

MultiCash[®] 3.23

Users Quick Reference

September 2012

Omikron Systemhaus GmbH & Co. KG
Von-Hünefeld-Str. 55
D-50829 Cologne (Germany)

Tel.: +49 (0)221 -59 56 99 -0
Fax: +49 (0)221 -59 56 99 -7

info@omikron.de
www.omikron.de

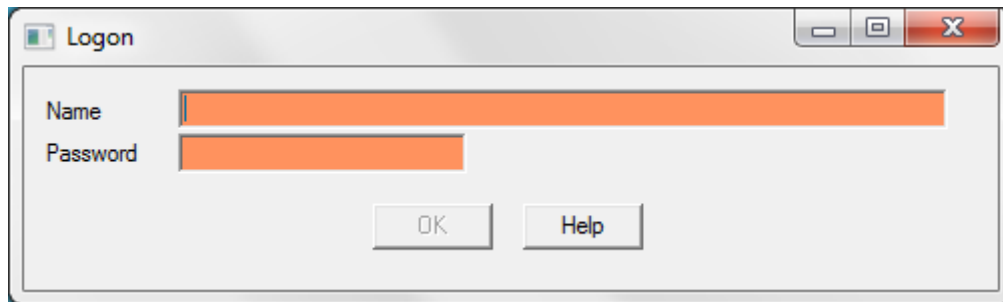
Table of Contents:

1	STARTING UP - WORKING WITH THE WIZARD FOR NEW USERS.....	3
2	HOW TO COLLECT ACCOUNT INFORMATION?	17
2.1	Define single collection order in File Manager.....	17
2.2	Define Autodial function.....	23
3	HOW TO EDIT AND SEND A PAYMENT?	27

1 Starting up - Working with the wizard for new users

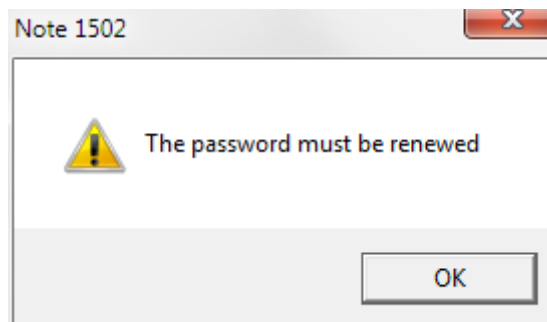
If you wish to logon to the program for the first time with your newly set up user name, you have to start this first using the respective entry in the start menu or via shortcut icon on the desktop.

Next you enter the user name and password issued by your system administrator. Please make sure to use small or capital letters (see Core module Chapter 4.4: *User Validation*).

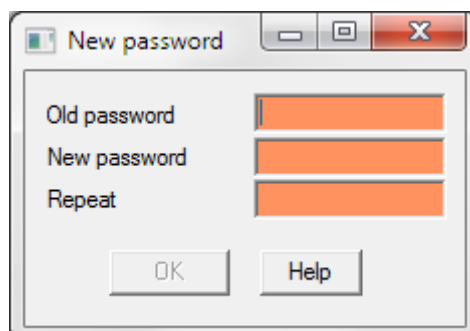


Confirm your entries by pressing [**OK**].

After having finished the First Logon Wizard (see next page), you are prompted to change your initial password.

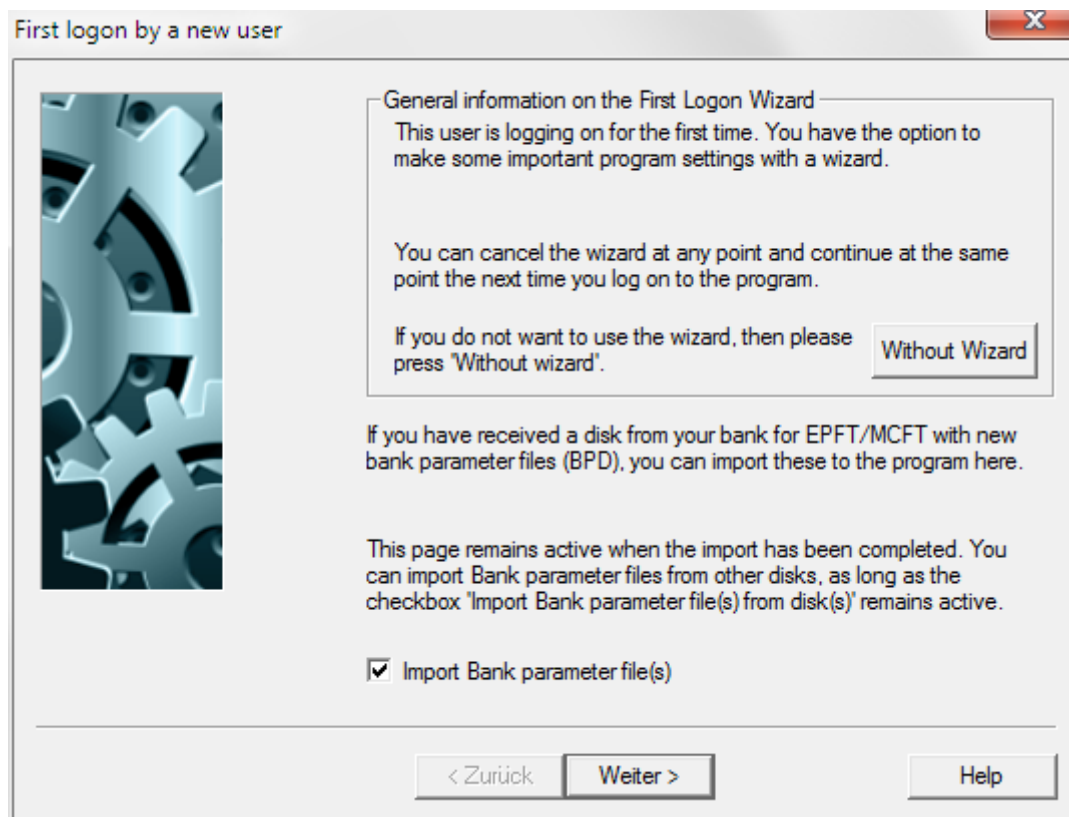


For this, enter the given (= old) password in the following dialog. Then you move to the next field using the TAB-key and enter your own (=new) password.



Since password entry is concealed, i.e. each key stroke is represented by an * (asterisk) on the screen, you are prompted to repeat the new password entry to ensure that it has been entered properly. Subsequently, confirm with <Return> or by clicking on [**OK**] (see Chapter 5.2 of Core module: *Assign new password*).

After the logon the **First Logon Wizard** will start. This wizard will assist you in making the necessary program settings (Comms. access, set up Electronic Signature etc.). You can close the wizard at any time using the close button and return to the same point, the next time that you start the program. If you do not wish the assistance of the wizard, please click on [**Without Wizard**].



If you accept the assistance of the wizard, it will guide you through the steps necessary at the **logon of a new user**:

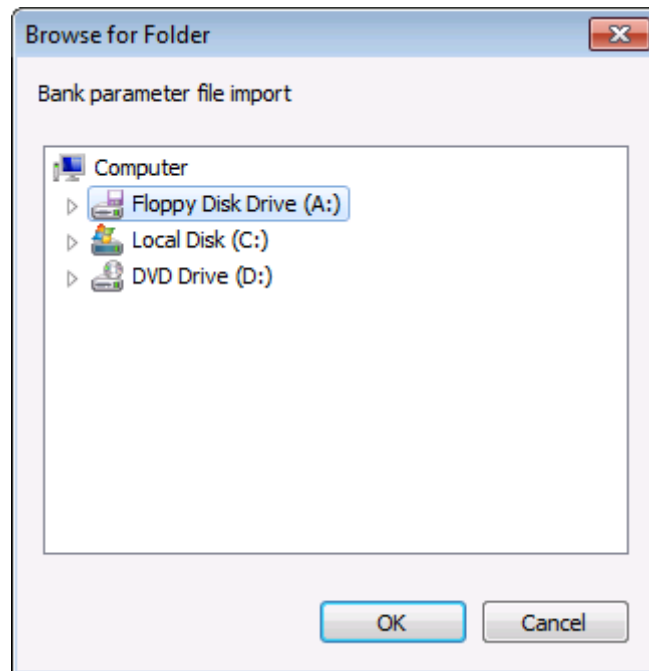
1 Import bank parameter file(s) (only with EPFT/MCFT)

In the case of a bank access via **EBICS** procedure you have to deactivate the "**Import bank parameter file(s)**" check box, in order to continue directly with step 2 using [**Next >**]. With EBICS no bank parameter file is imported, but an appropriate bank parameter file need to be set up before by the system administrator or by yourself according to bank information (see Comms. Chapter 3.5: *EBICS*)

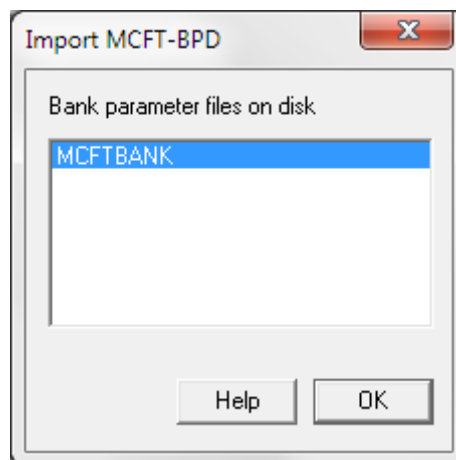
If you received bank parameter files from your bank with bank parameter files (for the EPFT or **MCFT** procedure) for the new user, you can import these at this point. This page remains active as long as the "**Import bank parameter file(s)**" check box is ticked.

If you want to import a bank parameter file, click on the [**Next >**] button.

Insert a data medium with the bank parameter file(s) or select an appropriate directory, where the bank parameter file(s) can be found.



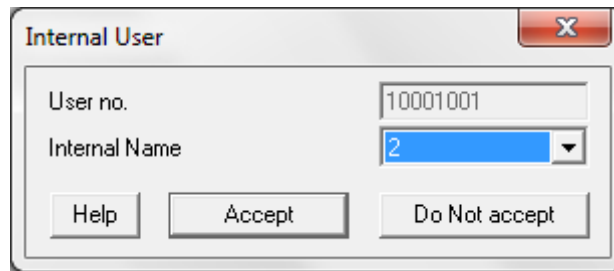
After confirming with [**OK**], a selection list of all bank parameter files on the medium or in the chosen directory is shown.



Select the required file(s) by mouse click and confirm with [**OK**].

If you are **importing an EPFT BPD**, the process is now complete (for further details, please see Comms. Chapter 3.1: *Create BPD*).

If you are **importing a MCFT BPD**, the user number ("external name") is now allocated to your internal user name. Confirm this by pressing the [**Accept**] button.

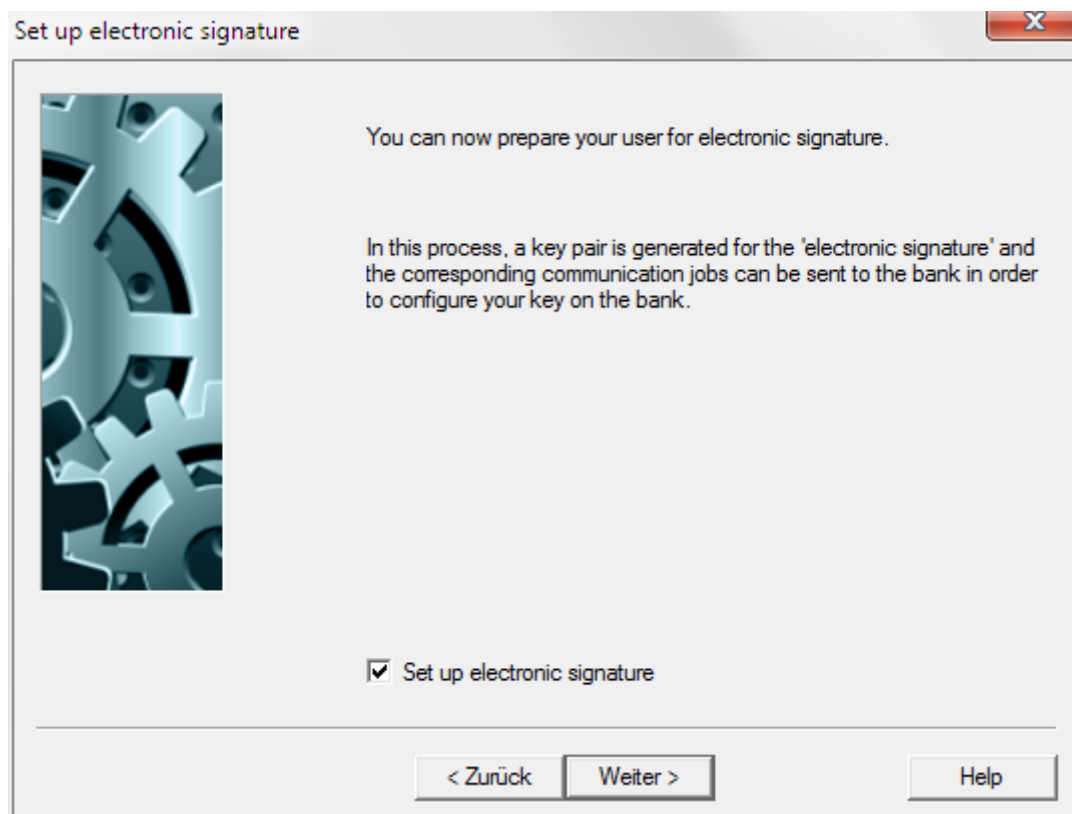
A dialog box titled "Internal User" with a close button (X) in the top right corner. It contains two input fields: "User no." with the value "10001001" and "Internal Name" with a dropdown menu showing "2". Below the fields are three buttons: "Help", "Accept", and "Do Not accept".

