access to the functions in Jyske Netbank. If you wish to have access to more functions, you can sign up in Jyske Netbank or you can contact your Jyske Bank branch.

1. Personal security solution

In order to use Skjern Banks Netbank you must use NemID which consists of a user ID, a password and a code card/code token.

It is also possible to install a NemID code app on a mobile device (for instance a smartphone or tablet) and use this as a code.

You must, however, keep your code card to be used in situations where the app or your mobile device is not accessible.

Your user ID, your password and your code card/code token/code app are personal and must be used solely by yourself. Consequently, your user ID, password and code card/code token/your PIN for your code app must be stored in such a way that they are not disclosed to others.

In the Netbank you are free to decide whether you want to use a code from your code card/code token/code app in connection with login. If you do not want to use a code in connection with login, you will solely be asked to enter user ID and password in connection with login.

If you have chosen that the Netbank should ask for a code in connection with login, you will not be prompted to enter a code to approve a transaction. You only need to enter your password to approve a transaction.

If, on the other hand, you have chosen that the Netbank should not ask for a code in connection with login, you will be prompted to enter a code to approve the first transaction. Hereafter you will only need to enter your password when you approve a transaction.

Approval of transfers between your own accounts and accounts for which you have a power of attorney does not require a password or code from your code card/code token/code app.

When entering a payment instruction in Skjern Bank's e-Banking it will be stated on the screen which details must be entered for the instruction to be executed correctly, for instance reg. No. (sort code) and account number.

You can use Skjern Banks Netbank every day, but Skjern Banks Netbank is closed the night between Saturday and Sunday between 02:00 CET and 06:00 CET and all others days between 03:00 CET and 05:00 CET.

2. Communication with the Bank

You can write to your branch or account manager through Skjern Banks Netbank. Communication via Skjern Banks Netbank is encrypted to prevent others from seeing it.

If you write after 12:00 CET, your inquiry may not be read or executed on that banking day.

3. Other functions

The page "Agreements" shows an overview of the functions that you have signed up for in Skjern Banks e-Banking and which require a separate agreement.

4. Blocking an unblocking

You can block your access to Skjern Bank's e-Banking and Skjern Banks Netbank

- in Skjern Banks Netbank on the page "Security and NemID"
- by contacting Spærreservice (Blocking Service) (available 24 hours a day) at tel. +45 75 94 50 93, stating that you are a client with Skjern Banks Netbank.

Your access cannot be unblocked by Spærreservice (Blocking Service).

When blocking your access to Skjern Banks Netbank, you receive a written confirmation of the blocking with an indication of the time when the access was blocked. Together with the confirmation you receive a form that you must return to Skjern Bank in order to unblock your access. You must hand in or forward the form to Skjern Bank, when you wish to have your access unblocked.

D00PDFXEBREGLP/6.1

Rules for Skjern Banks Mobilbank

1. Registration and deregistration

Once you register for Skjern Banks Mobilbank, you have access to many of the functions also available in Skjern Banks Netbank. The functions of Skjern Banks Mobilbank will be developed on an ongoing basis. When signing up you will be given a 6-digit mobile code. You must use the code together with your user name when you log on to Skjern Banks Mobilbank. You can always see your mobile code -and change your code - in Netbanken.

If you have a telephone/tablet that supports the use of a biometric solution, for instance, fingerprints, you can use this biometric solution to remember your mobile code to the extent that Skjern Banks Mobilbank supports this kind of use. You can activate the biometric solution under settings in Skjern Banks Mobilbank.

Generally, your user ID and your mobile code are personal and must not be disclosed or used by any other person than yourself. This is also the case if you use a biometric solution to remember your mobile code.

You can at any time deregister Skjern Banks Mobilbank in Netbanken.

1.1. Management and approval of payments and trades

Any payments you make through Mobilbank are included in the maximum daily amount available to you through Skjern Banks e-Banking.

Please note that you may be requested to update Mobilbanken before log-on.If so, you will receive a message.

When entering a payment instruction in Skjern Banks Mobilbank it will be stated on the screen which details must be entered for the instruction to be executed correctly, for instance reg. No. (sort code) and account number.

When you have entered a payment instruction or an order for a securities transaction in Mobilbank, you must authorise this with your mobile code and a code from your NemID code card or your NemID code token/code app. However, transfers between your own accounts and accounts for which you have a power of attorney do not require approval. Once you have made a securities transaction, you will receive confirmation on your mobile units, provided the call was not ended or interrupted. If you do not receive a confirmation, you have to contact Skjern Bank to find out whether the order was executed.

1.2. Blocking and cancellation of blocking

You must without delay block your access to Skjern Banks Mobilbank, if you become aware of or suspect irregularities or misuse of your Mobilbank, and if you lose your mobile unit. If Netbanken is blocked, Mobilbanken will also be blocked.

You can block your access to Skjern Banks Mobilbank

- in Skjern Banks Netbank on the page "Security and NemID"

- by contacting Spærreservice (Blocking Service) (available 24 hours a day) at tel. +45 75 94 50 93, stating that you are a client with Skjern Banks Netbank.

