

Special Terms and Conditions for Business eBanking

(Please note that these Special Terms and Conditions apply in addition to the General Terms and Conditions for Business. In the event of a conflict between these Special Terms and Conditions and General Terms and Conditions for Business, the General Terms and Conditions for Business prevail.)

Introduction

Business eBanking is our Internet-based office-banking system, which provides access to account information, payments and other banking transactions requested by our business customers such as you.

These Terms and Conditions for Business eBanking include a description how Business eBanking operates.

Part 1: describes the options available in Business eBanking and how to use the system.

Part 2: describes the security requirements for Business eBanking users.

Part 3: sets out some contractual aspects for connecting to Business eBanking.

Part 1-Business eBanking - general description

1. Modules and services

Business eBanking comprises separate modules and services. The Module Description comprises a description of the modules and services available via your Access Agreement.

2. Transactions

Business eBanking allows you to, for example, make payments and queries on balances and movements

in accounts registered in Business eBanking via the Access Agreement. Payments and queries are jointly referred to as “**transactions**”. Use of your Electronic Signature in accordance with the Special Terms and Conditions for Electronic Signature shall be your authorisation of and consent to payments through the Business eBanking service.

3. Registered accounts

3.1 Accounts must be registered in Business eBanking before you can make transactions via Business eBanking. Accounts are registered via the Access Agreement.

3.2 The following accounts can be registered in Business eBanking: (a) Accounts held by you and opened in your name with the Bank and affiliates and divisions of the Danske Bank Group, (b) Accounts held by third parties, including subsidiaries, provided that the third party or subsidiary has issued a third-party mandate to you authorising you to act on behalf of the third party or subsidiary.

3.3 Registered Accounts within the Danske Bank Group can also be managed via SWIFT MT101 or MT940; see Clause 3.4 for further details.

3.4 Accounts opened with banks outside the Danske Bank Group, and accounts within the Danske Bank Group which you wish to use for transactions via SWIFT MT101 or MT940,

can also be registered in Business eBanking via the Access Agreement. You may register both your own accounts and third-party accounts. You or third party must conclude an agreement with the account-holding bank concerning payment requests via MT101 or an agreement on balance reporting via MT940.

4. Unregistered accounts

If accounts held by you and/or a third party are not registered in Business eBanking, it is only possible to make payments into those accounts. It is not possible to inquire about or make payments from unregistered accounts.

5. Foreign Drafts

You may make payments by issuing a draft drawn on a Registered Account within the Danske Bank Group.

If you and/or a third party has an agreement concerning payment requests via MT101, drafts can also be drawn on Registered Accounts outside the Danske Bank Group, provided that this option is included in the agreement between you and/or third party and the bank outside the Danske Bank Group.

Issued drafts are regarded as banker's drafts, and the amounts are debited from the accounts on the date of issue.

You may have the proceeds of uncashed drafts deposited in Registered Accounts. If the proceeds from uncashed drafts are to be credited to your or a third-party's account, you or the third party must covenant to indemnify the Bank if a draft is subsequently presented.

6. Requests

A request by you or your Users for a transaction in Business eBanking, for example a payment, is called an electronic request.

6.1. Submission of requests

When a User submits an electronic request on your behalf and/or on behalf of a third party, we send an electronic receipt. The moment we have confirmed receipt of the request, the risk in relation to it being carried out in accordance with the instructions passes to us.

If a payment is authorised on your behalf but provides an incorrect Unique Identifier to us to identify the payee, we will not be liable if we process the payment in accordance with that Unique Identifier, but we will make reasonable efforts to recover the funds involved however, you agree that we may charge for this.

If we refuse to execute a payment authorised on your behalf via our Business eBanking Service, we shall notify you of this refusal as soon as

Danske Bank A/S (trading as National Irish Bank) is authorised by The Danish FSA in Denmark. Details of all Danske Bank A/S directors can be viewed at its registered offices.

possible by telephone, in writing, by email, by fax or such other reasonable means we may select.