If there are other users available in the system, this process will be repeated until all users from the selection list have been allocated to internal user names. If there is a user that you do not wish to import, press the button [**Do Not accept**] (for further details see Comms. Chapter 3.2.1: *Import MCFT bank parameter file*).

If you do not wish to import any more bank parameter file(s), deactivate the check box "**Import bank parameter file(s)**" and click on [**Next >**].

2 Setting up the Electronic Signature

At this point, you can prepare the Electronic Signature (ES). In the process, a key-pair will be generated and the appropriate message will be sent to the bank to set up your key at the bank. To set up the Electronic Signature, keep the checked box "**Set up Electronic Signature**" activated and click on [**Next >**] then.

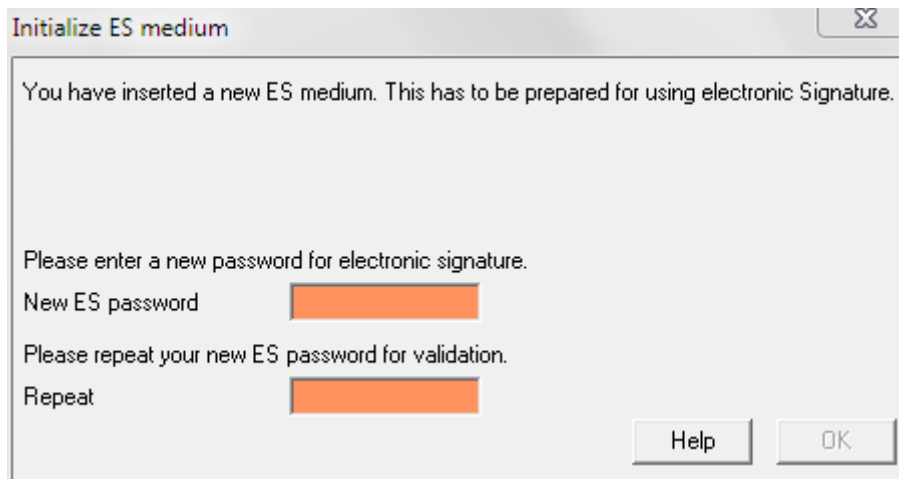
A dialog box titled "Set up electronic signature" with a close button (X) in the top right corner. On the left is a vertical image of interlocking gears. The main text area contains the following text: "You can now prepare your user for electronic signature." followed by "In this process, a key pair is generated for the 'electronic signature' and the corresponding communication jobs can be sent to the bank in order to configure your key on the bank." Below this text is a checked checkbox labeled "Set up electronic signature". At the bottom are three buttons: "< Zurück", "Weiter >", and "Help".

Initialize ES medium

In the first step you are prompted to insert the selected ES medium (e.g. a diskette, an USB stick). Confirm the appropriate message box with [**OK**] after insert.

If the ES medium is new (i.e. empty), the assignment of an **ES password** (ES PIN) for the access to the ES medium follows.

Entry of the characters is concealed, i.e. each character you enter is represented by an * (asterisk). You must then **repeat** the entry of the new ES password for your own protection.



The dialog box is titled "Initialize ES medium" and contains the following text and controls:

- Text: "You have inserted a new ES medium. This has to be prepared for using electronic Signature."
- Text: "Please enter a new password for electronic signature."
- Text: "New ES password" followed by a text input field.
- Text: "Please repeat your new ES password for validation."
- Text: "Repeat" followed by a text input field.
- Buttons: "Help" and "OK" at the bottom right.

Generate Key Pair

The field "**Generate new Key Pair**" is already marked in the next dialog. You have to enter a character string of your choice consisting of exactly **32 characters**. The character string is a random combination of 32 letters, numbers and special characters. Entry of the characters is concealed, i.e. each character you enter is represented by an * (asterisk). This random character string forms the basis for generating the keypair.

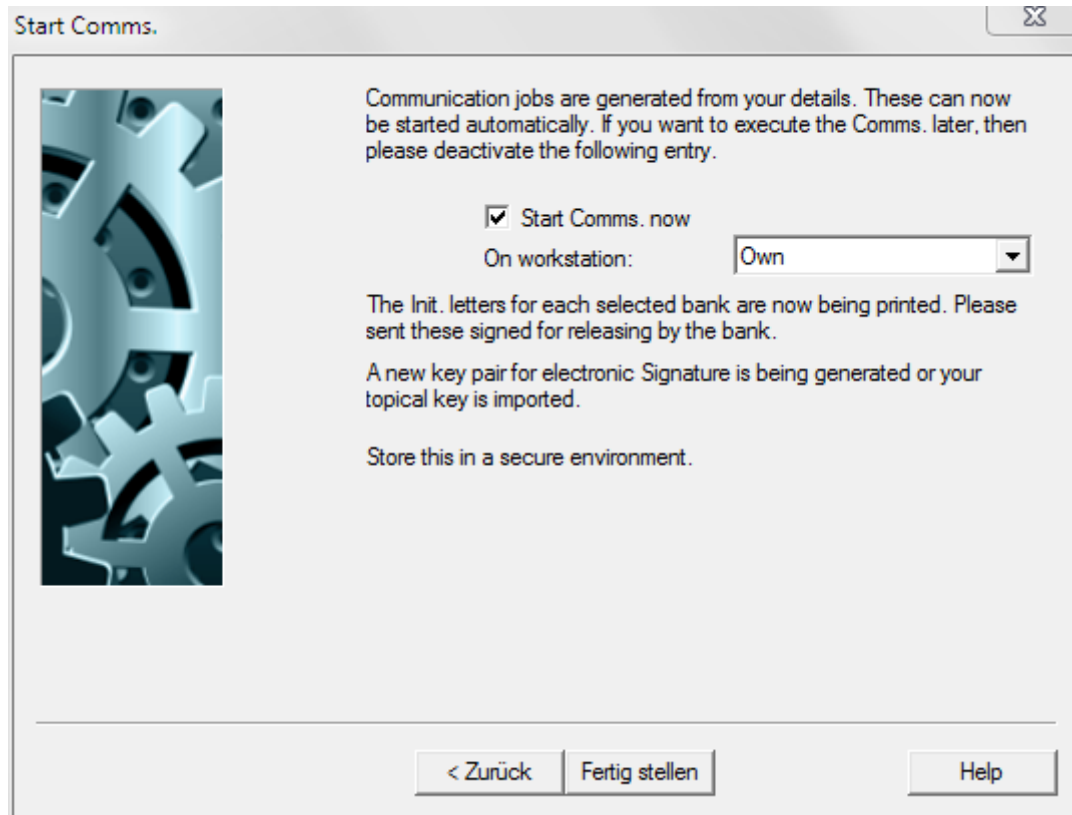
Confirm your entry by clicking on [**Next**] after the input of the 32 characters (just fill it up to the end).



The dialog box is titled "Generate key pair" and contains the following text and controls:

- Image: A graphic of interlocking gears on the left side.
- Text: "Do you wish to generate a new key pair for electronic signature, send the existing key pair to the bank(s) or import key pair from existing medium into your system ?"
- Text: "Generate new key pair" with a checked checkbox.
- Text: "To generate the key pair, please enter exactly 32 arbitrary characters ! These characters should be chosen as randomly as possibly."
- Text input field: A long text input field for entering the 32-character string.
- Buttons: "< Zurück", "Weiter >", and "Help" at the bottom.

Next a new key pair is generated, which is stored on the ES medium. For starting the key generation click on [**Finish**].



You can also import keys already existing on an ES medium into the system.
Further details can be found in Chapter 6.1 on Communication: *Generate / Send ES key pair*.

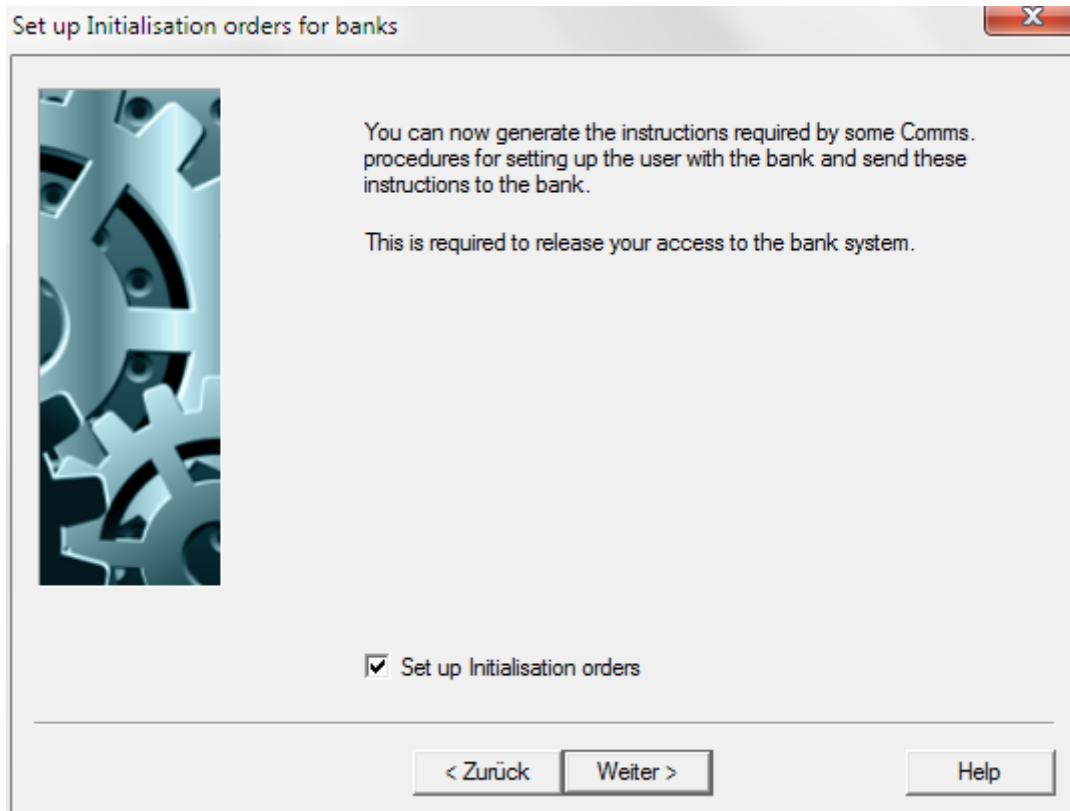


Please note:

Always keep the ES medium in a **secure place**.

