

MultiCash[®] 3.23

Communications

User Manual


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

Introduction

This document has been designed for electronic distribution and printing on a laser printer. Therefore, the used fonts and page layout have been chosen mainly to ensure an optimal result in print, whereas its suitability for on-screen usage was a secondary issue.

Use the main table of contents and the tables of contents at the beginning of each chapter to jump to a concrete topic. Clicking on an entry in the table (the cursor changes to ) takes you to the required page.

Printing this manual

This PDF document has been optimized for printout in DIN A4 format. Use your Acrobat Readers "Print" function to print the manual or parts of it.

Information on using this manual

Refer to chapter 3.1 of the Core module for further details on how to use the manual.

Online help

For reading the documentation on-screen, call up the online help provided with the program (refer to chapter 3.2 of the Core module manual for further details on using the help file). Unlike the manual, the online help enables key word and full text search as well, making it even easier to find information on specific topics.

Copyright

© 2000-2012 Omikron Systemhaus GmbH & Co. KG

All rights reserved.

No part of this document may be translated or edited by any means, including, but not limited to, electronic or mechanical.

All information contained in this manual has been collected and tested with the highest possible accuracy. However, mistakes can never totally be excluded. Omikron can take no responsibility and assumes no liability for any alleged or actual damage arising from incorrect information in this documentation. Suggestions for improvement, reports on mistakes and any kind of qualified criticism will be appreciated.

Omikron Systemhaus

Table of Contents

Table of Contents: Chapter 1	1-1
1 Data communications	1-2
1.1 Communication	1-3
1.2 Comms. methods	1-4
1.2.1 EPFT	1-6
1.2.2 MCFT	1-9
1.2.3 FTAM	1-13
1.2.4 FTP	1-18
1.2.5 EBICS	1-21
1.2.6 HBCI/HBCI+	1-25
1.2.7 ETEBAC	1-26
Table of Contents: Chapter 2	2-1
2 Communication menu	2-2
2.1 Comms. parameters	2-3
2.2 Modem PAD access property page	2-4
2.3 X.25 - leased line property page	2-7
2.4 Modem-Modem property page (direct connection)	2-10
2.5 ISDN CAPI property page	2-12
2.6 TCP/IP connection property page	2-13
2.7 Priorities property page (Comms. procedures)	2-15
2.8 AT Commands	2-17
Table of Contents: Chapter 3	3-1
3 Define Bank Parameter Data files	3-2
3.1 Create BPD	3-3
3.2 EPFT / MCFT	3-5
3.2.1 Import MCFT BPD	3-10
3.2.2 Export MCFT BPD	3-12
3.3 FTAM	3-13
3.4 FTP	3-17
3.5 EBICS	3-19
3.6 HBCI	3-27
3.7 HBCI+	3-32
3.7.1 Maintain period (HBCI and HBCI+)	3-35
3.7.2 Maintain TAN list (HBCI+)	3-36
3.8 ETEBAC3	3-37
3.9 WOP	3-41
Table of Contents: Chapter 4	4-1
4 Special communication functions	4-2
4.1 Change Comms Password (Session type PWA)	4-3
4.2 First initialization of bank access (Session type INI)	4-5
4.3 Reset EPFT/MCFT communication access (Session type RES)	4-10
4.4 Block a Comms. access (session type SPR)	4-13
4.5 Encryption for FTAM/FTP transmissions	4-15
4.5.1 Activate encryption with banks	4-16
4.5.2 Encryption return codes	4-21
4.6 Convert FTAM/FTP bank access to EBICS	4-22
4.7 Exchange EBICS authentication keys	4-26
4.8 Change EBICS Comms. password	4-31

4.9 Key media administration wizard	4-32
4.10 Manage certificates	4-34
4.10.1 Generate system key and certificate	4-35
4.10.2 Generate TLS key and certificate.....	4-36
4.10.3 Generate certificate request.....	4-39
4.10.2 Import certificate	4-41
4.10.3 Assign certificate.....	4-42
Table of Contents: Chapter 5	5-1
5 File Manager / Execute Comms.	5-2
5.1 File Manager.....	5-2
5.1.1 Database overview: File Manager.....	5-3
5.1.2 File Manager: View Details	5-20
5.1.2.1 Communications property page	5-21
5.1.2.2 Post-processing and transfer parameters property page	5-23
5.1.2.3 Comms. log / ES log property page.....	5-27
5.2 Wizard for collecting data from several banks / Autodial function	5-28
5.3 Execute Comms.....	5-33
5.4 Return codes.....	5-35
5.5 Post-processing / User Exits.....	5-50
5.6 Monthly statistics (supplementary module)	5-52
Table of Contents: Chapter 6	6-1
6 Electronic Signature.....	6-2
6.1 Generate / Send ES keypair	6-3
6.2 Change ES Password.....	6-8
6.3 Convert signature version	6-9
6.3.1 Convert ES version from A003 to A004 (only for FTAM/FTP accesses)	6-10
6.3.2 Convert ES version to A005 / A006 or M005 / M006	6-12
Index	I-1

Table of Contents: Chapter 1

	Page
1 Data communications	1-2
1.1 Communication	1-3
1.2 Comms. methods	1-4
1.2.1 EPFT	1-6
1.2.2 MCFT.....	1-9
1.2.3 FTAM.....	1-13
1.2.4 FTP.....	1-18
1.2.5 EBICS.....	1-21
1.2.6 HBCI/HBCI+.....	1-25
1.2.7 ETEBAC.....	1-26

1 Data communications

A variety of communications processes are available for data transmission.

The EPFT communication method is always installed with the Core module. The installation of other communication methods (such as FTAM, FTP, EBICS, HBCI/HBCI+, ETEBAC) is optional..

MCFT is a special form of EPFT. In addition to the advantages of secure transmission of compressed data, MCFT also allows the reproduction of enterprise signature hierarchies using the Electronic Signature facility. The signature is verified online so that the customer can be informed immediately about the validity of the transmitted signatures. The MCFT communication method is also installed as a standard application.

To use the MCFT and FTAM communication methods, the "Electronic Signature" supplementary module must first be installed.

The data transmission parameters which need to be set for the various communication methods are described in the Communications Menu.

You will find details for the meaning of the process specific Comms. return codes in Chapter 5.4:

- EPFT return codes
- MCFT return codes
- FTAM return odes
- FTP return codes
- EBICS return codes

Chapter 4.5.2: *Encryption return codes* describes the meaning of special encryption return codes used with FTAM or FTP transmissions.

1.1 Communication

In menu -Communication-, inter alia Comms. parameters are set, bank parameter files (BPD files) are created or changed, files in the file manager are signed and sent etc.

The menu item -Comms. Administration- contains commands to create and edit BPDs (Bank Parameter Data files) and define the parameters for data transmission.



Submenu items -Maintain TAN list- and -Maintain periods- are only displayed if you have installed the "HBCI" or "HBCI*" supplementary modules.

The submenu item -Encryption- is only shown if you have installed "FTAM" or "FTP" supplementary module.

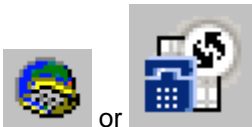
Information on the menu items can be found in Chapter 2: *Communications menu*.

The toolbar also contains the following icons which relate to the communications functions:



or

This icon corresponds to the menu item -Communication- / -File Manager-.



or

This icon corresponds to the menu item -Communication- / -Execute Comms favourite-.



or

This symbol corresponds to menu item -Communication- / -Assistant for collecting data from several banks -.

1.2 Comms. methods

A variety of communications processes are available for data transmission.

The EPFT and MCFT communications methods are always installed. Installation of other communication methods (such as FTAM, FTP, EBICS, HBCI/HBCI⁺) is optional.

MCFT is a special form of EPFT. In addition to the advantages of secure transmission of compressed data, MCFT also allows the reproduction of enterprise signature hierarchies using the Electronic Signature facility. The signature is verified online so that the customer can be informed immediately about the validity of the transmitted signatures.

The characteristics featured in optimum communications processes as defined by the ZKA standards are shown in the following tables (separately for Electronic Banking and Home Banking).

Electronic Banking:

	MCFT	FTAM	FTP	EBICS
Feature	special procedure, tailored for Electronic Banking needs	Combination of standard processes	Combination of standard processes	Internet
Verification of error-free data transmission	yes	only with ES	yes	yes
Compression	yes (ZIP procedure)	FLAM (optional)	FLAM (optional)	yes (ZIP procedure)
Encryption	Triple DES with asymmetric Diffie/Hellman key exchange	DES/RSA hybrid method (optional)	DES/RSA hybrid method	TLS(SSL) and DES / RSA-Hybrid procedure
Format validation	during transmission	after transmission	after transmission	after transmission
Pre-Authorization check	always	no	optional	optional
Notification of validation results	immediate at the end of the transmission	later in the log	immediate or later	later in the log
Authorization / Protection against manipulation	RSA ES 1024 bit RipeMD-160 <u>direct</u> validation (online)	RSA ES 1024 bit RipeMD-160 separate files offline validation	RSA ES 1024 bit RipeMD-160 optional: pre-validation (online) detailed offline validation	RSA ES 1024 bit / 1536 -4096 bit RipeMD-160 / SHA-256 optional: pre-validation (online) detailed offline validation
ES	yes (optional)	yes (optional)	yes (optional)	yes
Distributed ES	yes	no	yes	yes

Communi- cation media	Modem X.25 ISDN TCP/IP (Internet)	X.25 ISDN	TCP/IP (Internet)	TCP / IP (Internet)
Application	Electronic Banking Europe	Electronic Banking Germany	Electronic Banking German private banks	Electronic Banking Germany

Home Banking

	HBCI	HBCI+
Feature	Internet	Internet
Verification of error-free data transmission	TCP/IP	TCP/IP
Compression	yes	yes
Encryption	yes	yes
Validation (syntactic check)	no	no
Authorisation/ Protection against manipulation	RipeMD / RSA	PIN / TAN
ES	yes	no
Distributed ES	no	no
Communication media	TCP/IP (Internet)	TCP/IP (Internet)
Application	Home Banking	Home Banking

The communication methods use a variety of networks for data transmission. These are listed below.

Method	Feature	Speed	Hardware	Misc.
X.25	Packet transfer Public and private networks	9,600 - 28,800 bps depending on PAD	Modem or X.25 card	Service Provider
ISDN	Digital transmission Public networks	64,000 bps	ISDN card	
Com-Com	Analogue using telephone network	9,600 - 57,600 bps depending on network quality	Modem Digi board	
TCP/IP	Internet protocol	several megabits depending on service	Network card (DSL) modem	Service Provider Fire wall

1.2.1 EPFT

The EPFT communication method was developed in 1985 on the basis of standards adopted by the Central Credit Committee (ZKA) of the German banking industry, and thus incorporates all the features describing a secure communications process in these standards.