You can unblock your blocking of Mobilbank in Skjern Banks Netbank.

We recommend that you activate the keypad lock on your mobile units in order to avoid unauthorised use.

D00PDFXEBREGLP/6.1

SKJERN BANK

Rules for Skjern Bank's Beskedservice (text messages)

Skjern Bank's Beskedservice (text messages) offers you an opportunity to receive a message from the Bank through one or more media (for instance e-mail or SMS/text message). You are free to select which messages you want to receive.

Read more about Skjern Bank's Beskedservice under the Help tab in the Netbank.

1. Registration and deregistration

When you register, you approve the Service that you register for with your NemID as well as the medium on which you want to receive the message.

When you register a medium for Skjern Bank's Beskedservice (text messages), you receive a receipt of the registration on the medium that you have registered. If the information about your medium (for instance mobile phone number or e-mail address) is changed, you are responsible for updating such information in Skjern Banks Netbank.

You receive messages through the medium until you deregister from Skjern Banks Beskedservice on the "Beskedservice" page in Skjern Banks Netbank. You can deregister from Beskedservice without notice.

If you have registered Skjern Banks Beskedservice for an account, to which you have a power of attorney, the account will automatically be deregistered from Skjern Banks Beskedservice if your power of attorney is revoked.

D00PDFXEBREGLP/6.1

Sections 1-5 in 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 solution (Interactive Voice Response) 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.

It is also possible to install a NemID code app (hereinafter code app) on a mobile device (for instance a smartphone or tablet) and use this as a code. You must, however, keep your code card to be used in situations where the app or your mobile device is not accessible.

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 your 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 Act on Payments (lov om betalinger) 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 these conditions at www.nemid.nu.

Nets DanID refers to Nets DanID A/S, Business Reg. No. (CVR) 30808460

Unit refers to the unit from where NemID is used, e.g., PC, mobile phone 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 obliged to provide sufficient and correct information.

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

Please note that:

- your user ID, password and code card/code token/your PIN for your code app must be stored securely to prevent others from using them
- you may not disclose your password or your codes, or your PIN for your code app, 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/your PIN for your code app
- you may not store the password together with your code card/code token or on the mobile device on which your code app is installed or write the password on your code card/code token.
- you may only install your code app on your own mobile device

3.3. Security when using NemID

You must make sure that:

- your user ID, password and code card/code token/code app are only used by you and only in accordance with the conditions
- others cannot read your password or PIN when you enter it
- you use NemID on a computer where the operating system, Internet browser and other programmes are regularly updated with the latest security updates.

You must regularly check that you have not lost your code card /code token/your mobile device on which the code app is installed, 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. Temporary password

The first time you register for NemID, you will receive a temporary password that you can use to log in. This also applies if you have blocked your password; see Section 3.5 on blocking.

If you suspect that others have knowledge of your temporary password, e.g., if the letter with the temporary password has been tampered with, you should immediately request a new temporary password from Nets 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 your lost code card/code token, it must be destroyed.
- your code app if you have lost the mobile device on which it was installed, or if you suspect that others have access to your code app, or others have installed a code app with your NemID
- 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 - what to do

When you block your password and/or code card/code token/code app, you must provide your name, address and civil reg. no. (CPR) as required, or your user ID, or code card number, code app number, or code token number. You must also indicate whether you want to block your password or the codecard/code token/code app.

When you have blocked your password, Nets DanID will send you an acknowledgement, stating the time and cause of the blocking.

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

- visiting www.nemid.nu (round the clock), dialling: +45 72 24 70 10 (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/code app was blocked and the reason why.

3.5.3. Blocking by Nets DanID
Nets DanID will block your

- password if Nets DanID suspects or learns 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/code app if Nets DanID suspects or learns that others have gained access to codes from your code card/code token/code app

- Your code app if Nets DanID suspects or finds out for certain that the mobile device that you are using has been compromised or has significant security gaps.

- NemID, if Nets DanID learns that you have not complied with the conditions for NemID

- NemID, if the information you provided when registering for NemID is incorrect, or

- NemID, if Nets 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/code app has been blocked, some banks may allow you limited access to your netbank, 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, Nets DanID will process your personal data on behalf of the Bank. Nets DanID will process your data, i.e., name, address and civil reg. no. (CPR), to be able to identify you. Nets DanID will also use your e-mail address, if you have provided one, to notify you of any blocking, for example.

If your mobile phone number is registered with Nets DanID, Nets DanID will use your mobile phone number to send you text messages regarding NemID, for instance, messages regarding temporary passwords.

Log files can be saved on the user's unit whenever NemID is used. The user may delete these if desired. As part of the security Nets DanID registers the times that you use NemID, the IP address and any other information about the unit from which you use NemID.

Read more about log files and security on https://www.nemid.nu/dk-da/om-nemid/sikkerheden_bag_nemid/.