6.2. Binding requests

Requests carried out in accordance with the instructions in the electronic request are binding on you. Consequently, we cannot reverse payments, trades in foreign exchange or securities or other transactions, including draft issuance, finalised in accordance with the electronic request.

6.3. Retention of requests

We retain electronic requests for at least seven years. During this period, you and/or the third party whose account is debited may obtain a hardcopy of the request against payment of the fee charged by us for Administrative Assistance. Details of our current fees and charges can be found in our "Clear and Simple: Business Fees and Charges Explained" brochure.

7. User Authorisations for Business eBanking

All Users performing transactions in Business eBanking on your behalf or a third party must be duly authorised to do so by you. This authorisation is created via the User Authorisation in Business eBanking.

If a third party has signed a mandate in favour of you, you may delegate this mandate to a user. This is

Registered branch in Ireland Company No. 905623 with office at: 3 Harbourmaster Place, IFSC, Dublin 1.
Registered office in Denmark: 2 - 12, Holmens Kanal, DK - 1092 Copenhagen K, Denmark

done via the User Authorisation in Business eBanking.

If a User needs to have cash access, e.g. to carry out transactions via the cashier's desk, you must sign an account mandate form (which you can obtain from us) authorising the User to do so.

7.1. Viewing documents

A User may view a number of documents in Business eBanking.

The rights and authorisations granted to the individual User determine which documents the User can view in Business eBanking.

A User will, for instance, be able to view his or her individual User Authorisation in Business eBanking.

7.2. Access to accounts

For each User, you must state which accounts the User may inquire about and/or make payments from. If you authorise a User to make payments from an account, the User is granted access to the transaction types determined by you.

For each account that the User is granted access to, the User's Authorisation must be stated. The following authorisations are available at account level:

Danske Bank A/S Irish branch trades as National Irish Bank and NIB. Danske Bank A/S is a plc registered in Copenhagen, CVR-no. 61126228, at the Danish DCCA.

- Separate authorisation
- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

The various authorisations granted by us are described in Clause 9 below.

Note that the authorisation granted at account level is reflected in all Business eBanking Agreements under which the account is registered.

7.3. Transaction types

For each User, you must state which transaction types the User is to have access to:

- Payments between accounts registered under the Agreement in the same country within the Danske Bank Group
- Payment requests via SWIFT MT101
- Payments into accounts not registered on Business eBanking within or outside the Danske Bank Group - including payment by drafts
- Cross-border payments to registered and unregistered accounts within or outside the Danske Bank Group.

Furthermore, you must state whether the User is to be authorised to create and approve, or only to

create, the payments selected. If the User is authorised to both create and approve payments, the relevant authorisations for each transaction type must also be stated. The following authorisations are available at transaction level:

- Separate authorisation
- Two persons jointly (A authorisation)

The various authorisations granted by us are described in Clause 9.

In general, the selected authorisation is used for all payments within each payment type. If you have selected a more restrictive authorisation at account level, this authorisation will apply for payments to unregistered accounts and cross-border payments. Note that if the User has not been granted any authorisation at account level, this is also regarded as a restriction.

7.4. Confidential payments

You must state whether the User is authorised to make confidential payments. Confidential payments include payments such as wages and salaries, which may only be viewed, created or approved by Users with these privileges.

Users are authorised to make confidential payments within the transaction types to which they have been granted access.

Note that no distinction is made between confidential and non-confidential payments in connection with account queries.

7.5. Changing Business eBanking User Authorisations

If you wish to extend or limit a User's access to Business eBanking, a new User Authorisation for Business eBanking must be signed, replacing the previous one.

If the change relates to the User's authorisations at account level, you and/or the relevant third party must also sign an account mandate.

Note that a User's authorisation in Business eBanking may be affected if you issue an account mandate form.

7.6. Revoking Business eBanking User Authorisations

User Authorisations for Business eBanking remain in force until revoked by you in writing - physically or using your Electronic Signature on Business eBanking where applicable.