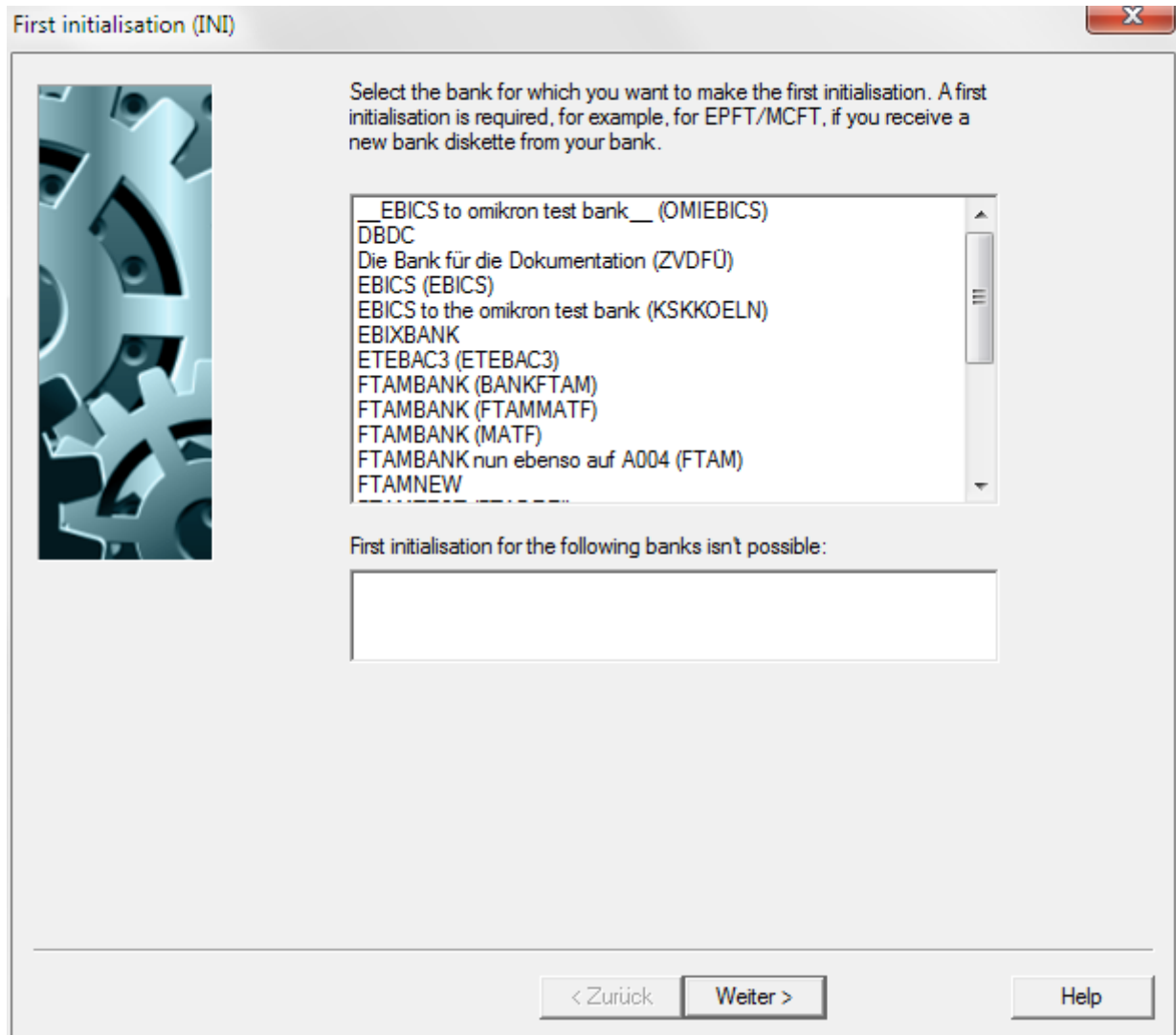
3 Setting up initialization requests for banks

To have the bank enable your access to their system, you can generate and directly send the necessary initialization request at this point. To set up the initialization request, let the "**Set up initialization orders**" box checked and click on [**Next >**] then.



Select the bank(s)

Click to select the bank(s) from the list for which first initialization is to be carried out. A first initialization is necessary, for example, for EPFT/MCFT when you have received a new bank diskette from your bank. Then press the [**Next >**] button.



Enter current and new password (not with EBICS)

Three mandatory boxes now appear below the selected bank(s). Enter your current Comms. password in the "**Current password**" box. This is needed by the bank to verify the first initialization. Use the current password contained in the PIN letter should you have received such a letter from your bank. Should you not have received such a letter, initial password is usually "start". Use the TAB key to jump to the next box and then enter the new password under "**New password**". This will be used for future communication sessions after it has been successfully sent to the bank.

Because password definition is concealed, i.e. when you press a key you only see an * (asterisk) on the screen, you must **repeat** the new password in the appropriate field for your own protection.

**Please note:**

In contrast to normal practice, entries are **not** converted into capitals when you enter the password. A differentiation is thus made between upper case and lower case entries. Please remember this when entering and then using the password.

Close password definition by clicking on the [**Next >**] button.

Enter previous and new password

Bank(s) Omikron Test INTERN

Previous password

Please enter your actual password.

If this is the first time you wish to initialize and you have received a PIN letter from your bank, you will find the first password in this letter, otherwise the password is 'start'.

Password

New password

Please enter the new Comms. password of your choice. Once successfully sent to the bank, this password will be needed for all future communication.

New password

Please confirm by repeating the password in the field provided.

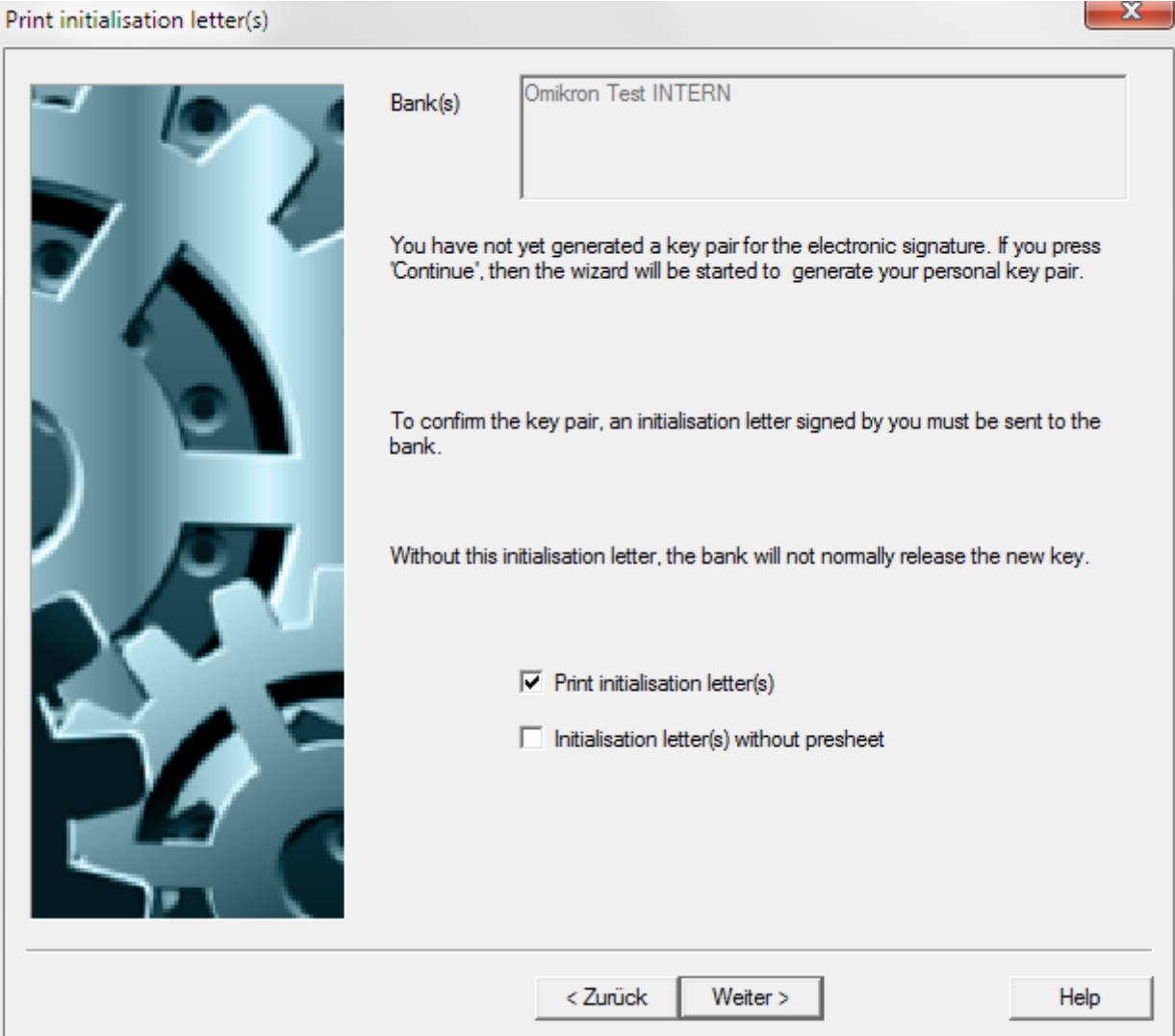
Please repeat

< Zurück Weiter > Help

Print initialization letter(s)

You will have to send a signed initialization letter to your bank (or several banks) to confirm the new keypair. Access will normally not be released by the bank until such time as the initialization letter has been received. If you would like the initialization letters to be printed, leave the default box "**Print initialisation letter(s)**" checked.

Together with the INI letters a cover letter is generated for each bank automatically. Address data is taken from the entries on the *Banks property page* (see Chapter 7.1.1 of Core module) and on the *Contacts property page* (see Chapter 5.4.4 of Core module).



If the cover sheet should not be printed each time for the same bank at the first initialization of several users, you can suppress the generation by ticking the "**Initialization letter(s) without presheet**" check box additionally.

Then click on the [**Next >**] button.

Further details can be found in Chapter 4.2 on Communication: *First initialization of bank access (Sessiontyp INI)*.

With the EBICS procedure further special steps follow:

4 Generate EBICS authentication keys (only with EBICS, if the wizard is executed the first time)

If you execute the wizard for the first time, a user-related authentication key is generated for you **one-time**. This key is required only for the EBICS communication.

Please enter in the field "**Comms. password**" your currently valid Comms. password also as new password for the authentication key. Since the password entry is made concealed, i. e. each keystroke is displayed by an * (asterisk), you must **please repeat** the password entry for security in the field planned for this.

To generate the key pair, please enter exactly **32 random characters**. This character string is an arbitrary combination of characters, numbers and special characters. The entry is made concealed, i.e. each entered character is displayed by an * (asterisk).

Generate EBICS authentication keys

Bank(s) EBIXBANK

Do you want to generate a new EBICS authentication key or send the existing key pair to the bank(s) ?

☒ Generate new authentication key

Now, new keys are generated. Please allocate a new password for the access to these keys. It is later used as 'Comms. password'.

Comms. password

Please repeat

To generate the key pair, please enter exactly 32 arbitrary characters ! These characters should be chosen as randomly as possibly.

☒ Also collect current bank key (HPB)

< Zurück Weiter > Help

Press finally the [**Next >**] button.

5 Enter the hash values of the bank keys (only with EBICS)

To ensure that you actually communicate with the correct partner -i.e. your bank-, the validity of the bank keys which are collected at the end of this wizard should be verified. This is made automatically after the retrieval of the keys.

Please enter for this the hash values of the bank keys in the planned fields (**Authentication hash of the bank (X0??)** / **Encryption hash of the bank (E0??)**). These hash values are notified to you by the bank or you can view the hash values on the Internet page of the bank.

You need not to enter all values. Normally a few digits are sufficient for the authentication. All values entered by you are reconciled with the transmitted values.

The values in the respectively first field are mandatory if they deviate from "00".

Enter hash values of bank keys

Bank(s)

To ensure that you actually communicate with the right Partner -i. e. your bank -, the validity of the bank keys should be verified.
This is made automatically after calling the keys, if you enter some values below.

For this, please enter here the hash values of the bank keys. These hash values are notified to you by your bank or you can view the hash values on the Internet site of the bank.

You need not to enter all values. Normally, a few digits are sufficient for the authentication, all digits entered by you are reconciled with the transmitted values.

If you do not enter values, bank access will be activated automatically without any verification.

Bank:

Authentication hash of the bank (X0??)

Digits 1-8:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 9-16:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 17-24:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 25-32:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Encryption hash of the bank (E0??)

Digits 1-8:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 9-16:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 17-24:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Digits 25-32:	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

< Zurück Weiter > Help

You can check the status of the bank keys in menu item -Communication- / -Bank parameter files- in the bank parameter file and repeat the verification later by entering and saving the hash values using the [**Hash values of bank**] button (see Chapter 3.5: *EBICS*).

Press then the [**Next >**] button.