If you use the self-service function at www.nemid.nu and choose to record where you have used NemID in the activity log, Nets DanID will also log the service providers with which you have used NemID. You can always deactivate this registration in which case Nets DanID will no longer log where you have used NemID. Nets 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 Nets 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.
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
Nets 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. Other amendments will be announced on www.nemid.nu no later than three months before becoming effective.

4. Special rules regarding public digital signature

- If you choose to use NemID for public digital signature, the conditions in Section 4 supplement the conditions in Section 2 and 3.

- You can ask for different NemIDs and thereby also different code cards/code tokens and user IDs to use for your online banking solution and your public digital signature, respectively.

4.1. Processing of personal data
When you have an OCES certificate issued and linked to NemID, you accept

- that Nets DanID makes a search in the CPR register to retrieve your name and your address

- that Nets DanID discloses the connection between your public digital signature and your civil reg. no. (CPR) to the public PID service at the Danish Agency for Digitisation (Digitaliseringsstyrelsen). The PID service is used for searches from public service providers to identify you. A private service provider can only have your civil reg. no. (CPR) disclosed if you accept this when you log on to the service provider

- that Nets DanID makes searches in the public PID service to retrieve any PID number from a previous digital signature.

When you have registered for NemID in connection with your online banking solution and you also want to use NemID for public digital signature, you also accept that the Bank discloses your personal details (name, address, civil reg. no. and any e-mail address and mobile phone number) to Nets DanID so that Nets DanID can use your information to issue and manage your public digital signature.

When you have received NemID in connection with the issue of public digital signature and you also want to use NemID for your online banking solution, you at the same time accept at the enquiry of the Bank that Nets DanID discloses information about NemID to your bank so you can use NemID in your online banking solution.

If you no longer want your personal information and/or information about NemID to be processed as described above, you can either block your public digital signature by contacting Nets DanID or a citizen service centre and/or close your access to your online banking solution by contacting your bank.

If you block your public digital signature, you can only use NemID in your online banking solution; if you close your

access to your online banking solution, you can only use NemID for public digital signature.

4.2. Your obligations and your responsibility as owner of a public digital signature with an OCES certificate
You must make sure that information about name and any e-mail address in the OCES certificate is correct.

If the information that appears from the OCES certificate is changed - for instance if you change your name - you must within 30 days renew your OCES certificate. If the OCES certificate is not renewed within 30 days and Nets DanID is aware that the information is not correct, Nets DanID blocks your OCES certificate.

You cannot use your OCES certificate to issue certificates to others.

4.3. Blocking of your OCES certificate
Nets DanID will block your OCES certificate if

- you ask Nets DanID to do so
- Nets DanID learns that you have not complied with the conditions for NemID.

When you block your OCES certificate, Nets DanID will send you an acknowledgement that the blocking has been completed, either in a signed e-mail or in a letter to your registered address if Nets DanID has access to it. If Nets DanID does not have access to your registered address, the acknowledgement is sent to the address that you have registered with Nets DanID. If Nets DanID blocks your OCES certificate without you having requested it, Nets DanID will notify you about the reason in a signed e-mail if possible.

4.4. Renewal of your OCES certificate
The validity period of the OCES certificate appears from your OCES certificate. An OCES certificate is valid for up to four years. No later than four weeks before the OCES certificate expires, Nets DanID will notify you in an e-mail or in a letter to your registered address if Nets DanID has access to it. Before the validity period expires, you may renew your OCES certificate by using the old OCES certificate. If your OCES certificate has expired or is blocked, you must order a new certificate.

4.5. Obligations and duties when you receive digitally signed data
If you receive digitally signed data, for instance because you exchange digitally signed e-mails or documents, you must, before you trust the OCES certificate, make sure that the sender's OCES certificate

- is valid - i.e. that the validity period, which appears from the OCES certificate, has not been exceeded
- is not blocked - i.e. that it is not listed on Nets DanID's blocking list at Nets DanID's website
- is used in accordance with any application limitations which appear from the OCES certificate.

4.6. Nets DanID's liability towards you as owner of an OCES certificate
Nets DanID's liability for damages in case of unauthorised or fraudulent use follows the general rules of Danish law. Nets DanID is not liable for losses if you did not comply with the NemID conditions. You must claim any damages relating to your OCES certificate from Nets DanID. The NemID conditions are subject to Danish law. Any discrepancies between you and Nets DanID, which cannot be resolved by negotiation, may be brought before the City Court of Copenhagen.

4.7. Nets DanID's liability to you when you receive digitally signed data
Nets DanID is liable for losses you suffer when you reasonably trust a sender's OCES certificate if the loss is caused by Nets DanID making a mistake in connection with registration, issue and blocking of the certificate. Nets DanID is not liable for losses if Nets DanID can establish that Nets DanID did not act negligently or intentionally.

5. Additional information
If you need additional information about NemID and public digital signature, please contact your bank, your citizen service centre or Nets DanID. You can also learn more on www.nemid.nu where key concepts are explained and here you can, as well, learn more about certificate technology.

Valid from 13 January 2021

Translation

The above is a translation of the Danish "Regler for Skjern Banks e-Banking - privat". In case of doubt the Danish original applies.