When we have received notice of revocation, we will send written confirmation that the User number and Key(s) have been deleted in our systems.

If you terminate the Agreement, we will construe this as revocation of all User Authorisations granted under the Agreement.

If you and/or a third party have granted the User an account mandate, this mandate must be revoked separately. It is not sufficient for you merely to revoke the User Authorisation.

8. Other mandates in Business eBanking

8.1. Third-party mandates granted to you

If you wish to make transactions on third-party accounts with the Danske Bank Group, the third party must sign our third-party mandate form.

If account queries should be possible using SWIFT MT940 on third-party accounts outside the Danske Bank Group, an agreement stating that the Danske Bank Group may receive data about the third party's external account(s) shall first be submitted to us.

If you should make payments from the third party's accounts outside the Danske Bank Group using SWIFT MT101, an agreement stating that you may send payment instructions to the third party's bank(s) via the Danske Bank Group shall first be submitted to us.

The Bank registers the third-party accounts in Business eBanking via your Access Agreement.

8.2. Authorisation to buy/sell foreign exchange and securities

If a User should have access to information, be able to view trade positions and buy and sell foreign exchange spot and forward, the User must have access to one or more 'Markets Online' modules. Access to buy and sell foreign exchange spot and forward also requires that you grant the user currency trading and/or securities trading authorisations. These authorisations only authorise the User to perform transactions on your behalf via 'Markets Online'.

All transactions relating to the purchase and sale of foreign exchange spot and forward are subject to the provisions of the separate framework agreement on netting and final settlement of trades concluded between you and us.

The User Authorisation must state the accounts and custody accounts that the User is authorised to inquire about or trade in.

8.3. Trade Finance Authorisation in Business eBanking

If a User should be able to issue letters of credit, collect debt and/or issue guarantees, you must register the User for the 'Trade Finance' module and sign the 'Connection to/Modification of the Trade Finance Module' in the Access Agreement.

In this regard, you must state whether the User shall have access to:

- letters of credit (exports and/or imports)
- debt collection (exports and/or imports)
- guarantees.

Furthermore, you must state whether the User shall have access to

- create and inquire
- create and approve - two persons jointly (A authorisation)
- create and approve – separately (Separate authorisation)

9. Authorisation types

The Bank operates with the following authorisation types:

- Separate authorisation
- Two persons jointly (A authorisation)
- Two persons jointly (B authorisation)
- Two persons jointly (C authorisation)

These authorisations allow the Customer to specify which Users may, separately or jointly, approve a payment or request. The authorisations are described below.

9.1. Separate authorisation

When requests or payments are created or changed by a User with this authorisation, they are automatically deemed to have been approved by the User. Users with this authorisation can also approve requests or payments entered by Users with all other authorisation types.

9.2. Two persons jointly [A authorisation]

When requests or payments are created by a User with an A authorisation, they are automatically approved by this User (1st approval). Further approval (2nd approval) by a User with Separate, A, B or C authorisation is required.

Users with A authorisations rank equally, and the order of approval is therefore of no consequence.

9.3. Two persons jointly [B authorisation]

When requests or payments are created by a User with a B authorisation, they are automatically approved by this User (1st approval). Further approval (2nd approval) by a User with Separate, A or C authorisation is required. Two Users with B authorisations cannot jointly approve a payment.

9.4. Two persons jointly [C authorisation]

When requests or payments are created by a User with a C authorisation, they are

automatically approved by this User (1st approval).

Further approval (2nd approval) by a user with Separate, A or B authorisation is required. Two Users with C authorisations cannot jointly approve a payment.

10. Customer support

The Bank provides support and service to you. Support and service includes:

- user administration
- telephone support
- Internet-based support functions
- on-site support

User administration often includes establishment of Access Agreements for new clients and authorisations, adjustment of your and your Users' access to the various support and service features, deletion and blocking of Users, ordering of temporary PINs and registration of modifications to authorisations, etc.