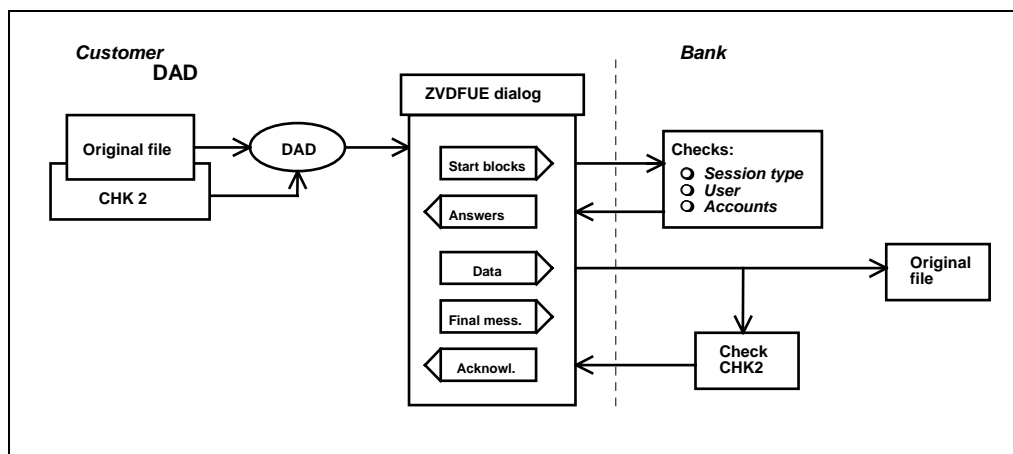
The procedure was enhanced permanently and extended e.g. by the Electronic Signature. In this form the procedure is called MCFT (**M**ulti**C**ash **F**ile **T**ransfer, see Chapter 1.2.2) and is currently used in Germany by around 50 banks. MCFT is also used by many banks in other European countries (Austria, France, Czech Republic, Hungary, Netherlands, Poland, Romania, Russia, Slovakia, Spain, Switzerland and others). This method was adopted as the national standard in Luxembourg in 1994.

	EPFT
Feature	Special process tailored to ZKA standards
Verification of error-free data transmission	yes
Compression	yes (ZIP procedure)
Encryption	Triple DES with asymmetric Diffie/Hellman key exchange
Format validation (syntactic check)	during transmission
Pre-Authorization check	always
Notification of validation results	immediate at the end of the transmission
Authorization/Protection against manipulation	PRF2 direct validation (online)
ES	no
Distributed ES	no
Communication media	Modem X.25 ISDN TCP/IP (Internet)
Application	Electronic Banking Europe

With the EPFT method (**E**lectronic **P**ayment **F**ile **T**ransfer), communication between customer and bank is divided into different stages for security reasons. A dialog takes place between the bank computer and the customer system.

The following diagram shows a simplified summary of these steps:

Online file transfer using EPFT



Dialog steps:

- **Start message**

Once the connection has been established between the customer and the bank, the customer computer logs on to the bank computer with a start message. In addition to the user number, the session type of the file to be transferred, the Bank ID and the account number, the KZV (Customer Payment Key) is a major component of the start message.

The Customer Payment Key (KZV) is a dynamic key calculated individually for each user using the **Diffie/Hellman Public-Key-Exchange** method. This method is illustrated later in this chapter.

The key itself is not transmitted, but forms the start value for the subsequent **Customer Payment Key Recalculation**. Only the change calculated in the Customer Payment Key is transmitted to the bank.

- **Answer message**

If the user is identified by the Bank computer on the basis of the start message (authorisation for the session type to be transmitted, PIN, etc.), the Bank computer sends an answer message. The data is only transmitted after the Bank computer's answer message has been received.

- **Online transfer message(s)**

The payment data is encrypted and compressed on the customer computer before transmission. It is decrypted and decompressed by the Bank computer.

To compress/decompress DTAUS and DTAZV files, a method has been specially developed for EPFT which ensures optimum compression. PKZIP is used to compress/decompress other file types (including MT 940 files).

- **Trailer message**

Once all online payment transfer messages which will be transferred in a single session have been transmitted from the customer computer to the Bank computer, the Bank computer receives a message that no further online payment transfer messages will follow. At the same time, the checksum for the transmitted data is sent to the Bank computer.

Return codes (cf. Chapter 5.4: *Return codes*), which describe the status or the result of the Comms, will also be transferred.

- **Acknowledgement message**

If all online payment transfer messages have been received without error by the Bank computer and the checksum sent by the customer computer matches the checksum calculated by the Bank computer, the Bank computer sends an acknowledgement message to the customer computer, closing the transmission session. This is followed by the recalculation of the KZV Customer Payment Key on both the customer and Bank computers (KZV Recalculation). The newly calculated KZV is required for the next transmission.

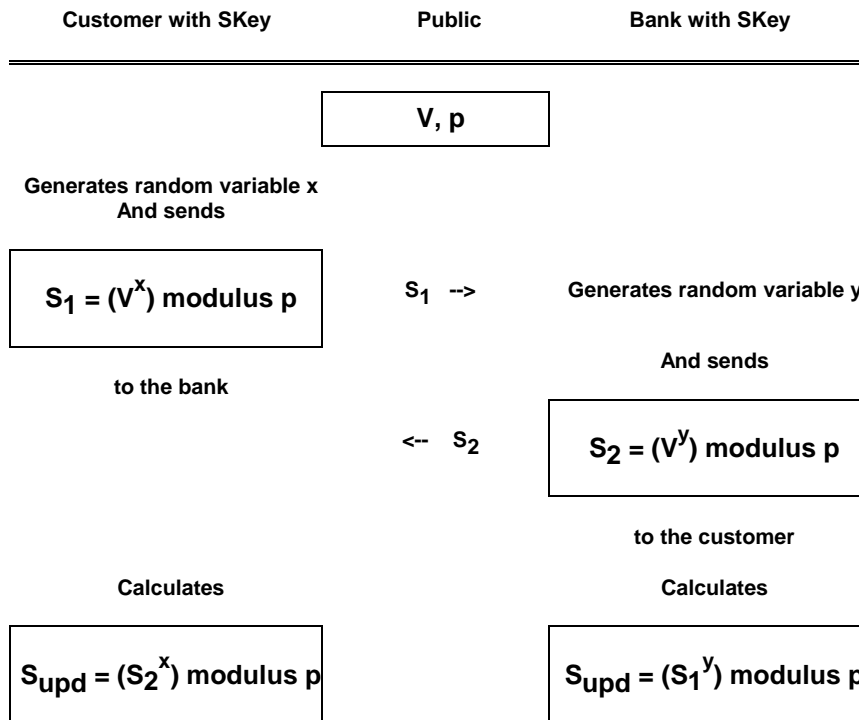
The Customer Payment Key (KZV) is a symmetric key, i.e. both communication parties (= bank and customer) use the same key to encrypt and decrypt the a message.

The change in key at both the bank and customer end after each transmission records which (user-oriented) Bank Parameter Data file was used for transmission. This is because file transfer can only take place if the keys are identical, i.e. each communicating party knows the agreed keys.

It is not possible to record which person (member of staff) transmits data using the user-oriented Bank Parameter Data file.

At the same time, this key replacement procedure provides secure protection against manipulation because each key is only used once.

Diffie/Hellman Public Key Exchange



S₁ and **S₂** cannot be used to deduce **Y** and **X** as this is a "one way function".

The variable **V** and the value of the modulus calculation **p** are accessible to all parties, i.e. they are public. Both numbers are prime numbers and it applies: $V < p$.

The CUSTOMER generates a random variable **x**. The public variable **V** is exponentiated by the random variable **x** and modulus **p** is calculated. The result of this calculation, the key **S₁** is sent to the BANK.

In turn, the BANK generates a random variable **y**. In this case too, the public variable **V** is exponentiated by the random variable **y** and modulus **p** is calculated. The result of this calculation, the key **S₂**, is sent to the CUSTOMER.

At both the customer and the bank side, the exchanged keys **S₁** and **S₂** form the basis for calculating the key update (**S_{upd}** or KZVUpdate). The **S_{upd}** is linked to the existing Session key (SKey) and thus forms the new SKey (= Session Key) to be used for the next transmission.

1.2.2 MCFT

MCFT is based on the standard EPFT protocol. This standard method has been extended by the inclusion of an Electronic Signature facility to provide a record of which person (member of staff) has transmitted data using the user-oriented Bank Parameter Data file.

All other features, for example compression and encryption, are identical to those of EPFT.

	MCFT
Feature	EPFT + ES
Verification of error-free data transmission	yes
Compression	yes (ZIP procedure)
Encryption	Triple DES with asymmetric Diffie/Hellman key exchange
Format validation (syntactic check)	during transmission
Pre-Authorization check	always
Notification of validation results	immediate at the end of transmission
Authorization/ Protection against manipulation	RSA ES 1024 bit RipeMD-160 <u>direct</u> validation (online)
ES	yes
Distributed ES	yes
Communication media	Modem X.25 ISDN TCP/IP (Internet)
Application	Electronic Banking Europe

You can use various Electronic Signature (ES) types using version M000, M001 and M002 to generate the ES on the customer computer (ARL, SNI, Concord-Eracom, Omikron). The version determines the method for calculating the hash value for the ES. The bank computer must be able to verify Electronic Signatures generated with all ES types using version M000, M001 and M002 and transmitted using MCFT.

The hash function generates a checksum for a file of any length (= original file). The hash value calculated in this serves as the basis for the Electronic Signature.

The **Electronic Signature** is based on an asymmetric encryption method. Each communicating party uses a keypair consisting of a private key and a public key. The most well-known public key method is **RSA**, named after its developers Rivest, Shamir and Adleman. It is also used in the customer and the bank system.

The "ES" supplementary module on the customer computer generates such a keypair. The public component of the keypair is transmitted online to the other communicating party (the bank or banks). In contrast, the private key is saved on a diskette additionally secured by an ES password. If messages are exchanged between the communicating parties, the message to be sent from the customer computer (= payment order) is encrypted using the private key. The other communicating party receiving the message (bank) decrypts the message with the public key sent to the bank. A communicating party can only decrypt a message if it also has the public key matching the private key.