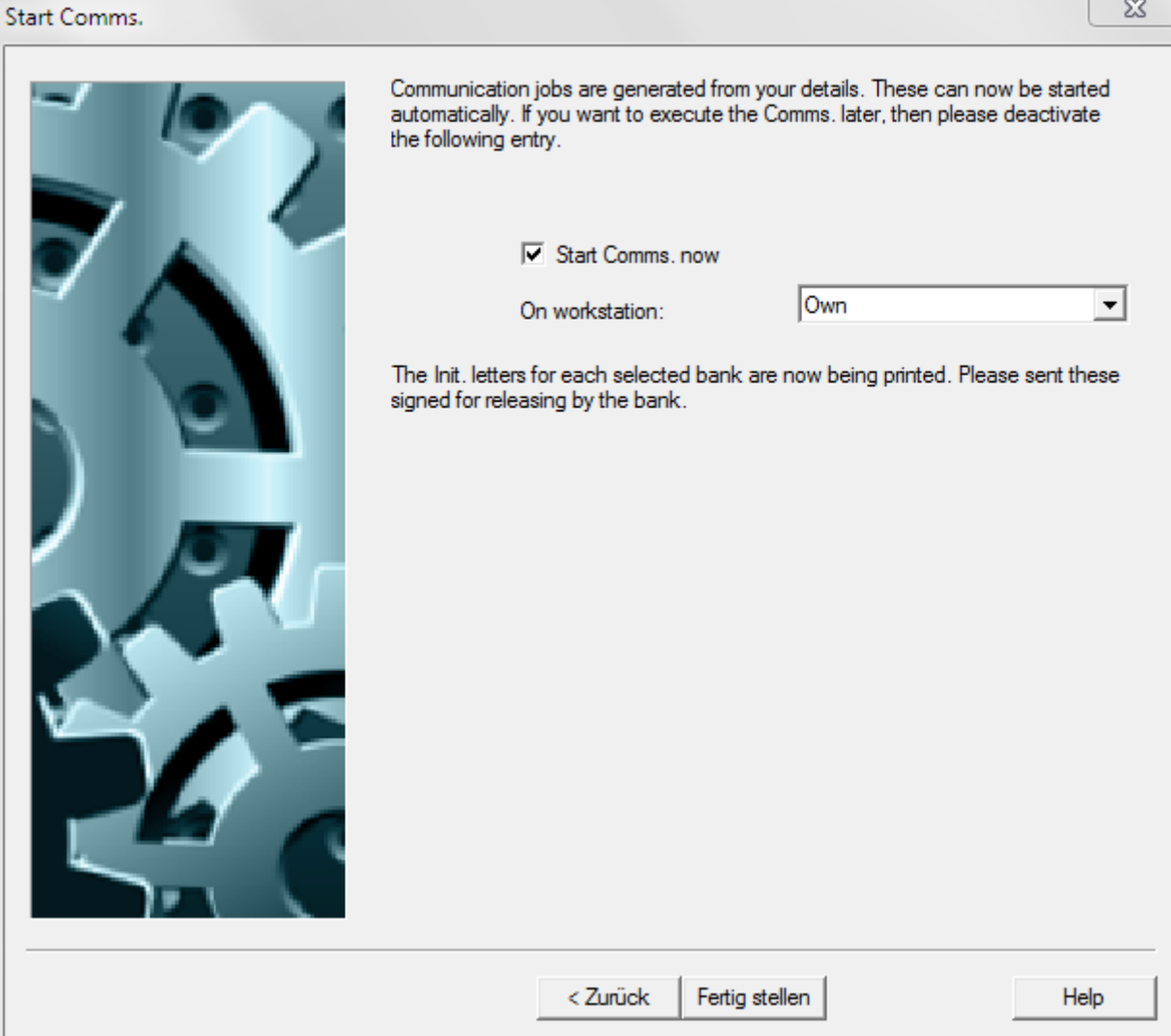
6 Start communication

A Comms. session file is generated from your entries (MCFT: INI / EBICS several: INI, HIA and HPB). Comms. can be started automatically during this last step if you confirm the **"Start Comms Now"** default entry using the [**Finish**] button.

If you do not wish to start the Comms. immediately, you have to deactivate the entry.

A message is shown then, under which ID group you can find the Comms. batch in the File Manager for further processing. Confirm this message with [**OK**].

If working in a network, you can select a computer which may have been specially designated for Communication sessions by selecting the list box **"On workstation:"** and start communication there.



With "Start Comms. now" the Comms. batches are executed immediately. After successful transmission, close the appearing message box with [**OK**].

With EBICS the bank keys can only be received if you were released on bank side. Therefore the HPB request is entered by the wizard with the status "Pending Comms." in the file manager, so that it can simply be executed there, after you were released by the bank. Confirm the appropriate message with [**OK**].

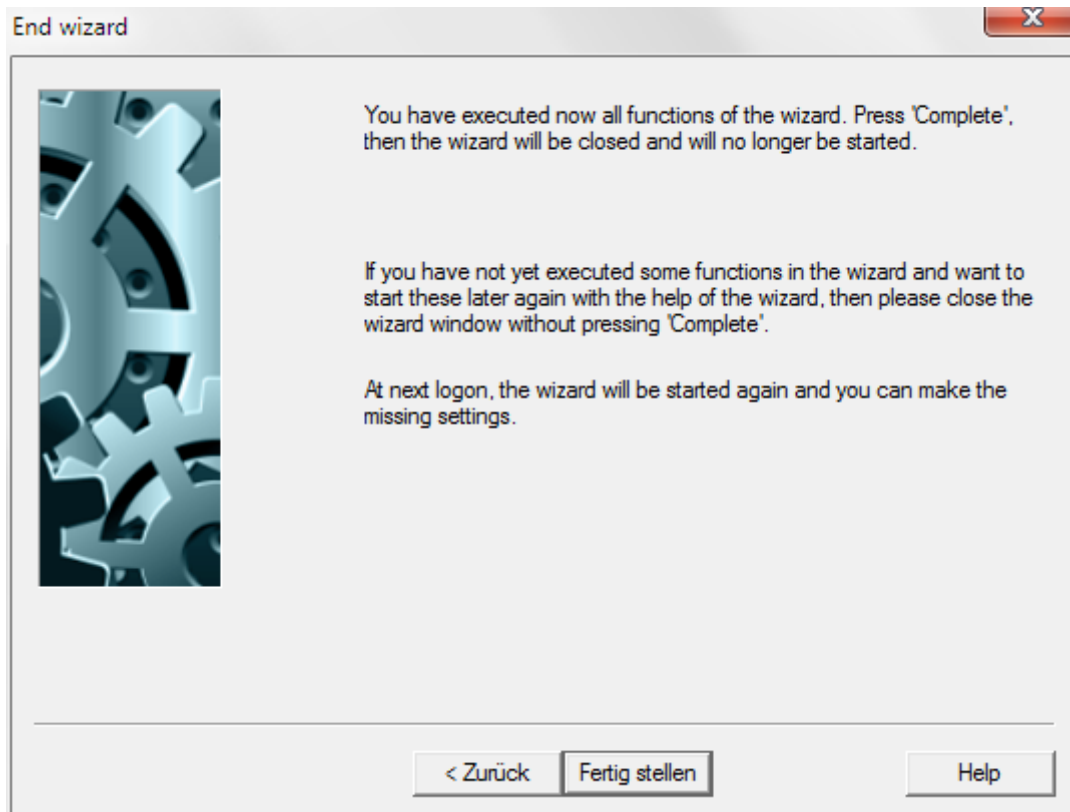
In the lower part of the Comms. dialog box information on the status of processing is displayed.

Complete the first initialization by finally clicking the [**Finish**] button.

The printed initialization letter(s) have to be signed and sent to the bank for the release.

7 Complete the wizard

All of the wizard's steps were completed. When you click on [**Finish**], the wizard will be closed and will not be started again.



If there are still some functions that you have not configured using the wizard and you wish to have the assistance of the wizard to complete these later, please close this window via close button and **without** clicking on [**Finish**]. In this case, the wizard will be started again the next time you start the program and you can configure the sections that have not yet been completed.

By clicking on [**< Back**], you can step back through the individual steps to make any changes that are needed.



Please note for EBICS:

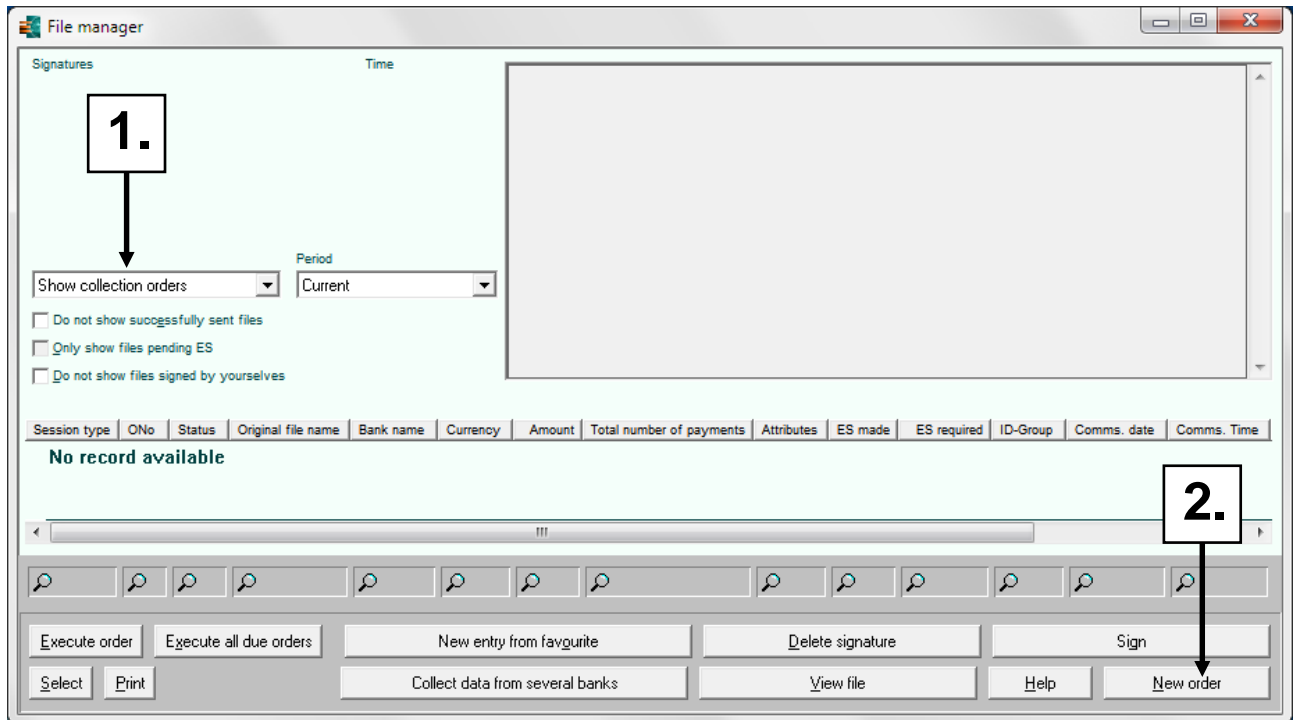
After release by your bank you still have to execute the HPB request in the file manager.

If you want to add another bank later, or add an FTAM-Bank, please refer to the **-Communication-** menu, where you will find the options **-Bank Parameter Files-** (with the button [**New BPD**]) and **-First Initialization-**. Wizards will walk you through these functions as well.

2 How to collect account information?

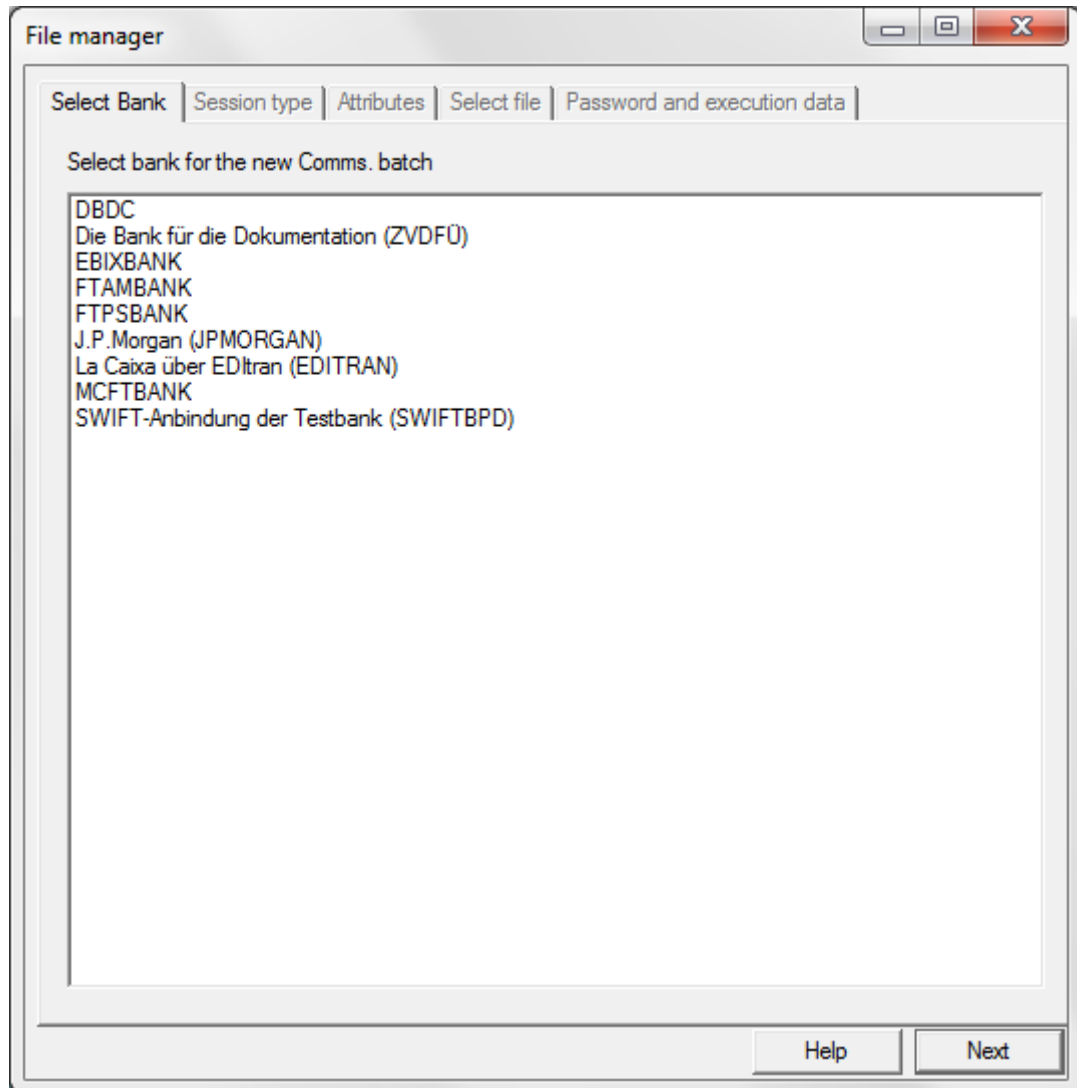
2.1 Define single collection order in File Manager

- 1 **Open File Manager via -Communication- / -File Manager-**
Choose the -Show collection orders- option from the pull-down menu (1.). Then click on the [**New order**] button (2.).