On-site support may include installation of and training in our office-banking system, as well as related troubleshooting. Troubleshooting may result in adaptation and/or modification of the computer setup. Installation and troubleshooting take place in cooperation with your IT department and at your risk.

Telephone support may include training, user instruction, troubleshooting assistance and guidance in relation to modification. Telephone support in connection with installation, set-up, training and troubleshooting, etc. of Business eBanking is provided in cooperation with your IT department and at your risk.

Internet-based support may include training, User instruction, troubleshooting assistance and guidance in relation to modifications. Internet-based support is provided in cooperation with your IT department and at your risk.

Part 2 - Business eBanking - security system**11. Technical issues****11.1. Transmission and access**

In order to use Business eBanking, you must establish a data communication link with us. You must establish and bear the costs related to the link and must purchase, install, set up and maintain the required IT equipment.

Likewise, you must ensure the necessary adaptations to your IT equipment in order to use the link and ensure continuity of operations.

We may at any time and without notice modify our own equipment, basic software and related procedures in order to optimise operations and service levels. We will provide notification of any

modifications requiring adaptation of your equipment in order to retain the link and access by giving one month's written notice via Business eBanking or in such other manner as we shall determine.

11.2. Distribution, control and storage of software

We distribute the programs required to install Business eBanking. You must download the programs from the Internet.

If we send CO-ROMs, they are sealed, and you must check that the seal is unbroken. If it has been broken, the program may have been tampered with and should not be installed. You must contact us immediately for a new set.

When programs are downloaded from the Internet, you or a User must check that the program delivery has been electronically (digitally) signed by us.

If the programs have not been electronically signed by us, the reason may be that they have been tampered with or do not come from us. The signature can subsequently be verified by checking the properties of the downloaded program file(s). If the electronic signature is not from us, the downloaded program may not be installed.

11.3 Data security

e-Safekey and EDISec are the general security systems used in Business eBanking. Using both systems ensures that:

- data is kept confidential (encrypted) during transmission to us
- data is not modified during transmission to us
- the sender is always identified
- a Digital Signature is appended to all financially binding transactions.

A User's Digital Signature is created using a private Key stored in your IT environment. Access to the Key is protected by the User's Password.

We reserve the right to block the your or a User's access to Business eBanking for objectively justified reasons relating to the security of the Business eBanking service or if we register attempts at misuse. If access is blocked, the Customer will be notified immediately by telephone, in writing, by email, by fax or other such reasonable means we may choose and we will unblock access to Business eBanking if the reasons for blocking cease to exist.

If you wish to apply for unblocking of your access to Business eBanking please contact your branch or business centre.

You must implement effective security procedures to prevent unauthorised use of Business eBanking and unauthorised access to User Keys.

12. Acquiring a User ID and a Temporary PIN

When a User is to be created in Business eBanking, we give the User an individual User ID and a Temporary PIN to be used for registering the User in the e-Safekey security system.

The Temporary PIN is used for first-time identification when the User is registered in e-Safekey. The Temporary PIN is generated and printed automatically and no-one knows it. If the envelope containing the Temporary PIN has been opened or ripped, the User should contact us to order a new Temporary PIN.

If the User has not received the letter with the Temporary PIN within three Banking Days after ordering, the User should, for safety reasons, contact us to cancel it and order a new one.

When registering in the security system, the User must enter a Password and subsequently destroy the Temporary PIN.

12.1. Security registration and key generation

Security registration takes place before the User starts using Business eBanking. In this connection, a private Key is generated. The Key is

stored in your IT environment and is used for generating the User's Digital Signature.

Access to the key, and thus to generating Digital Signatures, is protected by the Password.

12.2. Password

When registering in the security system, the User must enter a Password. The Password protects the Key against unauthorised access, thereby ensuring that Digital Signatures can only be generated by the User himself or herself.

The User should select a Password that is as difficult as possible to guess – for example using upper- and lower-case letters, numbers and symbols.