The transmission of payment orders is preceded by the transmission of a **start block**. This start block contains all information needed for verification, such as the customer ID, the user number, the account to be debited, the Electronic Signature and checksums for the complete file, plus the TAN (transaction authentication number) which unambiguously identifies the sender of an order. This allows errors

and/or manipulation attempts to be identified at an early stage and transmission of the actual payment data to be stopped.

If an **Electronic Signature** is transmitted using MCFT, the start block also contains the "fingerprint" for the Original file and the Electronic Signature itself. The advantage of this is that as long as all the required signatures have been entered, the Electronic Signature can be verified during transmission. Up to 6 signatures can be transmitted in the start block.

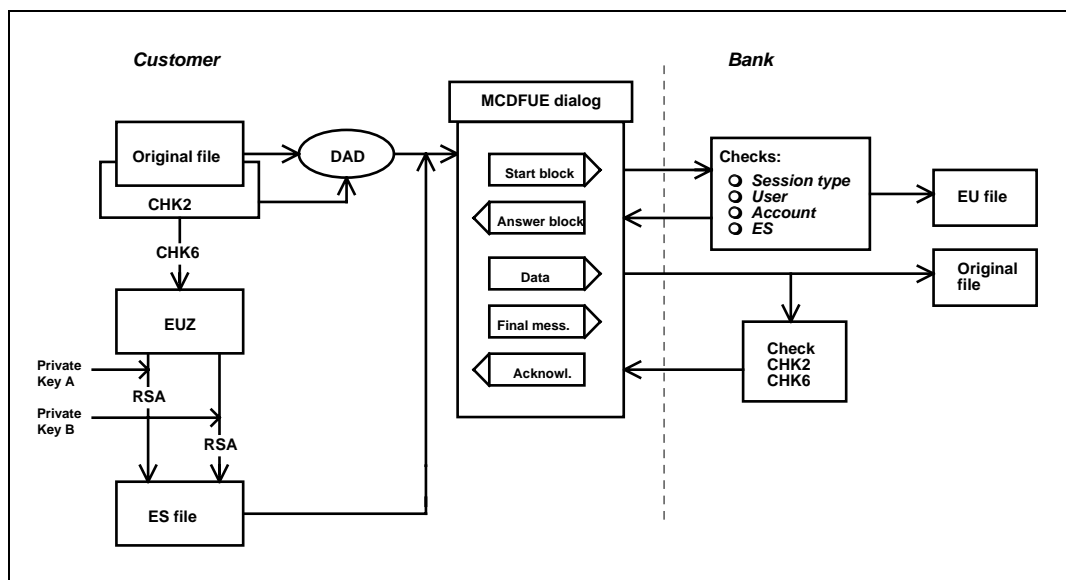
If verification by the Bank computer shows that

- a signature contained in the start block is incorrect, the communication session is cancelled before the Original file is sent.
- all signatures are correct, the Original file is transmitted. When the Original file has been transmitted, the Bank computer recalculates the "fingerprint" and compares it with the fingerprint which was transmitted in the start block and found to be correct. If the recalculation of the "fingerprint" matches the values previously transmitted, this is notified to the customer computer by an "OK" in the trailer block. If the recalculated "fingerprint" does not match the fingerprint transmitted in the start block, the original file is rejected.

Final messages are transmitted when either communications or the dialog has been completed. They contain return codes (cf. Chapter 5.4: *Return codes*), describing the status or results of communications.

The return codes received by the customer system are evaluated and displayed in the appropriate logs.

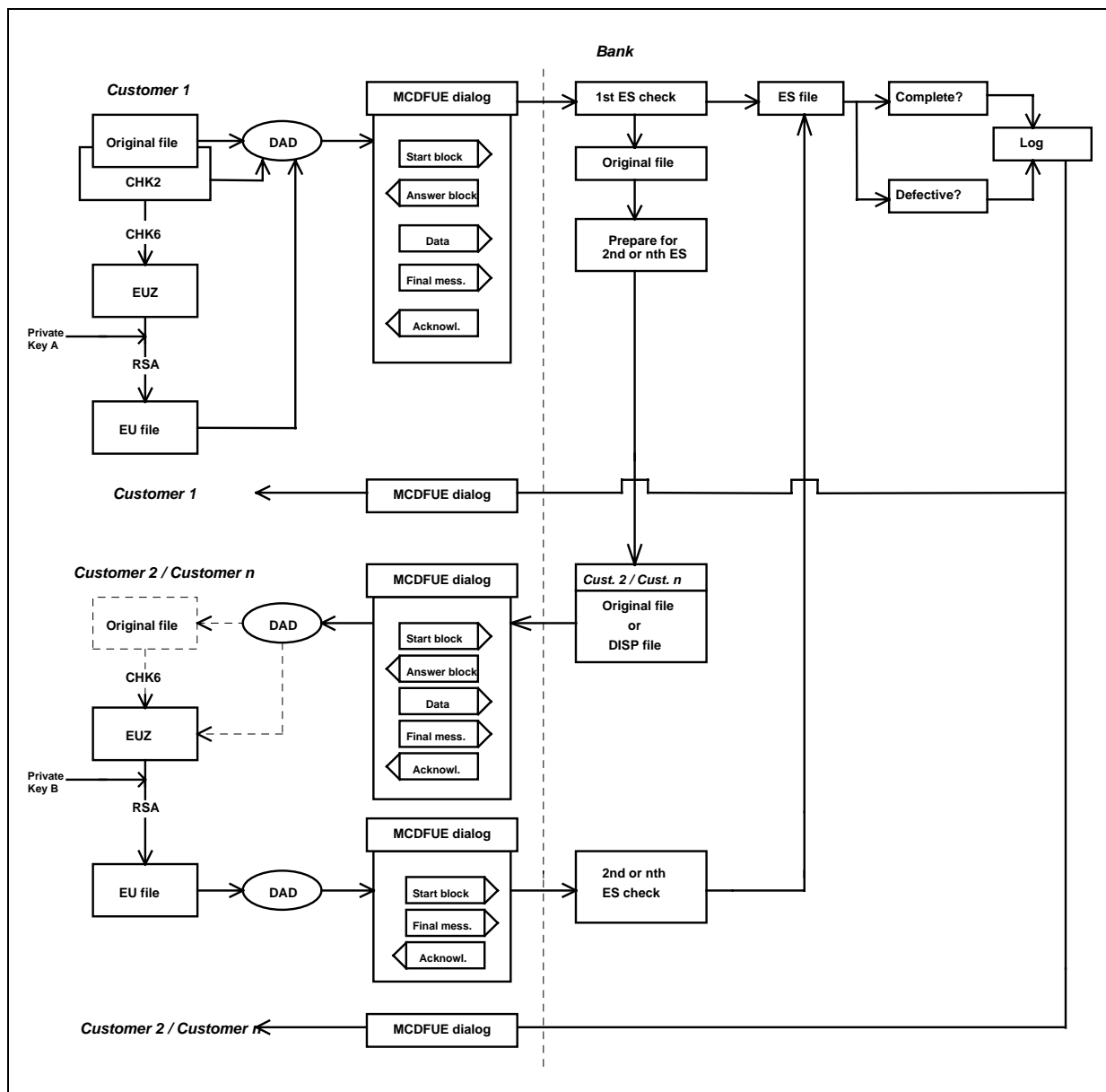
Electronic Signature (ES) with MCFT



CHK2 = Checksum 2
 CHK6 = Checksum 6
 DAD = Comms. order
 EUZ = ES Intermediate File
 RSA = Rivest, Shamir, Adleman encryption method

The hash value is formed using the original file. This hash value is added to the EUZ file (ES Intermediate File) together with the date and time of the original file hash generation, the name of the original file, etc. The EUZ file is "signed" using the private key and the result of this "signature" is added to the ES file, together with the name of the signatory, the date and time of signature, the ES type and version used, as well as other information.

Distributed Electronic Signature (ES) with MCFT



CHK2 = Checksum 2
 CHK6 = Checksum 6
 DAD = Comms. order
 EUZ = ES Intermediate File
 RSA = Rivest, Shamir, Adleman encryption method
 DISP file = Files displaying key compressed data of one or more orders (DISP = DISPLAY)

In addition to the method described above, it is also possible to use MCFT for "**Distributed Signatures**". This concept allows authorised signatories to sign original files saved on the bank computer from different locations. The "Distributed Signature" method thus allows signature hierarchies in internationally operating companies to be reproduced, i.e. the target group for the use of "Distributed Signatures" is corporate customers with a hierarchical corporate structure spread across a variety of geographical locations (groups of companies, branch networks).

System	Activity
Cust. computer 1	<ul style="list-style-type: none"> • Creation of Payment file • First signature • Transmission to bank
Bank system	<ul style="list-style-type: none"> • Verification of <ul style="list-style-type: none"> ♦ Access authorisation ♦ Transmission permission ♦ Signature ♦ Sufficient number of signatures • Online acknowledgement <ul style="list-style-type: none"> ♦ Payment rejected or ♦ Payment accepted or ♦ Forwarded for second signature • Prepare file for second or nth signature
Cust. computer 2 / n.	<ul style="list-style-type: none"> • Get payments for second or nth signature • Second or nth signature • Transmission to bank
Bank system	<ul style="list-style-type: none"> • Verification of <ul style="list-style-type: none"> ♦ Access authorisation ♦ Transmission permission ♦ Signature ♦ Sufficient number of signatures • Online acknowledgement <ul style="list-style-type: none"> ♦ Payment rejected or ♦ Payment accepted • Prepare logs for first signatory <ul style="list-style-type: none"> ♦ Payment rejected ♦ Payment accepted <ul style="list-style-type: none"> ♦ (File deleted after x days due to lack of second signature)
Cust. computer 1	<ul style="list-style-type: none"> • Get log

1.2.3 FTAM

FTAM is the abbreviation for "File Transfer Access Method" and describes a standard method of data interchange. The following extract of the ZKA features table shows which requirements have been implemented.

	FTAM
Feature	Combination of standard processes
Verification of error-free data transmission	only with ES
Compression	FLAM (optional)
Encryption	DES/RSA hybrid method (optional)
Format validation (syntactic check)	after transmission
Pre-Authorization check	no
Notification of validation results	later Validation results in log file
Authorization/ Protection against manipulation	RSA ES 1024 bit RipeMD-160 separate files offline validation
ES	yes (optional)
Distributed ES	no
Communication media	X.25 ISDN
Application	Electronic Banking Germany

As the standard processes described here (FTAM, FLAM [= Abbreviation for Frankenstein-Lidzba Access Method], ES) have been combined, no dialog (such as used with EPFT/MCFT) is possible. In particular, the ES cannot be verified online.