2 Select bank

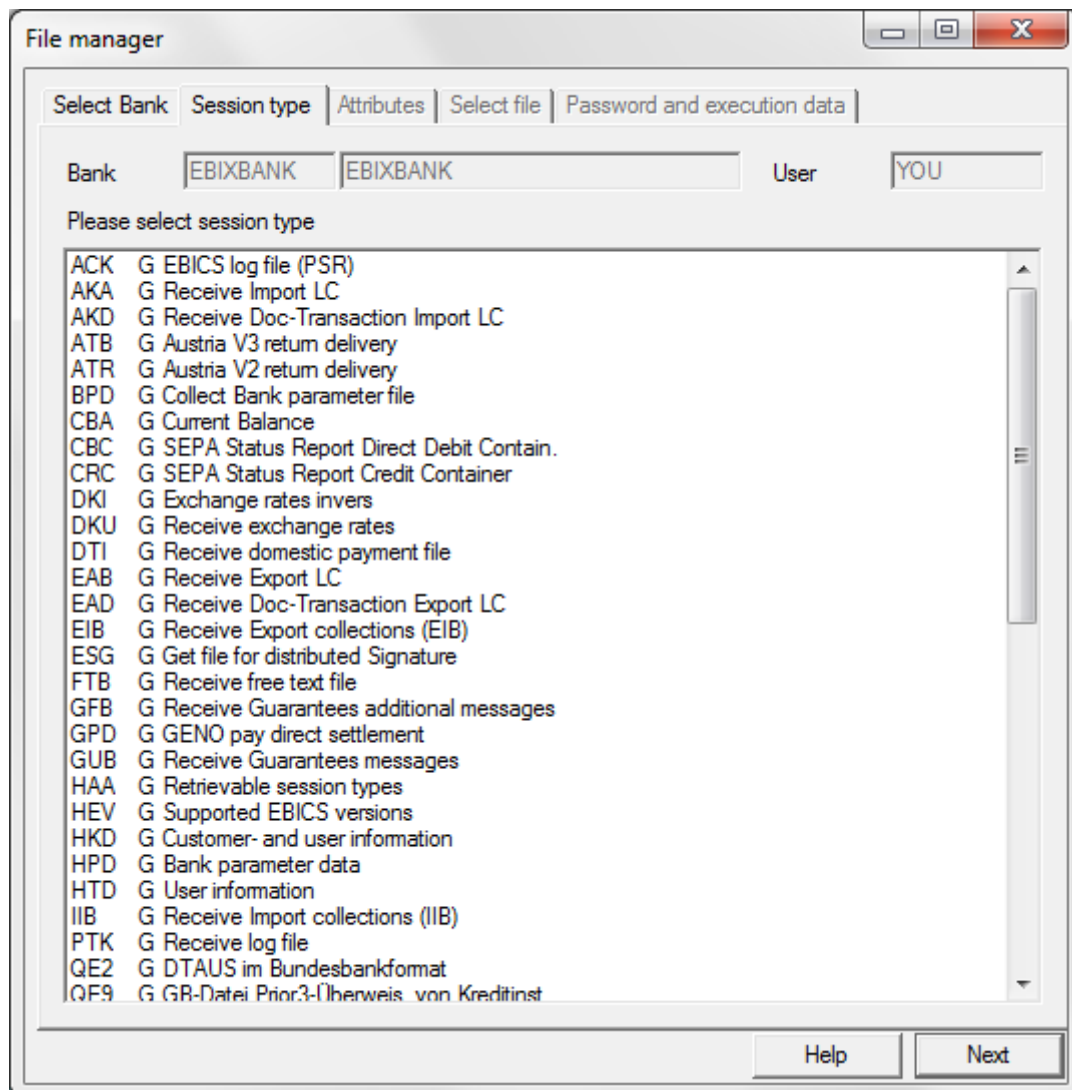
Now you have to specify the bank, which should be addressed by the order to be created.



Choose the desired bank by double-clicking on the respective entry. Immediately the program switches to the next property page.

3 Choose session type

The STA (Swift daily statement) session type is used for the collection of account information. Select the session type by double-clicking on it.



The program switches after the "Attributes" property page (not with MCFT), where you have to enter nothing (just to click on **Next**), to the last property page.

4 Enter Comms. password

As final step enter your Comms. password (1.) (if not saved in the BPD) and complete the order creation with **[Save]** (2.).

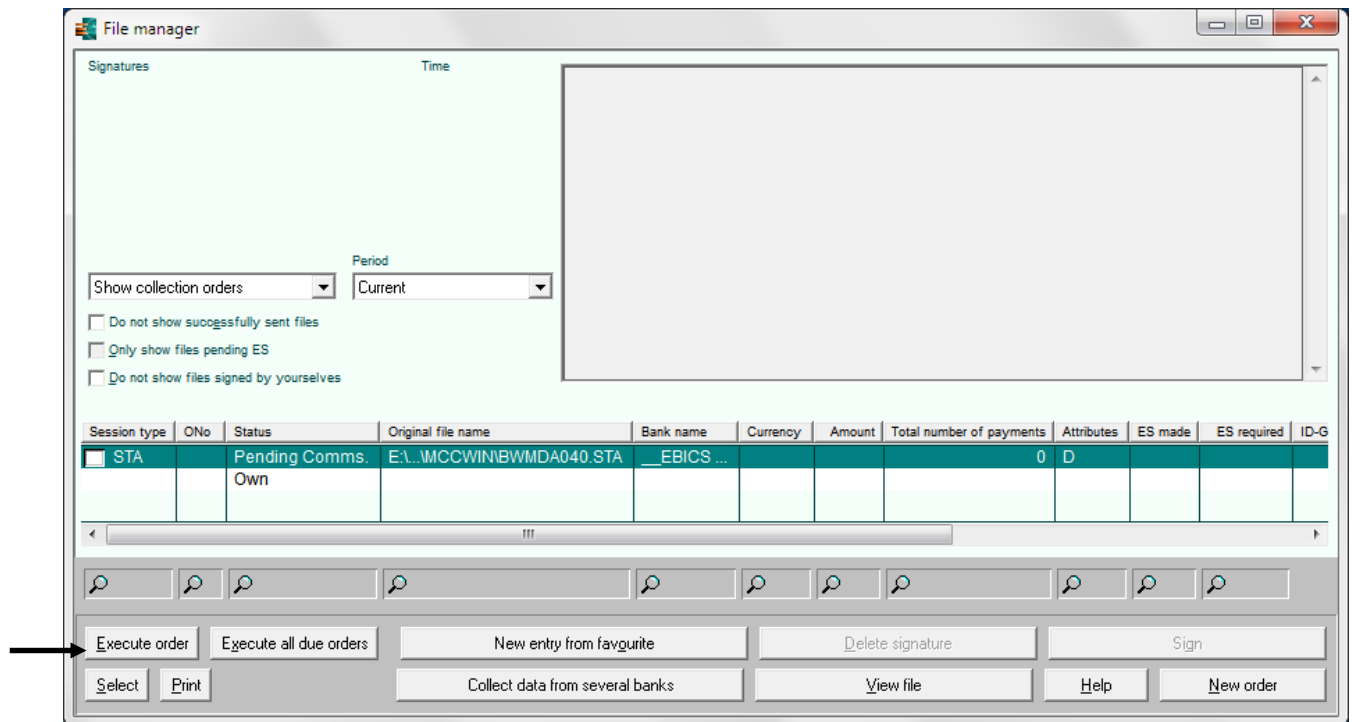
The screenshot shows the 'File manager' dialog box with the 'Password and execution data' tab selected. The fields are as follows:

- Bank:** OMIEBICS, Session type: STA, Attributes: Receive account data, User: MKA10001
- Session:** STA, File Type: Original file without signature, Encryption: (Hybrid DES/RSA)
- File:** E:_323\MCCWIN\BWMDA040.STA
- Password:** (Redacted with an orange box, indicated by arrow 1.)
- Other:** ID-Group: ?, Access class: ?
- Execution:** Repetition: Once, Pause in minutes before repetition?: 0, Execute on workstation: Own
- Period:** Collect data from/to: From 10.09.2012 To 10.09.2012

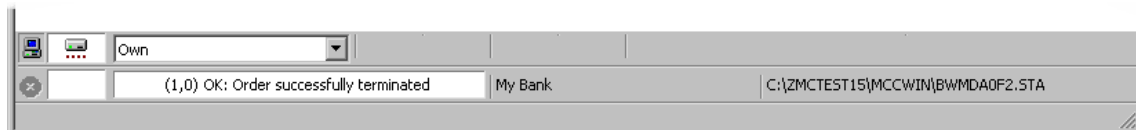
At the bottom right, there are 'Help' and 'Save' buttons. Arrow 2. points to the 'Save' button.

5 Execute order

The collection order now is created in the file manager. By clicking the [**Execute order**] button (→) you start the transmission of your order to your bank.

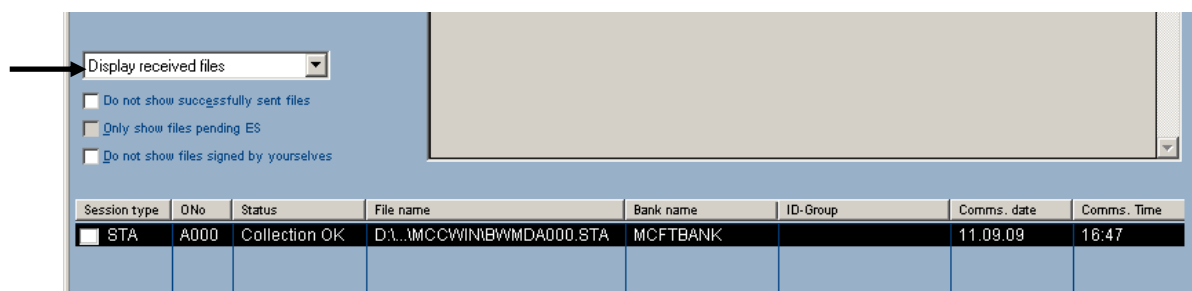


The transmission progress can be observed in the so-called Comms. bar:

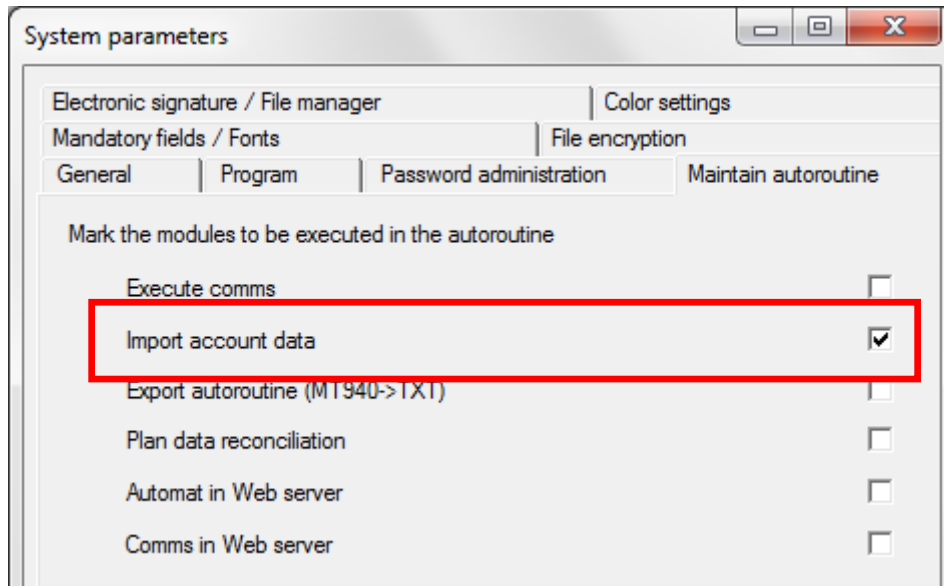


6 Display received files

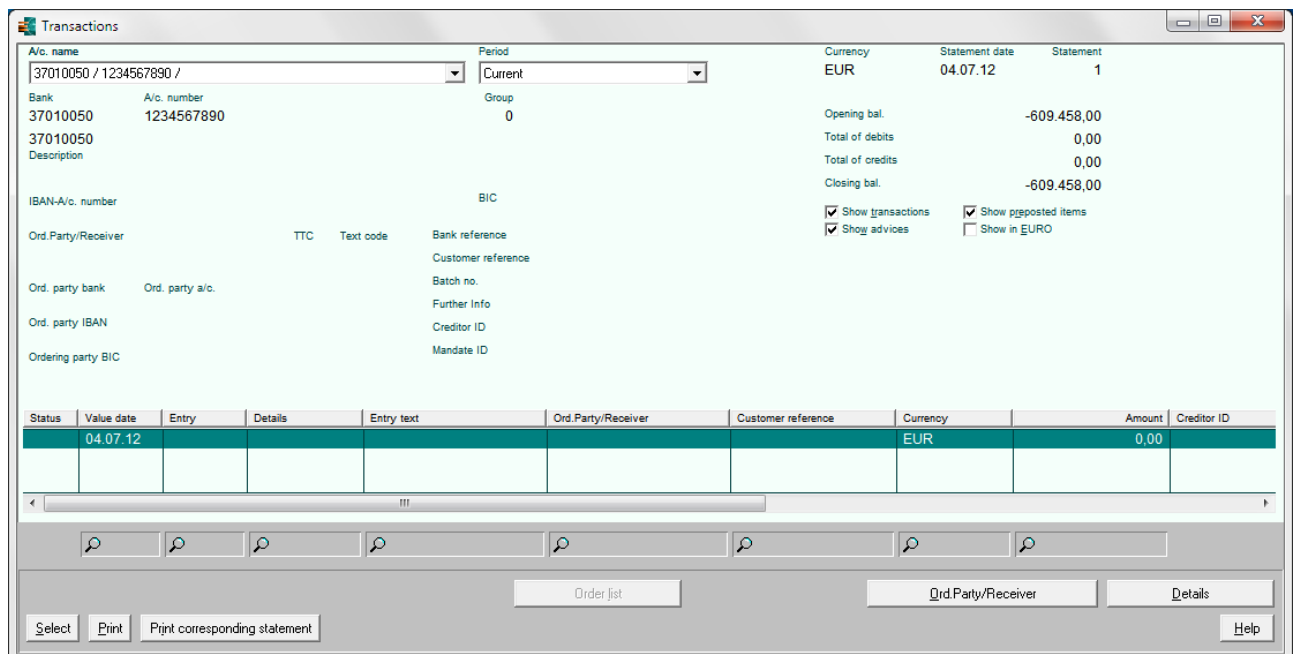
After successful transmission the single collection order disappears from the collection orders display. By selecting the "Display received files" option (→) the receipt of an appropriate file with account information can be controlled.



If you configured the system already so far that the collected account information is imported automatically (cf. Chapter 6.1.4 of the Core module: *Maintain autoroutine property page*),



You can now display these information using different reporting functions as balances, statements, value-dated balances etc. (for further information see the Chapters regarding Cash Management).



2.2 Define Autodial function

You can collect relevant information like statements, exchange rates, pre-posted items, FTAM logs etc. fully automatically via mouse-click from all your banks (so-called autodial function see Chapter 5.2 on Communication: *Wizard for the collection of data from several banks / Autodial function*).

To define or to change collection orders please choose the menu item **-Collecting data from several banks-** from the **-Communications-** menu.

A wizard will guide you through the steps that need to be taken to define collection orders from several banks.

1 Select the banks / Session types

Choose the bank from which you want to collect data by mouse-click from the list of banks (🏦). Select the download **session type STA**. By pressing the **[Add session type]** you will add the selected session type to the list of pre-defined collection orders.

The orders defined by you are shown in each case in the list below the bank (📄).

Repeat this process for each of the banks from which you want to collect data.

For the autodial function Comms. batches will be generated from the given information, which start the transmission automatically at the specified time.

The automatic data collection is made for all banks at the same time if you leave the predefined highlight of the checkbox **"Use the same execution frequency for all collection orders"** unchanged. If you want to start automatical data collections for different banks at different times or define several automatical data collections daily, you have to remove the highlight and enter an execution frequency separately for each collection order. Then press the **[Next >]** button.

Collect data from several banks

Bank / Session type	Compression	Encryption
123-Bank (123)		
EBICS mit Bankdaten (EBC323KK)		
STAG Receive account data	Yes	Yes
EBICS to omikron test bank__ (OMIEBICS)		

☐ Compress data ☐ Encrypt data

Abbreviation of batch order: AUTOMAT [New]

Available session types for bank:

- HTD G User information
- IIB G Receive Import collections (IIB)
- PTK G Receive log file
- QE2 G DTAUS im Bundesbankformat
- QG2 G MT103 im Bundesbankformat
- RDT G Direct debit return to customer (DTAUS0)
- SAM G Collect batch files
- ST1 G Account statements SWIFT (FR) non EUR
- ST2 G Account statements CFONB (FR) Pooled
- ST3 G Account statements CFONB (FR) individual
- STF G Receive CFONB account data

[Add session type]

[Remove marked collection order from processing]

Execution frequency

Comms. batches will be created from your details. These are normally configured so that the Comms. batch is started automatically on the corresponding due date.

Or you use the menu item to manually start all of these orders when you wish to do so.

☐ Start Comms. manually

☒ Use the same execution frequency for all collection orders

Repetition: Once

How many minutes pause before a repetition? 0

1. Transmission: 10.09.2012 00:00

Last date: 10.09.2012 00:00

< Zurück Weiter > Help

2 Enter Comms. password

Enter your current Comms. password (if not stored in the BPD). This is needed by the bank to verify the Comms. session.

The password definition is concealed, i.e. when you press a key you only see an * (asterisk) on the screen.

If you use the same comms password for all selected banks you can check the corresponding check box "**Use the same password for all banks**". This way, you will need to enter the password only once.

The screenshot shows a window titled "Enter password" with a close button (X) in the top right corner. Inside the window, there is a label "Bank(s)" next to a text field containing "J.P.Morgan". Below this, a paragraph of text reads: "You must now enter in each case the valid Comms. password for each selected bank. If you have the same Comms. password for all selected banks, then please activate this in the following field, then you have to enter the Comms. password only once." Below the text is a checkbox labeled "Use the same Comms. password for all banks", which is currently unchecked. Further down, there is a label "Comms. password" next to a text field containing "J.P.Morgan". Below this field, a paragraph of text reads: "Please enter your valid password. This is used for validation of the communication access with the bank." Below the text field is a label "Password" next to a small orange rectangular button with a blue icon. At the bottom of the window, there are three buttons: "< Zurück", "Weiter >", and "Help".

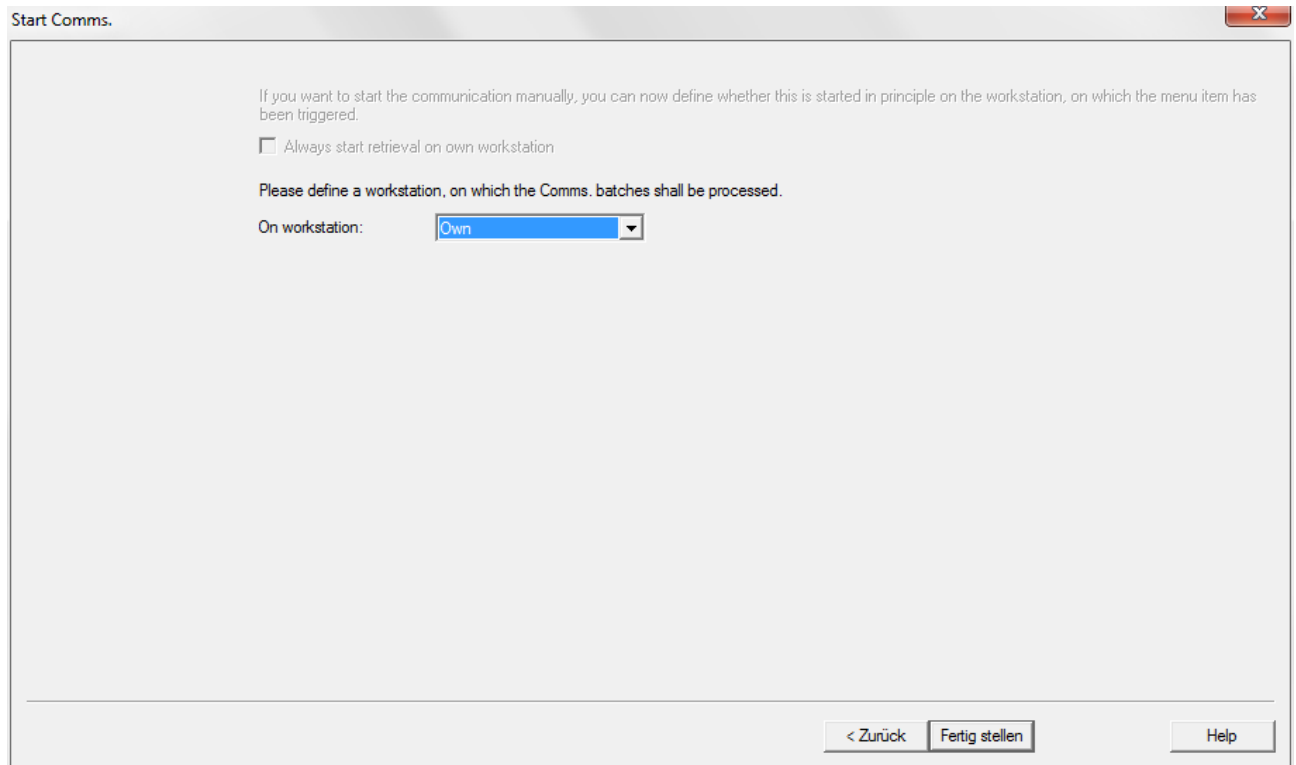
Your session will be saved. Step 2 is no longer required the next time you contact your bank. You will only be required to enter your Comms. password for verification if you add further session types.

Close password definition by clicking on [**Next >**].

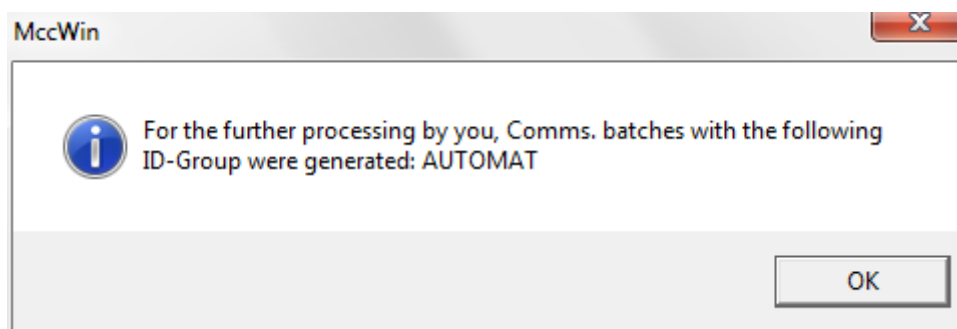
3 Complete definition of collection orders

Under the option "**On workstation:**" you define a computer within a network which should process the Comms jobs.

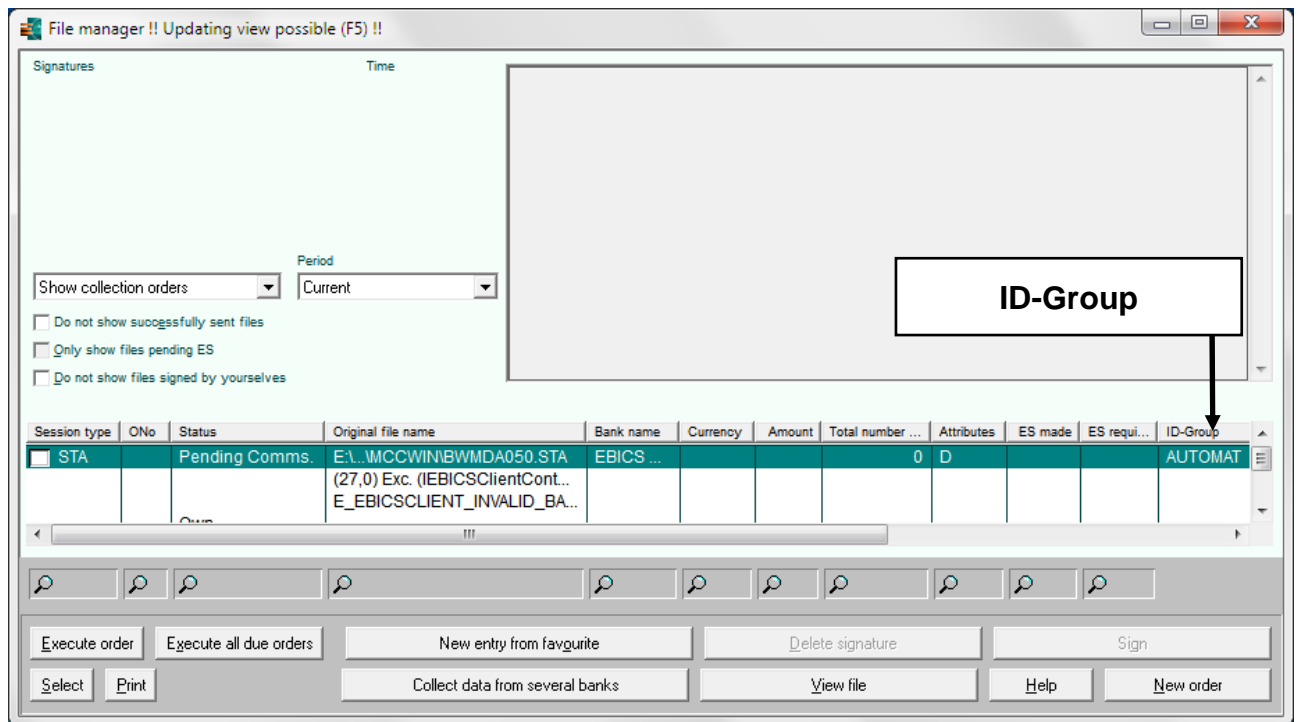
You can return to previous steps and make any necessary alterations using the [**< Back**] button



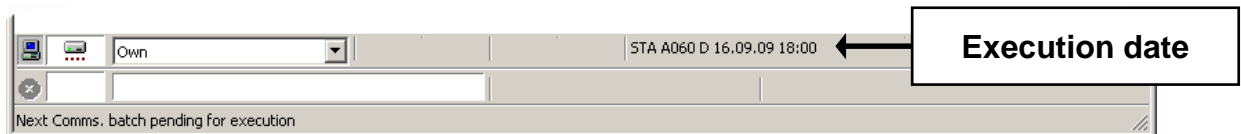
Using the [**Finish**] button the communication jobs are generated from your data. You can view these jobs in the "File Manager" and process them. Den entsprechenden Hinweis darauf bestätigen Sie mit [**OK**]:



You will find prepared orders with the ID-Group "AUTOMAT" in the File Manager then.