The User must ensure that others do not know the Password and must store it in a suitable and safe manner, see Clause 12.5.

12.3. Changing the Password

You must prepare guidelines to ensure that the User regularly changes his or her Password. It is your responsibility to ensure that the guidelines are observed.

For further information, read the security recommendations under the 'Security' menu in Business eBanking on the Website and any other

guidelines provided or made available to you from time to time.

12.4. Deregistering Users/Keys

You must inform us if Users should be deleted. You are responsible for all transactions performed by a User until we are requested to delete or block the User.

12.5. Misuse or risk of misuse of Key

You or any User should immediately contact the Bank in order to invalidate the Keys if

- it is suspected that the Password or your and/or that User's Key has been misused
- others have had access to the Password or have gained possession of the personal Key file.

13. Ban on encryption

You should be aware that local, national legislation in the country where Business eBanking is used may include a general ban or limitations on encryption. Therefore, national legislation should always be checked.

Part 3 - Contractual aspects

14. For business purposes only

Business eBanking is to be used for business purposes only. The information made available to

Registered branch in Ireland Company No. 905623 with office at:
3 Harbourmaster Place, IFSC, Dublin 1.
Registered office in Denmark: 2-12, Holmens Kanal, DK-1092
Copenhagen K, Denmark

you, including price information, is solely for your own use. You may not pass on the information to others, except by written permission from us.

15. Changing Business eBanking

Business eBanking gives access to the services offered by us at any time.

We may at any time extend the scope of Business eBanking without notice, whereas one month's notice is required prior to any reduction in the scope and/or content. We shall provide written information of any changes via Business eBanking or otherwise.

16. Changes to service and support

We may change the scope and content of our service and support at any time by giving one month's written notice via Business eBanking or otherwise. The price list below shows the prices charged for the various services and support functions.

17. Responsibilities and liability

17.1. Your responsibilities

You use Business eBanking at your own responsibility and risk.

The risk borne by you includes, but is not limited to, the risk in relation to:

- sending information to us, as well as the risk that a transmission is destroyed, lost, damaged, delayed or affected by transmission errors or omissions, e.g. during intermediate handling or processing of data content
- information becoming accessible to third parties as a result of errors or unauthorised intrusion on the data transmission line
- misuse of Business eBanking.

You cannot hold us liable for any consequences thereof.

It is your responsibility to:

- check that the content of User Authorisations always matches the authorisations given to the User by you and any third party
- ensure that the content of the User Authorisation is in accordance with your wishes
- ensure that the content of the User Authorisation is in accordance with the User's wishes
- inform us as soon as possible if you find that the statement of any registered account includes any item authorised via Business eBanking which seems to be incorrect. On becoming aware of an unauthorised amount having been debited to such an account, you should telephone

your branch or business centre as soon as possible and, in any event, no later than thirteen months after the debit date in which case you will be able to obtain a refund from us, subject to all applicable laws and if a prompt investigation by us demonstrates that the transaction was, in fact, unauthorised. You should confirm such telephone call in writing to your branch or business centre within seven days.

Furthermore, it is your responsibility to ensure that users are aware of the Special Terms and Conditions for our Business eBanking Service and the Special Terms and Conditions for Electronic Signature, and that all Users observe them, and that they comply with the on-screen Help requirements.

You are responsible for:

- all operations and transactions made using your own Key or that of a registered User
- ensuring that Users keep their Passwords secure so that no third party becomes aware of them
- ensuring data security in connection with storage of Users' Keys in your IT environment to prevent unauthorised access to the Keys

- any incorrect use or misuse of Business eBanking by registered Users.

In the event that any Password or Electronic Signature or Key relating to your access to our Business eBanking Service has been misappropriated or used in an unauthorised manner, you must notify us by telephoning your branch or business centre. You should confirm your notice by writing within seven days to your branch or business centre.