The FTAM data transmission process currently implemented is a national standard.

The characteristic feature of FTAM transmission is that the data is currently not exchanged in encrypted form and compression is optional, i.e. data interchange is transparent. An Electronic Signature is vital to secure the transmitted data.

A component of the files transmitted using FTAM is an internal program name (= OSI FTAM name). The bank and the customer system use the structure of this file name to identify the communicating parties and the file type. The internal file name is generated for each file.

The general convention for this internal file name is:

An.kkkkkkkk.aaa.dddNN.Annn{.pppp}

Example of a compressed and encrypted "From/To" STA session:

A3.KUNDE1.STA.DFHNN.A001.V990814.B990815.H1A2B3C4E5112BCDEA7C81A2AB2782C

Example of a VPK session with Electronic Signature:

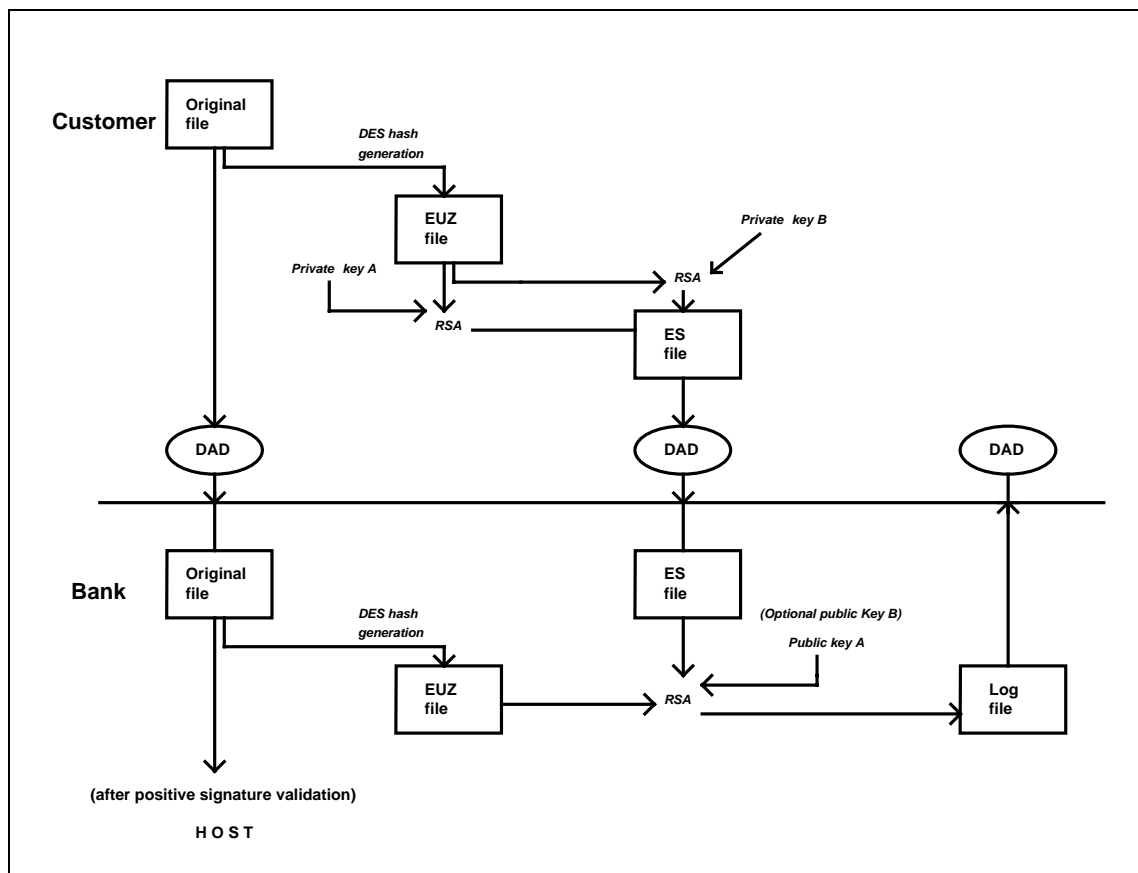
A3.KUNDE1.VPK.BNNNN.A001.UUSER1

A total of three transmission sessions are required to transmit payment orders from the customer computer to the bank system, as the original file and the signature file are sent separately to the bank. The ES file associated with the original file is verified for accuracy and completeness on the bank computer. The result of the validation is saved in a log file which must be downloaded by the customer from the bank in a separate (= third) Comms. session. Only when the log (ES log) containing a positive confirmation has been received can the customer be sure that his payment order has also been executed. In the event of defective or incomplete signatures, the ES log contains appropriate messages.

For the meaning of specific return codes, which describe the status and/or the result of the Comms., see Chapter 5.4: *Return codes*).

To generate the Electronic Signature (ES) on the customer computer, you can use one of the various ES types (ARL, SNI, Concord-Eracom, Omikron). In contrast to MCFT, the individual ES types are available in versions A002, A003 and A004. The version determines the method for calculating the hash value for the ES. The bank computer must be able to verify Electronic Signatures generated in all versions using all ES types and transmitting using FTAM.

Generation and verification of the "Electronic Signature" (ES) for FTAM transmissions



Encryption of files sent using FTAM

The main focus of the encryption concept (cf. Chapter 4.5: *Encryption for FTAM/FTP transmissions*) is the exchange of public keys generated on the customer and the bank computer. The private keys of the keypair remaining on the customer and bank computer are used to decrypt the messages encrypted by the other communicating party using the public key.

Two session types will be used for the transfer of public keys from the bank to the customer and from the customer to the bank:

VPB	Collect Encryption Public key from Bank
VPK	Send Encryption Public key (Customer)

These two (administration) session types will be executed using an appropriate wizard (see Chapter 4.5.1: *Activate encryption with banks*).

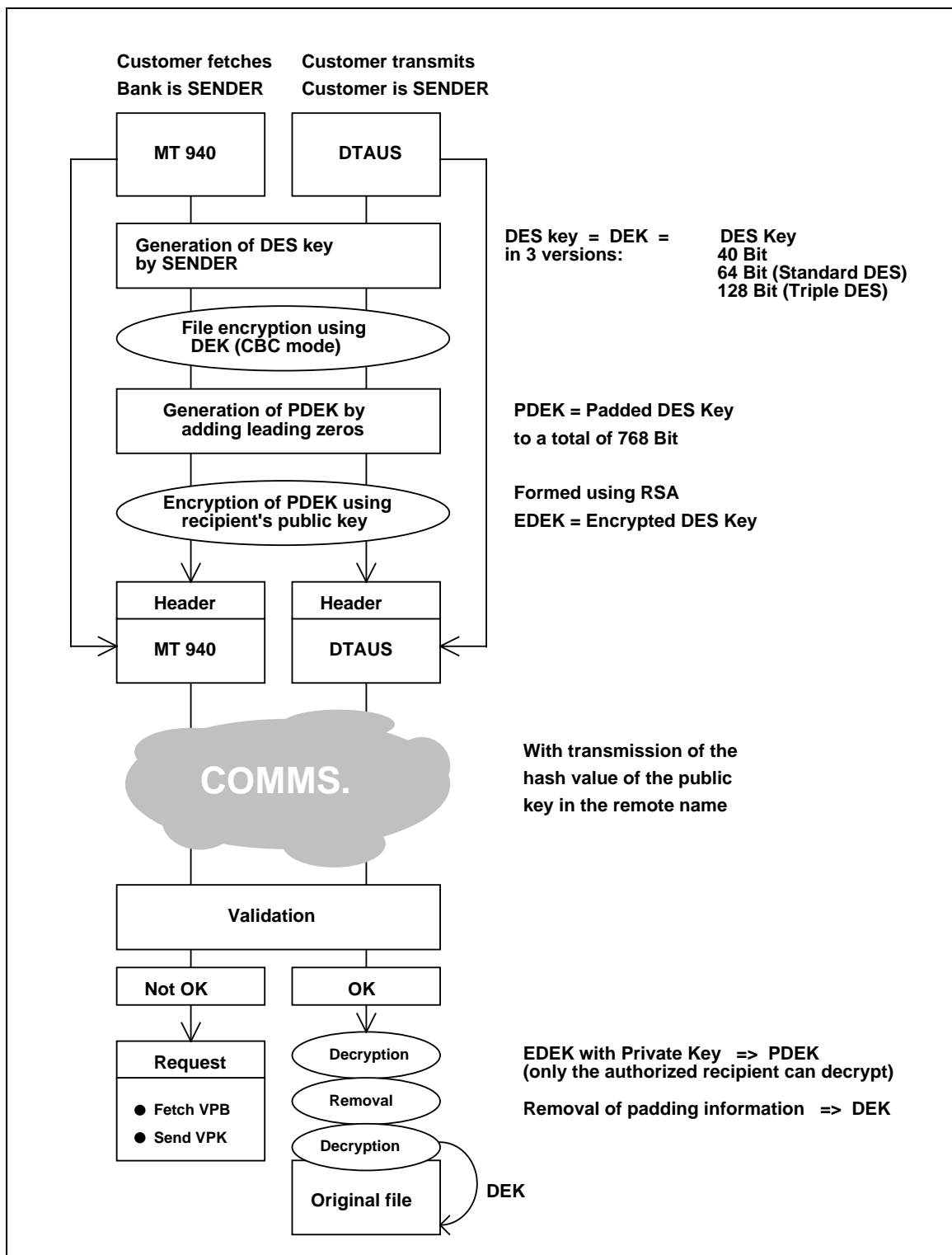
Encryption of the files to be transmitted using FTAM therefore uses a

- **Bank-specific keypair**
(for encryption of the data to be transmitted)
 - ♦ Generation of a keypair on the bank computer
(can be repeated as often as required)
 - ♦ Downloading of the **public key** by the customer
(session type **VPB**)
 - ♦ If the public key is no longer valid,
the bank sends a message and automatically initiates a new customer VPB sessionand a
- **Customer-specific keypair**
(based on the customer ID; saved on the customer's hard disk)
 - ♦ Generation of a keypair on the customer computer
(can be repeated as often as required)
 - ♦ Transmission of the **public key** to all (encrypting) banks (session type **VPK**)

You can find the respective return codes on encryption in Chapter 4.5.2: *Encryption return codes*.