With activated Comms. bar (-View- menu) the collection process starts automatically on reaching the execution date defined before.



3 How to edit and send a payment?

In order to use this feature it is necessary that you have **installed** the Electronic Banking system components (see Chapter 2.2 of the manual for the Core Module), successfully **started the program** for the first time and properly **configured** the program system. The PC is normally set up by an administrator.

Start the payments module by clicking the relevant icon within the core module:



e.g.

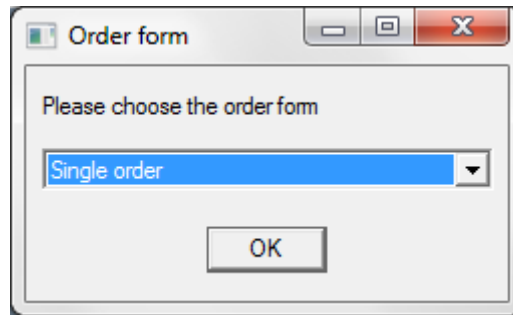
To create payment orders and send them to the bank(s), please follow the following steps:

1 Entering a payment order

To enter a payment order, select the symbol **Enter Payments**. If you have not yet entered payment orders, you will see an empty overview screen, which would normally contain a list of pending single orders. If you want to view another type of order than single orders, you must pre-select this using the list-box "Show order type". After this, you can move to the screen for entering new orders with the button [**New Order**].

Payment orders										
Order no. / End-To-End	Order form	Type	Ordering party	Partner	Currency	Amount	Due date	Approvals	from	
MCCT120910000001 E2EC120910000001	Single order	Credit transfer	Auftraggebername POBADEFF DE60700517550000007229	Partnername POBADEFF DE60700517550000007229	EUR	1.234.567,89	10.09.12	1	1	
MCDD120621000001 E2ED120621000001	Single order	Direct debit	Auftraggebername POBADEFF DE60700517550000007229	Partnername COLSDE33XXX DE97370501980033633322	EUR	12.345,00	04.09.12	0	1	
MCDD120621000003 E2ED120621000002	Single order	Direct debit	Auftraggebername POBADEFF	Partnername COLSDE33XXX	EUR	1.000,00	04.09.12	0	1	

If "All orders" have been displayed, you can select the wanted order form now.



You now see a form for keying payments (in this case SEPA Payments). Within this you can determine right above the exact type of the payment, e.g. credit transfer, direct debit etc. Here you can enter

- Account, ordering party and partner,
- (currency and) amount and
- details of your payment

If you have details available in your reference tables (especially the **bank parameter files** described in chapter 1 must have been **allocated** to the banks), you can access these by clicking on the [?] - Button in the relevant place in the overview, which allows you to accept the full data by mouse-click. Further details on your payment can be added on the relevant Register cards. All details which must be entered for the payment to be fully prepared are highlighted with a special background colour.

The field "Earliest transmission" allows you to determine when the payment should be sent to the bank. By default, the current date is entered here.

If you want to use the payment you have entered also as a template for keying further payment orders, you select the button [**Save and store as Standard**]. Otherwise you complete the entry by pressing the button [**Save**].

New entry Single orders

Additional information | Direct debit additional | LDGR data | Times

Payments | Partner | Ordering party / Internal | Ultimate parties

Order number MCCT120910000002 Single order

End-To-End reference E2EC120910000002 Credit transfer

Access class ?

A/c. code ? 2 Swift address POBADEFF IBAN DE60700517550000007229

Ord. party ? 3 Ord. party name Ordering party name

Ultimate ordering party ?

Payment purpose

Partner ? Partner name Partner name

IBAN DE60700517550000007229 Swift address POBADEFF Country

Currency EUR Amount 1.234.567,89 Gross/Net Add

Details

Approvals 0 of 1 Due date 10.09.2012 Earliest transmission 10.09.12

Save and store as template Help Save

After payments entry close the database overview showing all payment orders using the close button [x]. Further details on working with payment orders can be found in Chapter 4 of the manual for the payments module.

2 Approving a payment order

After you have entered your payment(s), these have to be approved. Please select the button **Single Approval**. An overview of payments pending approval is displayed.

PLEASE NOTE: If required, the due date of the direct debit collections is adapted according to the SEPA policies!

Order no. / End-To-End	Order form	Type	Ordering party	Partner	Currency	Amount	Due date	Approvals	from
MCCT120910000002 E2EC120910000002	Single order	Credit transfer	POBADEFF DE60700517550000007229	POBADEFF DE60700517550000007229	EUR	1.234.567,89	10.09.12	0	1
MCDD120621000001 E2ED120621000001	Single order	Direct debit	Auftraggebername POBADEFF DE60700517550000007229	Partnername COLSDE33XXX DE97370501980033633322	EUR	12.345,00	04.09.12	0	1

Buttons: Select, Print, Details, Do not display approved ones, Show order type: Single orders, Help

Mark the required payment with a double click. Then you will see full details of the payment and can approve it using the [**Approval**] button.

Single approval Single orders

Additional information | Direct debit additional | LDGR data | Times

Payments | Partner | Ordering party / Internal | Ultimate parties

Order number: MCCT120910000002 | Single order

End-To-End reference: E2EC120910000002 | Credit transfer

Access class: [] []

A/c. code: 2 | Swift address: POBADEFF | IBAN: DE60700517550000007229

Ordering party: 3 | Ordering party name: []

Ultimate ordering party: []

Payment purpose: []

Partner: [] | Partner name: []

IBAN: DE60700517550000007229 | Swift address: POBADEFF | Country: []

Currency: EUR | Amount: 1.234.567,89

Details: []

Approvals: 0 of 1 | Due date: 10.09.2012 | Earliest transmission: 10.09.12

Buttons: < > Print Help Approval

Alternatively you can make the approval also directly in the database overview by selecting menu item -Approval- with the right mouse button. Then close the approval database overview using the close button [x].

If a second approval is required, this can only be made if the module is closed and a new user with an authorization for approval logs on.

Larger numbers of payment orders can be approved more easily using the function **Approval per account**.

NOTE: Marked entries will be approved. (Mark with mouse or space-bar)
 With double-click you can view details of the order
 PLEASE NOTE: If required, the due date of the direct debit collections is adapted according to the SEPA policies!

Account / Swift address / IBAN / A/c. currency
 1 / COLSDE33XXX / DE97370501980033633322 / EUR

Value-dated balance including approved records: -4.000,00
 Total of non-approved records: -12.345,00
 Total of approved records: 9.880.543,21

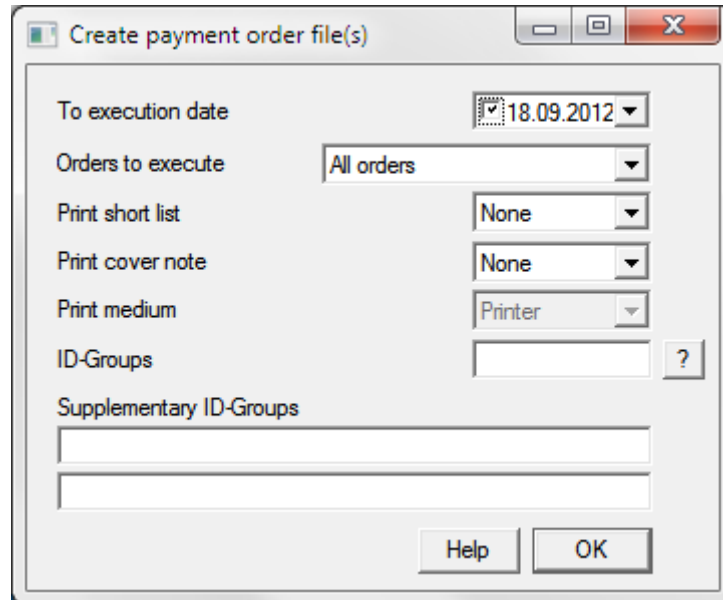
Order form	Order number	Ordering party	Partner	Currency	Amount	Due date
✓ Single order...	MCCT120828000003	OPDRACHTGEVER NAAM	PARTNER NAAM	EUR	4.000,00	28.08.12
Single order...	MCDD120625000001	ORDERING PARTY NAME	PARTNER WITH COUNTRY	EUR	12.345,00	04.09.12

Buttons: Highlight all, Delete highlight(s), Help, Approve orders

Further details on approving payment orders can be found in Chapter 5 of the manual for your payments module.

3 Creating a payment file (multi-bank oriented, without preview dialogs)

After selecting the function **Create payment order files**, a screen opens, allowing you to specify the payment file to be created. Close the window, if necessary after the input of data, by clicking on [**OK**].



The screenshot shows a Windows-style dialog box titled "Create payment order file(s)". It contains several configuration options:

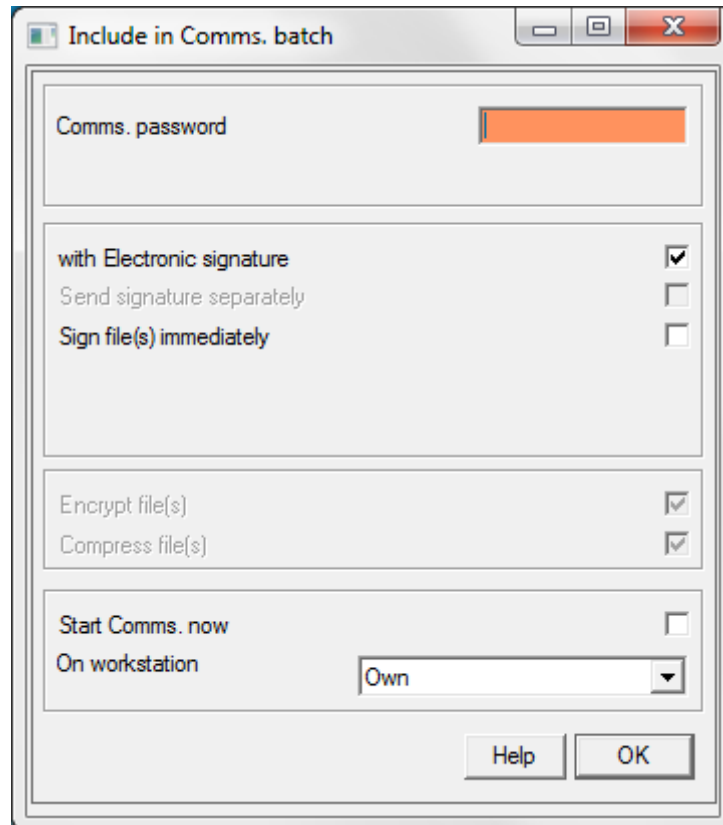
- To execution date:** A date picker set to 18.09.2012.
- Orders to execute:** A dropdown menu set to "All orders".
- Print short list:** A dropdown menu set to "None".
- Print cover note:** A dropdown menu set to "None".
- Print medium:** A dropdown menu set to "Printer".
- ID-Groups:** A text input field with a help icon (?) to its right.
- Supplementary ID-Groups:** Two empty text input fields.

At the bottom right of the dialog are two buttons: "Help" and "OK".