Subject to any applicable laws, you cannot make any claims on us in respect of errors and omissions resulting from you circumstances, including non-observance of your safety and control procedures.

17.2. Our responsibilities

We will be liable for damages if, through errors or neglect, we are late in performing our obligations under the Agreement or perform our obligations inadequately.

However, we are not liable for errors and omissions resulting from:

- errors and omissions in third-party software which is part of the Business eBanking security system
- a User's disclosure of the Temporary PIN and/or the Password

- modifications to the security system (not performed by us)
- the security system's integration with other systems or software not supplied by us.

In areas that are subject to stricter liability, we will not be liable for losses resulting from:

- IT system failure/downtime or corruption of data in these systems as a result of the events listed below, irrespective of whether we operate the systems itself or has outsourced operations
- telecommunication or power failures at our offices, statutory intervention or administrative acts, natural disasters, wars, rebellions, civil unrest, acts of sabotage, terrorism or vandalism (including computer viruses and hacking)
- strikes, lockouts, boycotts or blockades, irrespective of whether the conflict is targeted at or initiated by us or our organisation and irrespective of the cause of the conflict. This also applies if the conflict affects only parts of our organisation
- any other circumstances beyond our control.

Our exemption from liability does not apply if:

- we should have predicted the circumstances resulting in the loss at the

time when the Agreement was concluded, or should have prevented or overcome the cause of the loss

- legislation under any circumstances renders us liable for the cause of the loss.

In accordance with general liability provisions in force we are liable for direct losses attributable to errors made by us. Apart from that, our liability is limited to remedying the deficiencies. No further claims can be made against us, including for indirect or consequential damage.

18. Other terms and conditions

18.1. Structure of the Business eBanking agreement

An agreement in relation to Business eBanking (an "Agreement") is comprised of the following:

- the Access Agreement
- all User Authorisation(s)
- all Module Descriptions
- the Special Terms and Conditions for our eBanking Services, these Special Terms and Conditions and the Special Terms and Conditions for Electronic Signature, to each of which our General Terms and Conditions for Business also apply
- our "Clear and Simple: Business Fees and Charges Explained" brochure.

- The "Getting Started" user guide on the Business eBanking website and onscreen Help, as well as other sets of rules applying at any time, as stated in the individual module agreements or the Access Agreement.

By signing the Access Agreement for Business eBanking you also acknowledge having read and accepted all parts of the Agreement.

18.2 Prices

We may at any time change our prices by giving one month's written notice via Business eBanking or otherwise. We will debit various fees and charges from the account(s) specified as fee account(s). Details of our current fees and charges can be found in our "Clear and Simple: Business Fees and Charges Explained" brochure.

18.3. Assignment, transfer and third parties

Your Agreement has been concluded by us on behalf of the Danske Bank Group. This means that any member of the Danske Bank Group is entitled to fulfil and enforce your Agreement. It also means that we may transfer our rights and obligations thereunder to another member of the Danske Bank Group at any time.

We are entitled to transfer the performance under your Agreement to subcontractors. Such

transfer shall not affect our responsibilities under your Agreement .

19. Termination and breach

You may terminate the Access Agreement without notice - provided that you do so in writing. Requests and agreements made before the time of termination will be carried out. Paid subscription fees will not be refunded. We may terminate the Access Agreement in writing by giving one month's notice.

We may, however, terminate the Access Agreement without notice if you are in breach of any part of your Agreement . You are in breach if you, for example, omit to pay as agreed in the Access Agreement, suspend your payments, are subject to bankruptcy proceedings or other insolvent administration of your estate, negotiates for a composition or are subject to an execution or attachment order.

20. Governing law

This Agreement is governed by Irish law and subject to the jurisdiction of the courts of Ireland.

If you are registered for a module that is solely intended to be used abroad, you accept – to the same extent as us – that you are subject to the legal rules and usage applying in the country where you operate.

Danske Bank A/S (trading as National Irish Bank) is authorised by The Danish FSA in Denmark. Details of all Danske Bank A/S directors can be viewed at its registered offices.