The steps before and after transmission of the encrypted data using FTAM are illustrated in the diagram below:

Transmission of encrypted data using FTAM



1.2.4 FTP

FTP is the abbreviation of "File Transfer Protocol" and describes the standard method for exchanging data using TCP/IP. The following features table shows which requirements have been implemented.

	FTP
Feature	Combination of standard procedures
Verification of error-free data transmission	yes
Compression	FLAM (optional)
Encryption	DES/RSA hybrid method
Format validation (syntactic check)	after transmission
Pre-Authorization check	optional
Notification of validation results	immediate or later (validation results in log file)
Authorization/ Protection against manipulation	RSA ES 1024 bit RipeMD-160 optional: pre-validation (online) detailed offline validation
ES	yes (optional)
Distributed ES	yes
Communication media	TCP/IP (Internet)
Application	Electronic Banking

An (internal) file name is defined for processing an FTP session, which both the bank and the customer system uses to identify the communication partner and the file type. This file name is generated for each file.

The general convention for this internal file name is:

B1.kkkkkkkk.aaa.dddNN.Annn

Key:

B1	Version number of the application protocol
kkkkkkkk	Customer ID (8 alphanumeric characters)
aaa	Session type (3 alphanumeric characters) e. g. IZV, AZV, ...
dddNN	Session attribute (5 alphanumeric characters)
character 1 :	File type: D File without signature O Original file for which a signature file is required I Info file for D or O S Info file with ES for O
character 2 :	Compression type:

	N	No compression
	F	with FLAM compression
	X	Xpress compression (planned)
character 3 :	N	No encryption
	H	with Encryption (DES hybrid method)
character 4 :	N	Reserved for future use
character 5 :	N	Reserved for future use

Annn Session number (4 alphanumeric characters)

character 1 :	A
character 2 :	Customer identification in the network starting with A
character 3 and	
character 4 :	Sequential character (per character 0 - 9, A - Z)

An FTP Comms. session consists of at least two, but normally three file types:

- the logon file for user validation/logon
- the information file for specifying the session, optionally with ES
- the user data file (not needed if only the ES is being transmitted)

A total of three transmission sessions are required to transmit payment orders from the customer computer to the bank system. Firstly for the logon file, then for the information file, and finally for the original file (user data file). The ES file associated with the original file is verified for accuracy and completeness on the bank computer. The result of the validation is saved in a log file which must be downloaded by the customer from the bank in a separate Comms. session. Only when the log (ES log) containing a positive confirmation has been received can the customer be sure that his payment order has also been executed. In the event of defective or incomplete signatures, the ES log contains appropriate messages.

For the meaning of specific return codes, which describe the status and/or the result of the Comms., see Chapter 5.4: *Return codes*).

To generate the Electronic Signature (ES) on the customer computer, you can use one of the various ES types (ARL, SNI, Concord-Eracom, Omikron). The version determines the method for calculating the hash value for the ES.

The workflow for the preparatory and subsequent steps for transmitting encrypted data using FTP is the same as that for sending encrypted data using FTAM (see Chapter 1.2.3: *FTAM*). Also in this case the encryption (cf. Chapter 4.5: *Encryption for FTAM/FTP transmissions*) is made by the exchange of public keys generated in each case on customer and bank side. The two (administration) session types VPB and VPK are executed using an appropriate wizard (see Chapter 4.5.1: *Activate encryption with banks*).

In contrast to FTAM, however, data is **generally transmitted in encrypted form** if FTP is used. The only exception is the collection of the encryption public key of the bank (VPB) by the customer, which is necessary for the encryption of the files to be transferred. Afterwards all files of the customer and the bank are transmitted only in encrypted form.

You can find the respective return codes on encryption in Chapter 4.5.2: *Encryption return codes*.

In addition, it is possible to make a **Distributed Signature (DS)** with FTP. The concept of a "Distributed Signature" is that the authorized signatories may sign the original files stored on the bank server from separate locations (see Chapter 1.2.2: *MCFT*).

The procedure of Distributed Signature can therefore be made to match the signature hierarchies within international companies, i.e. the target group for the implementation of Distributed Signature is corporates with a multi-layer, multi-regional structure (Corporate Groups, branch outlets).

Distributed Signature using the FTP-Process:

1. Customers who are set up on the bank server for Distributed Signature can initialize the signature by sending an original file to the bank without all necessary signatures. In addition to the original file, the customer attaches a second file informing the bank which other customers must provide a signature for this order. An additional option is provided by a list on the bank side containing the names of authorized parties for second signature. If the customer does not supply the names of signatories in a specific order, the files will be routed to the named parties from this central list.
2. The bank prepares the signature data in the form of ESG-files (**E**lectronic **S**ignature **G**et) for collection by the customers as defined by the customer initiating the Distributed Signature. The signature data consist of a hash calculated either over the display file or the entire original file. These data are, however, only prepared by the bank for the customers to collect if the electronic signature of the first customer has been successfully validated. If the bank has several orders to be signed by one specific customer, the ESG file will be appended, i.e. the ESG file will in this case contain several orders pending signature.
3. The ESG-file is collected by a user who is authorized for the session type "ESG". If necessary, the ESG file collected from the bank is split into individual orders on the customer side and these can be viewed in the File Manager.
4. The process is completed when another electronic signature from an authorized user has been made and sent.
5. Steps 3 and 4 must be repeated until the bank has sufficient signatures from authorized parties for the original file in question.

The original file is always sent by the customer initializing electronic signature, as this is the only way in which the content of the original file can be validated. Since the user initiating the process does not have to be an authorized signatory (set up as Single, First or Second signatory on the bank server), a special signature class is available. This signature class "T" is used only for securing the transport of the original file. With Electronic Signatures of class "T", various validation checks are not made, including the ES check, a check against double sending of the orders and check for account authorization and limits.

1.2.5 EBICS

The internet-based Comms. procedure EBICS (**E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard) has been defined on behalf of the German Central Credit Committee (ZKA), a consortium of all top organizations of the German banking industry, and will replace the Communication protocol FTAM used for the corporate banking of banks. The support of the "Distributed Electronic Signature", enabling a shared authorization of payments from different locations, as well as the always cryptographically secured transmission of data between customer and bank must be considered to be the most important enhancement in comparison to FTAM. Due to its high performance, the EBICS procedure is especially suitable for the transmission of mass order payments.

The first common initiative of the German and French bank associations, the new EBICS version 2.4 will be supported by banks in both countries from autumn 2009.
For France, there are only minimal adaptations to the existing handling (replacement of ETEBAC-3). In the first phase, e.g. only transport signatures, but no personal electronic signatures are supported for payment authorization. Special order types allow the upload (FUL: **F**ile **U**pload) and download (FDL: **F**ile **D**ownload) of files with associated file type attributes for general and bank-specific formats.
For Germany, the decisive factor for this upgrade is the enhanced security in the support of longer signature keys (new EBICS protocol version H003 with ES versions A005 and A006 [existing side by side]). If new keys are generated, new EBICS keys of the versions X002 and E002 are also generated.

With EBICS version 2.5 the protocol H004 is supported. After switching to this protocol version the session numbers for transmit sessions are no longer generated by the client system, but by the bank server.

With EBICS 2.5 -as alternative to the well-known session type PTK- a customer log file in XML format can be retrieved using session type HAC. This is also correlated with the appropriate file manager entry and is being prepared for display analog PTK.

The following feature table shows which requirements are realized.

	EBICS
Feature	Internet
Check on correct data transmission	yes
Compression	yes (ZIP procedure)
Encryption	TLS (SSL) and DES/RSA-Hybrid procedure
Format validation (syntactic check)	after transmission
Pre-Authorization check	optional
Notification of check results	later in the log
Authorization / Manipulation protection	RSA signature 1024 Bit (from 2.4: 1536-4096 bit, Default: 2048 bit) RipeMD-160 (from 2.4: SHA: 256) optional: pre-validation (online) detailed offline validation
ES	yes
Distributed ES	yes
Communication media	TCP / IP (Internet)
Application area	Electronic Banking Germany

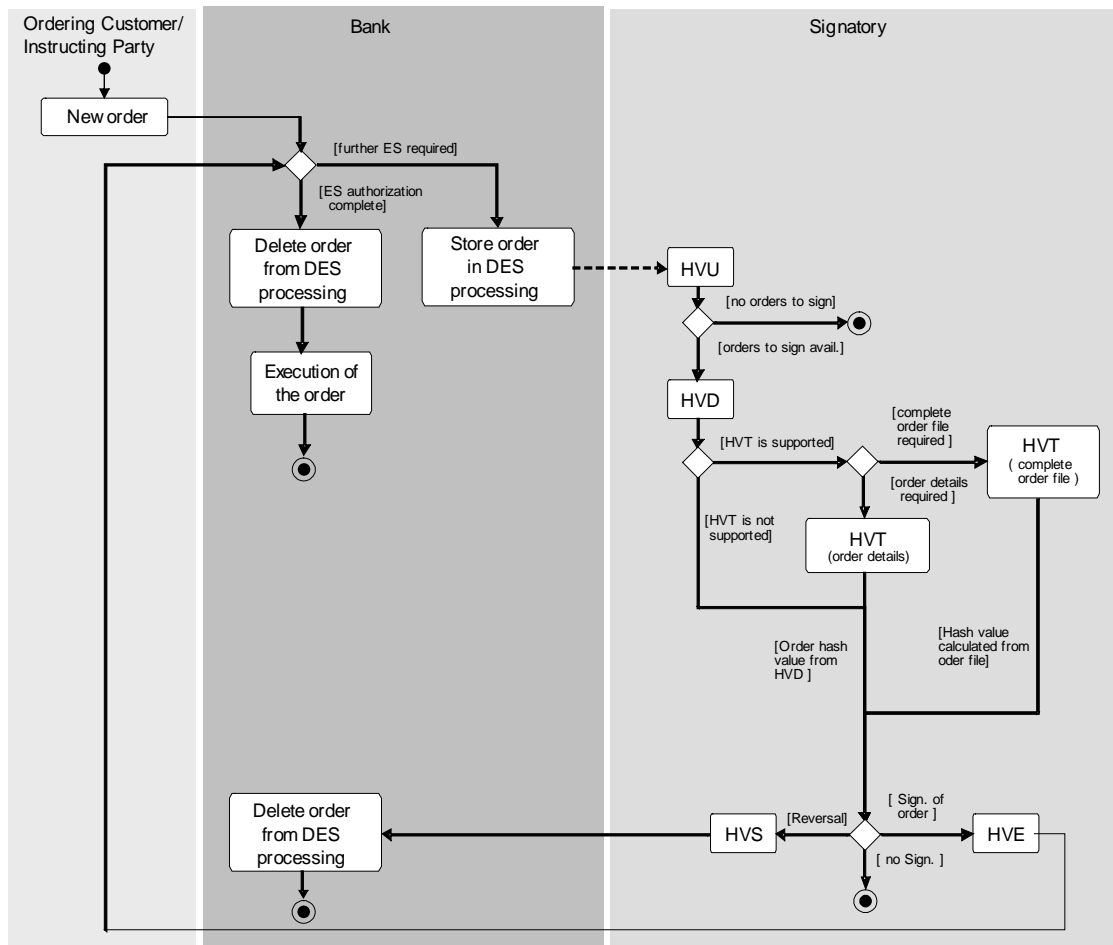
The features in detail:

- EBICS is IP-compatible and uses the Internet transport protocol HTTPS for the data transmission, ensuring a secure transmission using the TLS (SSL) transport encryption. The application data embedded in a XML container is transferred block by block, whereas each block is secured using an authentication signature (Authentication key starting from version X001). If not all blocks are transferred successfully, a recovery function enables to begin again with the last successfully transferred block.
- In addition to the transport encryption, it is ensured due to the integrated encryption (Encryption key starting from version E001) according to the BCS hybrid procedure that the application data is always transferred in encrypted form (thus double encryption).
- To ensure the authenticity of the files to be transferred, they have to be always authorized by the user using the Electronic Signature (ES) (Signature key starting from version A004).
- For an efficient transmission, the data is always compressed using a ZIP algorithm.
- EBICS supports in addition the use of the Distributed Electronic Signature, which enables companies to authorize payment orders from different locations.

In Chapter 3.5: *EBICS* you can find information on the required settings in the corresponding bank parameter file.

The functionality of the Distributed Electronic Signature (DES) means, that signatures of customer systems in separate locations can only be made by the communication with the respective bank system. This can be configured on the bank system for each customer.

The Distributed Electronic Signature allows to authorize orders from several users – also cross-customer like -, irrespective of location and time. An underlying order remains here saved in the DES processing until either the required number of signatures (having the adequate authorization) for the DES orders is received, a bank-server time limit has been exceeded or a cancellation of the order occurred.

Workflow diagram of the Distributed Electronic Signature for EBICS:

One user triggers the DES processing by remitting an order with an insufficient number of bank-specific signatures having the required authorization classes. It is mandatorily required that this order is remitted signed (either with bank-specific signature of the classes "A", "B" or "E" or with transport signature = signature class "T").

The bank system verifies first the delivered ES(s) and the authorization of the user for the given session type. Then it reconciles the number and signature classes of the delivered ES(s) with the locally stored ES requirements for the given session type. In the case that signatures are still pending, the order with the already transmitted ESs is added to the DES processing and thus is stored for authorized customers to accomplish DES.

The following session types are supported:

The individual EBICS Requests are summarized on the applicational level and will be processed with the session types well known for the Distributed Signature:

ESG (Electronic Signature Get); this session type encapsulates the two following EBICS-Requests:

- HVU (Collect DES overview)
- HVD (Retrieve DES status)

ESP (Electronic Signature Put); this session type encapsulates the following EBICS-Requests:

- HVT (Retrieve DES transaction details)
- several HVE (Add DES signature)
- HVS (DES cancellation)

The user collects in the first step an overview, for which orders he is authorized to sign with DES, from the bank (session type HVU). In a second step, then the status is retrieved for each order (session type

HVD). In essence the retrieved information contains the hash value of the original order, the cover note as well as the users who have already made signatures for this order. These two steps are encapsulated in the program so that the user does not have to start the HVD request manually after the HVU request for each individual order.

After the request the individual orders are added to the file manager with the status "Waits for ES". In addition, for identifying DES orders, a new ID-Group ("VEU" = german abbreviation for DES) is allocated for these orders.

For a HVU/HVD request, the program proceeds as follows with DES orders already available in the file manager:

1. DES order has not yet been processed (no user has accomplished a signature; Status = "Waits for ES")

These orders are overwritten in the file manager. If such orders are still pending on bank side, the HVU/HVD request provides the corresponding information again. The overwriting avoids that for an identical DES order several entries are generated in the file manager.

2. DES order is in processing, but not yet completely terminated (user has accomplished signature, but has denied the prompt for signature completeness; Status = "Waits for ES")

Such orders remain in the file manager and are not overwritten, since these are not yet terminated. No further entry is generated for this order in the file manager. New information from the HVD request (e.g. list of the signatures already made for this order) is added to the existing entry.

3. DES order is in processing, but not yet completely terminated (user has accomplished signature, but not yet transferred it to the bank; Status = "Waits for Comms.")

Such orders remain in the file manager and are not overwritten, since these are not yet terminated. No further entry is generated for this order in the file manager. New information from the HVD request is added to the existing entry. The status is not changed, since the signature already made, but not yet sent can be the last required one. The user can thus send immediately his accomplished ES.

4. DES order is in processing, but not yet completely terminated (user has accomplished signature and transferred it to the bank, but not yet collected the log with final ES check; Status = "OK")

Such orders remain in the file manager, since these are not yet terminated. New information from the HVD request is added to the existing entry. In this case, the status of the order is reset to "Waits for ES" in order that further users can add signatures.

5. DES order is completely terminated (user has accomplished signature and transferred it to the bank; log with final ES check has been collected). The status is set to "ES check OK".

If a log request for a pending DES order is made, the status is set as follows:

If the order is still pending on bank side, no status change is made.

If the order has been successfully processed in the meantime on bank side because another user has signed it, the status is set to "ES check OK".

Such orders remain in the file manager as audit trail for the order execution.

The information from the customer log (result of the signature check) is allocated to the orders in the file manager. For the identification of the order, the Customer ID, the User ID and the order numbers (order number remittance original file, order number of the order for making a further signature using HVE) are used for this.

For the HVT request, a limit can be included for the file size for collecting the original file on the bank server.

1.2.6 HBCI/HBCI+

The HBCI method (= Homebanking Computer Interface) should replace BTX. Using modern cryptographic functions and smart cards, HBCI - adopted the first time in the version 1.0 in 1996 by the Central Credit Committee of the German credit and finance (ZKA)- provides a secure communication in open networks (e.g. internet).

Meanwhile (2003) with the HBCI version 3.0 the spreading standard FinTS (Financial Transaction Services) was created, which contains on the one hand HBCI 3.0 and on the other hand PIN/TAN as alternative safety procedure.

The HBCI+ procedure is based on the HBCI standard, but the protection against manipulation is ensured through PIN and TAN. In relation to VTX banking (German BTX) however up-to-date functions like e.g. the European Union standard transfer are available. The procedure is location independent in relation to the procedure with smart card.

The following table shows which requirements have been implemented for the two versions of HBCI.

Feature	HBCI	HBCI+
	HBCI with Chip card/Diskette	also known as HBCI Plus, HBCI with PIN /TAN or PIN/TAN extended
Verification of error-free data transmission	TCP/IP	TCP/IP
Compression	yes	yes
Encryption	yes	yes 128 bit SSL (Browser)
Validation (syntactic check)	no	no
Authorisation/ Protection against manipulation	ES RipeMD / RSA	PIN / TAN
Distributed ES	no	no
Communication media	TCP/IP (Internet)	TCP/IP (Internet)
Application	Home Banking	Home Banking

1.2.7 ETEBAC

ETEBAC (=Echange télématique entre banques et clients) is the Comms method used by French banks. ETEBAC is a national standard defined by the AFB (*Association Française de Banques*) – the Association of French Banks.

There are two different versions of ETEBAC: ETEBAC3 and ETEBAC5. An appropriate supplementary module has to be installed for each version. Please contact the customer services department at your French bank should you wish to exchange data with French banks using this method.

A detailed description on how to use the ETEBAC3 module can be found in Chapter 3.8: *ETEBAC3*

Table of Contents: Chapter 2

	Page
2 Communications menu.....	2-2
2.1 Comms. parameters	2-3
2.2 Modem PAD access property page	2-4
2.3 X.25 - leased line property page.....	2-7
2.4 Modem-Modem property page (direct connection)	2-10
2.5 ISDN CAPI property page.....	2-12
2.6 TCP/IP connection property page.....	2-13
2.7 Priorities property page (Comms. procedures).....	2-15
2.8 AT Commands	2-17

2 Communication menu

The Communication menu contains all the menu items relating to the communication between the customer and the bank system, i.e. data transmission.

The -Communication- menu contains the following menu items:

- **File Manager**
Information on the File Manager is contained in Chapter 5.1: *File Manager*.
- **Execute Comms favourite**
Information on the execution of preferred bank connections is contained in Chapter 5.1.1: *Database overview: File Manager*.
- **Assistant for collecting data from several banks**
- **Monthly statistics (additional module)**

- **Comms. parameters**
You cannot upload or download files unless the Comms. parameters have been properly configured. The Comms. parameters define the settings to be used for each Comms. facility (e.g. ISDN or X.25).
- **Bank parameter files**
A BPD (Bank Parameter Data file) describes access to a bank. You need a separate BPD for each bank. The BPD contains the access data for the bank as well as the NUA (Network User Address = "data communication telephone no." with which you can reach the bank). When a Comms. session is generated, the bank is always selected in the form of a Bank Parameter Data file.

- **First initialization (INI)**
- **Generate / Send ES key pair**
- **Change ES password**
- **Change Comms Password**
- **Change EBICS Comms. password**
- **Key media administration**
- **Manage certificates (additional module)**

- **Convert FTAM/FTP bank access to EBICS**
- **Change EBICS authentication keys**
- **Reset EPFT/MCFT communication access**
- **FTAM/FTP encryption**
This menu item is only available if you have installed FTAM or FTP.
Further information on the subject of encryption is contained in Chapter 4.5: *Encryption*.
- **Block Comms. access**

2.1 Comms. parameters

To be able to transmit and download data properly, a number of Comms. parameters related to the Comms. method must be defined. You need only configure the Comms. methods you are using by adapting the corresponding Comms. parameters.



Please have the necessary documentation at hand (modem manuals, passwords, IDs/codes, etc.) when you configure the Comms. parameters. If you need help, please contact your bank's Customer Service Department.

The following Comms. methods are currently supported:

- Modem PAD access
- X.25 leased line
- Modem-Modem direct connection
- ISDN CAPI
- TCP/IP connection (Internet)

Click on the corresponding tab to select the property page. The dialog boxes contain the default values for this data transmission method.