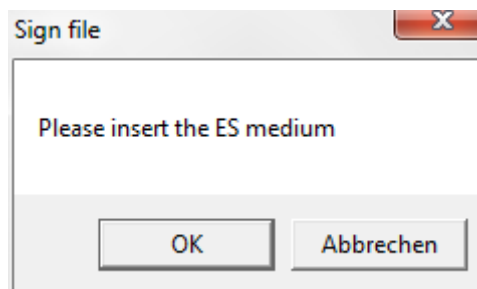
Further details on creating payment files can be found in Chapter 6 of the manual for your payment module.

4 Prepare payments for sending (including signature)

Enter the Comms. password in the appropriate field, if not stored in the BPD and already entered here.



If you mark the field "**Sign file(s) immediately**", you can enter the "**ES password**". The accomplishment of the signature then follows directly. Otherwise, the file will be entered first in the File Manager, from where you can add signature(s) later (continue with step 6). Close the dialog box after the entry of the ES password by pressing [**OK**].



After inserting the ES medium confirm with [**OK**].

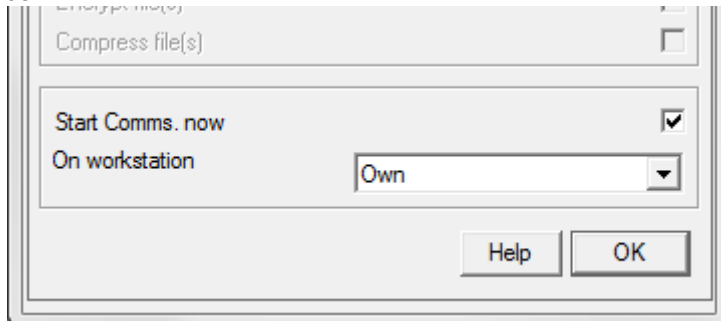
Now the signature file associated with the original file is created.

You finish the entry of further signatures by answering the prompt for further signatures with [**No**].

Answer the concluding question for completeness with [**Yes**]. Then the file is entered with the status: "Pending Comms." in the file manager, where you have to execute it subsequently.

5 Execute payment file immediately (i.e. send it directly)

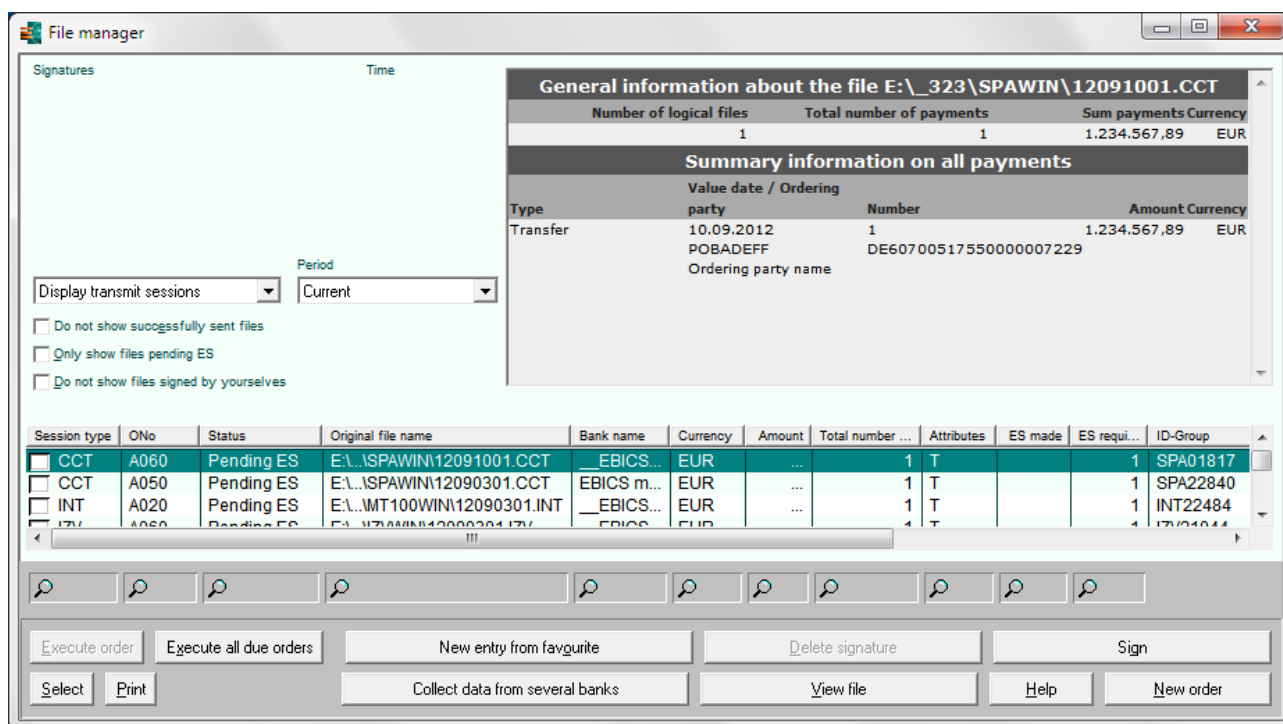
If you mark the parameter **"Start Comms. now"** and confirm with **[OK]**, the communication to the bank is started at once.



6 Signing and sending payment file(s) later

After calling the **File Manager** in the core module, you will see a database overview with payment files pending communication, with the newest files at the top.

If you wish to sign one or more files, select the relevant file and click on the **[Sign]** button.



In an additional window which opens next to the file display, you are prompted to enter your "ES-Password" and "ES-User".

An **ES-User** name only has to be entered if another user than the one currently logged on has to make the signature. This "new" user can of course have his own ES-Password. If he enters this ES-Password, the key disk should be held ready. If the signature is to be made by the user already logged on, the field can remain unchanged.

The **ES-Password** is the password with which the key pair was encrypted on the key disk.

Sign file

General information about the file E:_323\SPAWIN\12091001.CCT

Number of logical files	Total number of payments	Sum payments	Currency
1	1	1.234.567,89	EUR

Summary information on all payments

Type	Value date / Ordering party	Number	Amount	Currency
Transfer	10.09.2012 POBADEFF Ordering party name	1 DE607 00517550000007229	1.234.567,89	EUR

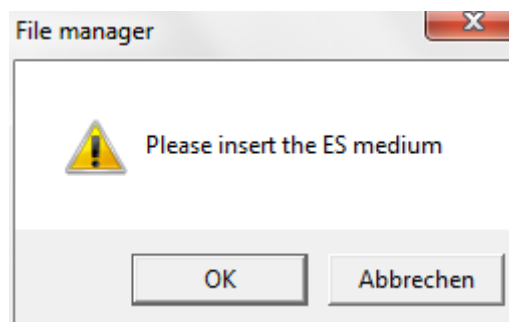
Hash value: A5C8F601 (CHK.2)

User: 2

ES password:

Help OK

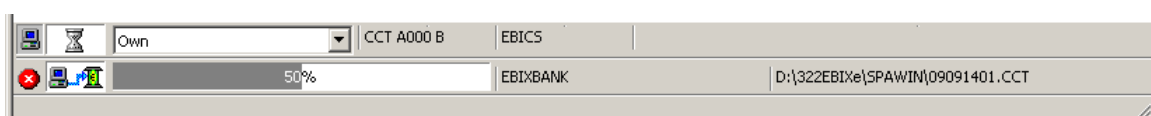
Following this, the procedure is according to the steps defined under step 4. You are prompted to insert the ES medium and to confirm it with [OK].



The following prompt for signature completeness is to be answered with [Yes] (Status in the file manager: "Pending Comms.").

To send a file, select the file to be sent and press the [**Execute order**] button. You can send several files at once (this function can also be used for signing), if you have activated several orders before using check boxes in the session type column.

With active Comms. bar (to be started using the appropriate item in the -View- menu) the connection to the bank computer is established immediately and the transmission starts.



After successful Comms., the status of the file is changed to "OK".

If an error occurs during transmission, the message "Defective" is shown; under the file name you will see an error number and a short error text (e.g. (11/0) Transmission interrupted). Tips on what to do in such situations are included in the manual on Communication, Chapter 5.4: *Return codes*, where the error numbers of the various comms processes are listed and described.

With MCFT the reconciliation of status information concerning the ES check takes place immediately within the transmission via so-called acknowledgement messages. In contrast to that with FTAM/FTP/EBICS you have to start a **log collection** order after the transmission. This can be made automatically, if it was stored in the respective bank parameter file accordingly:

EBICS - Bank parameter file

Description of the bank parameter file:

Bank connection details:

Address (URL): Check access

Authentication status of the bank:

Information regarding the bank:

Customer-ID: Host name: Operation mode: EBICS-Protocol version:

Automatic collection of PTK files:

How many minutes after sending a file (0=Never)?

Allocations Internal user and user no. at bank:

Internal name	External name	Save Comms. password	Default user	Current ES version	EBICS status
SYSADMIN	MKA10004	No	No	A004	Ready
2	MKA10002	No	No	A004	New
10	MKA10001	No	No	A004	Ready
1	MKA10001	No	Yes	A004	Ready
MEIER	MKA10001	No	No	A004	Ready

New user Change Comms. password Hash values of bank EBICS parameter Help Save

With the status "ES check OK" in the file manager the payment transmission is completed.

Session type	ONo	Status	File name	Bank name	Currency	Amount	Attributes	ES made	ID-Group
<input checked="" type="checkbox"/> IZV	A0K5	ES check OK	C:\...IZVWIN12032701.IZV (1,0) OK	EBICS ...	EUR	1.234.567,89	B	1	1

In the detailed view of the database record you can control the result of the transmission / the ES check on the "ES log" property page:

File manager

Communications | **ES log** | Post-Processing

File name: C:\ZMCTEST21\IZVWIN\12032701.IZV

BPD file name: OMIEBICS | _EBICS to omikron test bank_ | ES check OK

File type: IZV Domestic payments file

Access class: ?

☐ Received ☒ Send

Attribute: B Order number: AOK5

```

27.03.12 09:55:50    Unterschrift zur Bank uebertragen
      Hostname      : EBICSSRV
      Auftrag       : Inlandzahlungsverkehrsdatei          IZV AOK5
      Teilnehmer     : MKA10000 MKA10001 mka A
      Ergebnis      : Uebertragung in Ordnung [01]

27.03.12 09:55:50    Datei zur Bank uebertragen
      Hostname      : EBICSSRV
      Auftrag       : Inlandzahlungsverkehrsdatei          IZV AOK5
      Teilnehmer     : MKA10000 MKA10001 mka A
      Ergebnis      : Uebertragung in Ordnung [01]

27.03.12 09:55:51    Unterschriftspruefung [21]
      Hostname      : EBICSSRV
      Auftrag       : Inlandzahlungsverkehrsdatei          IZV AOK5
      Kunde         : MKA10000
      Teilnehmer     : MKA10000 MKA10001 mka A
      Ergebnis      : EU unvollständig, Warten auf VEU [38]
      Dateiname     : C:\ZMCTEST21\IZVWIN\12032701.IZV

      Bankleitzahl   : 37050299
  
```

< > Print Help Save

Further information on executing Comms. can be found in Communication-Chapter 5.

7 Logs

All logs concerning Comms. and all other events in the system can be displayed in the Core module using menu item -Logs- / -View system log -.

System log (Log size: 2047 records) (Searching pauses)

File SPAWnd.cpp
 Line 2022
 Function CSPAWnd::SpeichereStandardSatz
 Number 2008
 RC 4

Text
 Template STANDARD 000005 was added to the database

Date	Type	User	Application	Text	Return code	BPD file	User ID	Session type	Job number
10.09.12 16:49:25:988	System	2	MCC	Database maintainance Sign and send files	0				
10.09.12 16:49:23:789	System	2	SPA	End SEPA Payments	0				
10.09.12 16:49:13:666	Error	2	SPA	No order found.	0				
10.09.12 16:47:52:051	System	2	SPA	Internal module Create payment order files	0				
10.09.12 16:44:36:841	System	2	SPA	Dialog Approval by account of payment orders	0				
10.09.12 16:41:57:302	System	2	SPA	Database maintainance Single approval of payment orders	0				
10.09.12 16:40:17:151	Error	2	SPA	Partner has not yet been approved after change.	0				
10.09.12 16:39:55:423	System	2	SPA	Database maintainance Enter, view and change payment orders	0				
10.09.12 16:39:43:148	System	2	SPA	Database maintainance Enter, view and change Partners	0				
10.09.12 16:39:06:449	Info	2	SPA	Template STANDARD 000005 was added to the database	4				
10.09.12 16:36:47:297	System	2	SPA	Database maintainance Enter, view and change payment orders	0				
10.09.12 16:36:44:552	System	2	SPA	Internal module Autoroutine	0				
10.09.12 16:36:44:552	System	2	SPA	Program start SEPA Payments	0				
10.09.12 16:36:43:819	System	2	MCC	External Program ..\SPAWINPRG\SPAWIN31.EXE	0				

Select Print Archive Additional information Help

More information regarding the logs can be found in Chapter 2.4 of your Payments module or in Chapter 6.10 of the Core module.