21. Definitions

Defined terms used in these Special Terms and Conditions shall have the meanings given to them in the General Terms and Conditions for Business, unless otherwise defined herein.

Access Agreement: Agreement between you and us concerning the use of Business eBanking.

Agreement: Has the meaning given to it in Clause 18.1.

Authorisation/mandate: Any User Authorisation for Business eBanking, account mandate, Business eBanking account mandate or one of our other mandate forms for Business eBanking.

Authorisation/mandate holder: One or more registered mandates or authorisations and/or physical persons who have been granted authorisations/mandates.

Business eBanking: Collective term used about our business systems, comprising:

(i) **Business PC:** a PC-based payment and information system; and

(ii) **Business eBanking:** an Internet based payment and information system.

Confidential payments: Confidential payments are payments (such as wages and salaries) that may only be seen or processed by users with special

privileges. Payments classified as confidential can only be processed by users with these privileges.

Cross-border payment: A payment is a cross-border payment if it crosses a national border - even if it involves only one transaction currency, e.g. the euro. This applies to Payments between Registered Accounts as well as payments to unregistered accounts. In the countries where the Danske Bank Group is represented, payments between accounts in the same country are not cross-border payments.

Payments managed via SWIFT are not included in this category either.

Customer support: Function at our offices offering technical support or support for Business eBanking users by telephone.

Data delivery: Transfer of data between you and us. For example, a data delivery may contain payment instructions.

Digital signature: An electronic signature appended to binding transactions via Business eBanking, e.g. payments, and used when linking to us.

EDISec: Security system used for other links than the programs mentioned.

Electronic Signature: Has the meaning given to that term in the Special Terms and Conditions for Electronic Signature.

e-Safekey: Security system for the programs mentioned.

Registered branch in Ireland Company No. 905623 with office at: 3 Harbourmaster Place, IFSC, Dublin 1.
Registered office in Denmark: 2 - 12, Holmens Kanal, DK - 1092 Copenhagen K, Denmark

Danske Bank A/S Irish branch trades as National Irish Bank and NIB. Danske Bank A/S is a plc registered in Copenhagen, CVR-no. 61126228, at the Danish DCCA.

Instruction: Electronic, written or oral request to us to carry out changes, transactions, etc.

Keys: Each User generates two keys (a set of keys) - a private key used to generate digital signatures and a public key used to verify the digital signature. Each User has his or her own private key in order to create unique, personal digital signatures. Access to use the keys is protected by the user's password. The keys are stored in a key file or key database on your IT system.

Module Description: Bulleted description of the functionality of the individual modules registered under the Agreement.

On-site support: Training, technical assistance or other assistance provided by us at your premises.

Password: A code to protect a User's private key that is used to create digital (electronic) signatures. The password has between eight and sixteen characters and should include upper- and lower-case letters, as well as numbers and symbols.

Payments between Registered Accounts: Payments between your own Registered Accounts on Business eBanking in the same country within the Danske Bank Group.

Registered Accounts: any account registered in Business eBanking in accordance with the Agreement.

Security/registration: The registration process that a User must go through before using Business eBanking for the first time.

SWIFT MT101 means request for a payment transfer sent via the SWIFT network.

SWIFT MT940 means electronic account statement received via the SWIFT network.

Temporary PIN: A code issued and sent by the Bank to a customer's User(s). The code consists of four or eight characters and is used by your User(s) to register in the Business eBanking/Business PC security system.

Transactions: Payments, payment requests and queries in Business eBanking.

User: A user is a person (for example an employee) who has been authorised by you to act on your behalf via Business eBanking. If your and our IT systems are directly integrated, a user may also be a computer or system located within your organisation.

User Authorisation: Your authorisation of a User, specifying the services, accounts, authorisations and privileges to which the individual User has access.

User ID: A six-digit number assigned to the individual Business eBanking User. The User ID is stated in the User Authorisation.