Once you have selected the communication method and configured any Comms. parameters, use the *Priorities property page* to tell the program the sequence of Comms. methods it should use.

Local Comms. information is specified in the Comms. parameters. Since for the data transmission special hardware need to be addressed, these settings are administered for each computer in the network. If several computers should communicate with the banks, the Comms. parameters have to be maintained on each computer. Only computers with defined Comms. parameters are offered for Comms. in the application.

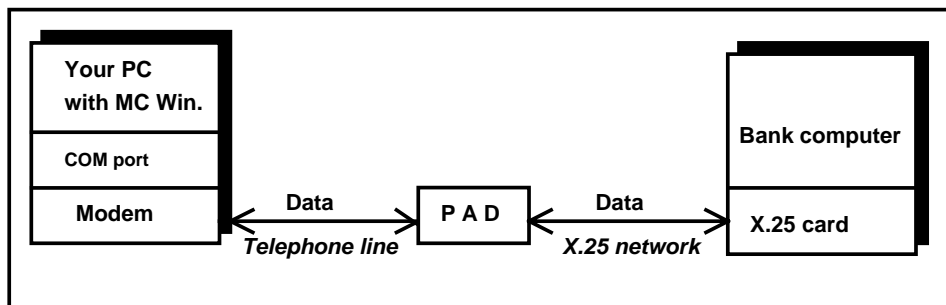
An exception is the TCP/IP protocol, which usually establishes the connection using the standard network card. Therefore it can be defined for this on the *Priorities property page*, that the TCP/IP parameters should be valid globally. In this case TCP/IP must only be activated on any computer once and also the proxy parameters need to be entered only once. They are then used by all computers in the network.

Confirm your entries with [**Save**].

2.2 Modem PAD access property page

To use this communication method, you need a free COM port and an external modem or an integrated modem card, plus a telephone line. The communication between a customer and its various banks takes place only via one PAD (= "**P**acket **A**ssembly/**D**isasassembly" = description of any device that combines incoming messages into a single message or extracts individual messages from data sent in a single transmission sequence).

The communication process is illustrated in the diagram below:



The text boxes in the dialog box contain the standard settings for data transmission using a standard modem. Use the blank boxes to enter the values applying to your modem.

If you are not using a standard modem, the settings must be adapted to the modem you are using. You can read about this in the instruction manual for your modem.

The following text boxes are available:

Modem type

Choose the modem from the list of modems that are installed on your computer via the Windows Control panel (settings will be re-used) or select "Individual settings".

PAD Access

Select your country- or bank-specific PAD access you wish to use from the list of possible PAD accesses.

The screenshot shows the 'Comms. parameters' dialog box with the 'Modem PAD access' tab selected. The 'Modem type' dropdown is set to 'Individual settings'. The 'PAD access' dropdown is set to 'Germany (DATEX-P)'. The 'ID' field is empty, 'Password' is empty, 'No.' is '19553', and 'Alternative no.' is empty. The 'Serial port' is 'COM1', 'Baud rate' is '9600', 'Parity' is 'None', and 'Bits' is '8 Bits'. The 'Initialisation string' is 'AT&C1&D2!~'. The 'Dial command' is 'ATDT' and the 'Hang-up command' is '+++~ATH0'. The 'Disconnect modem' checkbox is unchecked. The 'Dialling' section has 'Tone' selected. The 'Telephone link' section has 'Main line' selected and 'Line ID' is '0'. 'Help' and 'Save' buttons are at the bottom right.

ID**Password**

These two boxes are for the PSN ID and password. The password is concealed on entry. Each character is represented by an asterisk (*).

The PSN ID and password are notified by your local network provider.

No.

To configure automatic dialling of the nearest PSN node, enter the corresponding information in the "Number" box.

Alternative No.

In addition to the primary PAD number (PSN node number), you can also enter a second number in the box "Alternative No." This number will be dialled if your normal PAD is busy.

Port

Choose between serial ports COM1, COM2, ..., COM8 for the PC/modem port.

Baud rate

The Baud rate is the speed at which data can be transmitted. Of course, the baud rate also depends on the performance of your modem. The standard setting is "2400", but you can also set a Baud rate of between "300" and "64000".

Parity

The parity check refers to the requirements of the PAD. Set the parity check to either

- even or
- none (no parity)

Bits

This entry defines whether transfer will be in 7-bit or 8-bit mode. The definition depends on the requirements of the PAD.

Initialisation string

Certain commands are needed to initialise the modem. These commands normally form part of the **AT instruction set**, which has become a de-facto standard. However, the modems available on the market differ in the way they handle this instruction set and the number of instructions they use. In some modems, all AT commands have to be entered in CAPITALS. You will find further information on this topic in Chapter 2.8: *AT Commands*

Dial command

To configure automatic dialling of the nearest PSN node, enter the corresponding information in the "Dial command" box.

The **Dial command** will be set automatically in accordance with your entries.

Structure of the dial string: **ATDabb**

Replace the digits as follows:

- a** = "T" for Tone dial access lines
"P" for Pulse dial access lines
- b** = Outside line.
In PBXs, the outside line may be accessed from the extension with "0W", with "0" standing for the number used by the telephone to access an outside line. "W" tells the modem to Wait until the outside line has been established.

For further information on the AT instruction set please refer to Chapter 2.8: *AT Commands*

Hang up command

Enter in this box the command to be used to disconnect the link between your modem and the PAD.

Disconnect modem

This box is normally clear.

If you leave the box clear, the PAD link will not be disconnected when all Comms. sessions have been processed. Once a Comms. session has been processed, and a connection to another bank is required, it simply disconnects from the current bank and immediately establishes a connection with the next bank. This saves having to redial and saves costs.

If you check this box, however, the modem will automatically disconnect after **each** data transmission, so that if you need to process further Comms. sessions, a connection to the PAD must be re-established before connecting to the bank.

This expensive procedure may be necessary depending on the PAD you are using.

Dialling

Here you can choose whether your modem supports tone ore pulse dialling.

Telephone link

Here you can define, whether the telephone link used by you is a main line or a sub line. If necessary you can enter a Line ID in the corresponding field.

If you make any subsequent manual changes, the "Dial command" box is updated accordingly.

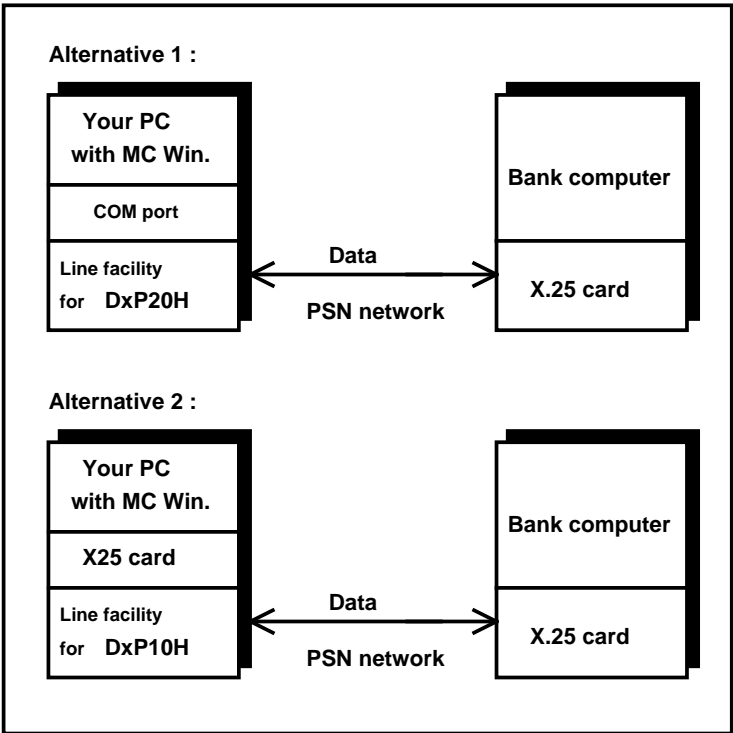
Select	Field Dial command	Additional entry Dial command
Tone	ATDT	-
Pulse	ATDP	-
Primary line	-	-
Extension	-	0W
Outside line (x)	-	(x)W

2.3 X.25 - leased line property page

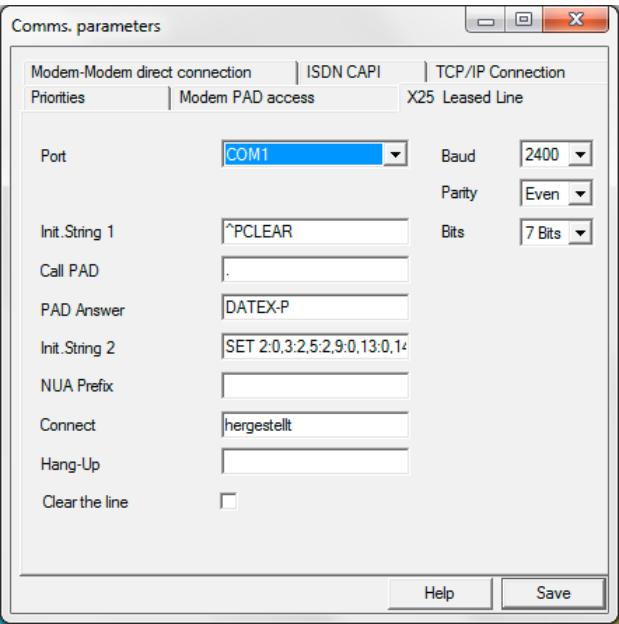
To use this communication method, your will need

- either** a free COM port and a Datex-P20 data link (asynchronous dial-up data link) with corresponding line circuit facilities
- or** an X.25 card and a Datex-P10 data link (synchronous X.25 data link) with corresponding line circuit facilities.

The communication process is illustrated in the diagram below:



The layout of the property page opened depends on the **port** you are using for communications.



X.25

If you have defined "X.25", you must have a Datex-P10 data link (synchronous X.25 data link) and have loaded the card driver **BEFORE** you start Windows. No further configuration is required in this case.

COM1 to COM8

It may be necessary to modify the transmission parameters to suit the installed modem. Please refer to the user manuals of your Comms. facilities for advice on the parameters to be used.

Key to the text boxes in the dialog box:

Baud

The Baud rate is the speed at which data can be transmitted. Of course, the baud rate also depends on the performance of your modem. The standard setting is "2400", but you can also set a Baud rate of between "300" and "64000".

Parity

Set the parity check to either

- even or
- none (no parity)

Bits

This entry defines whether transfer will be in 7-bit or 8-bit mode.

Init. String 1

Inittext 1 depends on the modem you are using. Please refer to the modem documentation for the commands to be entered.

Call PAD

PAD answer

The characters entered in the first box tell the PAD that a transmission will take place. The PAD answers tells the program that a connection has been established. The values to be entered in the "Call PAD" and "PAD answer" boxes depend on the PAD.

When using Deutsche Telekom PADs, the standard Connect message is:

Default for **Call PAD** is a . (point).

Default **PAD answer** (answerback) is "DATEX-P".

Init. String 2

As with Inittext 1, Inittext 2 depends on the modem you are using. Please refer to the modem documentation for the commands to be entered.

NUA prefix

The **NUA** (Network User Address) is the "telephone number" under which special PADs (incl. foreign PADs) can be reached. The PAD provider will tell you which entry to make.

The NUA prefix is **PAD-specific**.

Enter the notified NUA into the text box **WITHOUT** any spaces between the individual characters.



The field must be blank when using Deutsche Telekom PADs.

Connect

Enter the character string to be sent to the remote station when a connection is being established in the "Connect" message box. This tells the remote station that a connection has now been established. The entry in this box is **PAD-specific**.

When using Deutsche Telekom PADs, the standard Connect message is:

"connected".

Hang up

This tells the program the command to be used to disconnect the link between your modem and the PAD.

Clear the line

If you select this box, the modem will automatically disconnect after data transmission has been completed. If not, you must disconnect manually (potentially much later).

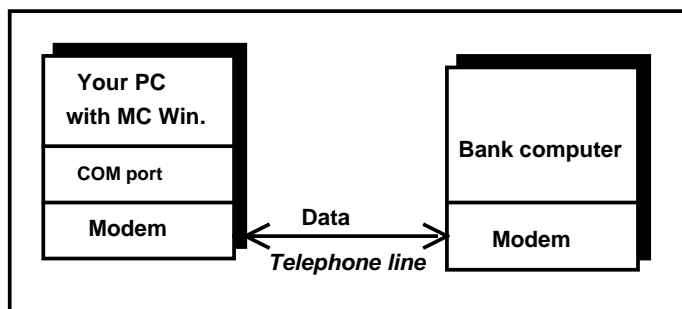
The advantage of checking **-No-** here is that if you are processing session files containing orders for a variety of banks, the link to the PAD is not disconnected.

In such cases, you do not need to redial the PAD before connecting to the new bank when processing further Comms. sessions.

2.4 Modem-Modem property page (direct connection)

To use this communication method, you need a free COM port and an external modem or an integrated modem card, plus a telephone line.

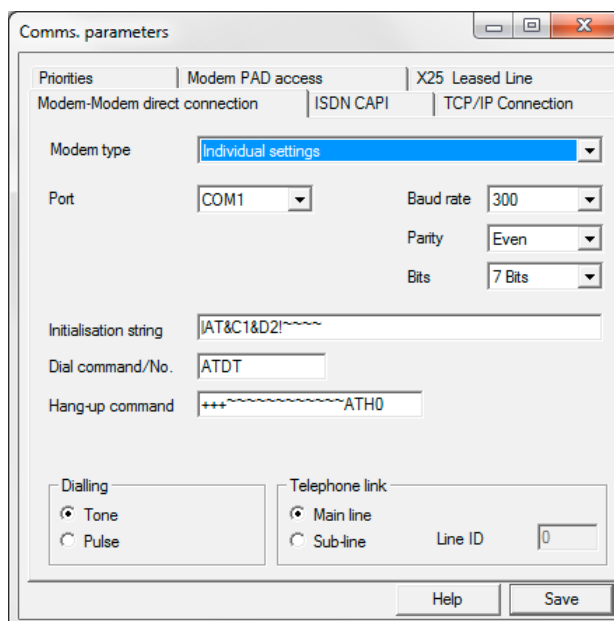
The communication process is illustrated in the diagram below:



You need only enter parameters for a dial-up modem connection if the bank to/from which you are transmitting data can only support "modem <---> modem" communications.

The text boxes in the dialog box contain the standard settings for data transmission using a standard modem. Use the blank boxes to enter the values applying to your modem.

If you are not using a standard modem, the settings must be adapted to the modem you are using. You can read about this in the instruction manual supplied with your modem.



The following text boxes are available:

Modem type

Choose the modem from the list of modems that are installed on your computer via the Windows Control panel (settings will be re-used) or select "Individual settings".

Port

Choose between serial ports COM1, ..., COM8 for the PC/modem port.

Baud rate

The Baud rate is the speed at which data can be transmitted. Of course, the baud rate also depends on the performance of your modem. The standard setting is "2400", but you can also set a Baud rate of between "300" and "64000".

Set the parity check to either

- even or
- none (no parity)

Bits

This entry defines whether transfer will be in 7-bit or 8-bit mode.

Initialisation string

Certain commands are needed to initialise the modem. These commands normally form part of the **AT instruction set**, which has become a de-facto standard. However, the modems available on the market differ in the way they handle this instruction set and the number of instructions they use. In some modems, all the commands have to be entered in CAPITALS only. You will find further information on this topic in Chapter 2.8: *AT Commands*

Dial command

To configure automatic dialling of the nearest PSN node, enter the corresponding information in the "Dial command" box.

The **Dial command** will be set automatically in accordance with your entries.

Structure of the dial string: **ATDabb**

Replace the digits as follows:

- a** = "T" for Tone dial access lines
"P" for Pulse dial access lines
- b** = Outside line.
In PBXs, the outside line may be accessed from the extension with "0W", with "0" standing for the number used by the telephone to access an outside line. "W" tells the modem to Wait until the outside line has been established.

For further information on the AT instruction set please refer to Chapter 2.8: *AT Commands*

Hang up command

Enter in this box the command to be used to disconnect the link between your modem and the bank modem.

Dialling

Here you can choose whether your modem supports tone ore pulse dialling.

Telephone link


Here you can define, whether the telephone link used by you is a main line or a sub line. If necessary you can enter a Line ID in the corresponding field.

If you make any subsequent manual changes, the "Dial command" box is updated accordingly.

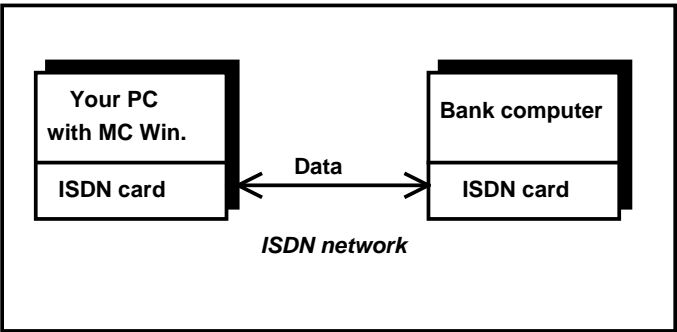
Select	Field Dial command	Additional entry Dial command
Tone	ATDT	-
Pulse	ATDP	-
Primary line	-	-
Extension	-	0W
Outside line (x)	-	(x)W

2.5 ISDN CAPI property page

To use Comms. method, you need an ISDN card and an ISDN line. Your bank must also be capable of receiving and transmitting data using ISDN.

 You must configure your ISDN card as instructed by the manufacturer. Further information is contained in the documentation supplied with the ISDN card. The ISDN card drivers must always be loaded **BEFORE** you start Windows.

The communication process is illustrated in the diagram below:



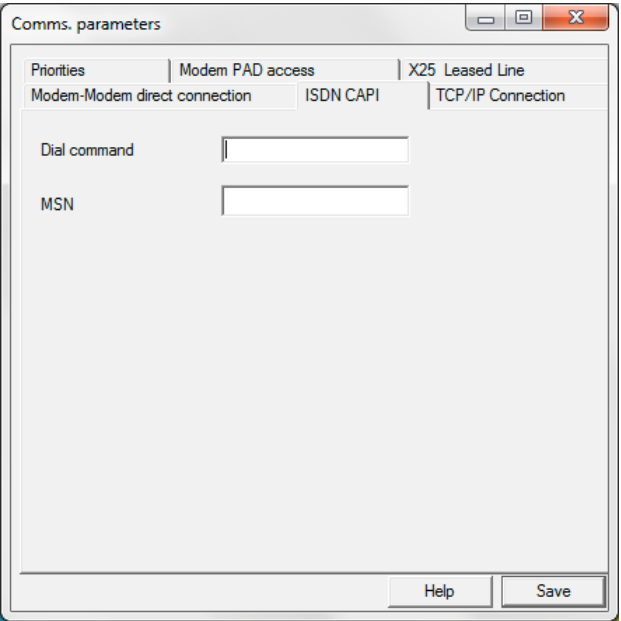
The following parameters are available for ISDN:

Dial command (Outside line)

In PBXs, the outside line may be accessed from the extension with "0", with "0" standing for the number used by the telephone to access an outside line.

MSN (Multiple Subscriber Number with EURO-ISDN)

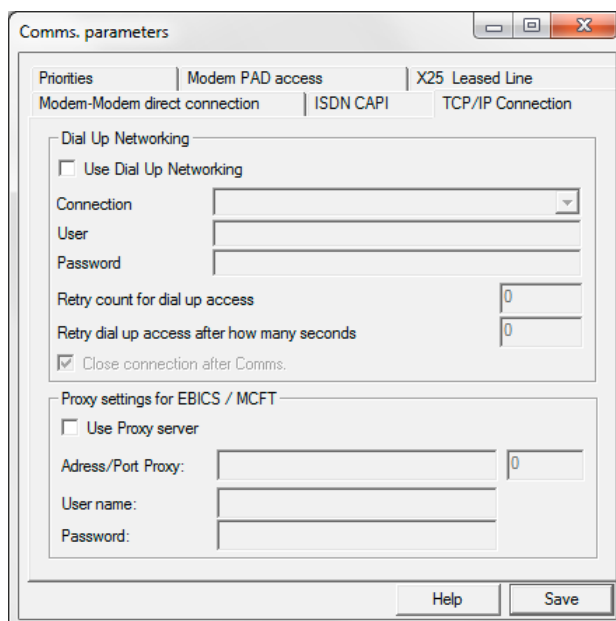
Enter to your multiple subscriber number (up to 6 digits) assigned to your terminal device here.



2.6 TCP/IP connection property page

Check the "TCP/IP connection" box on the *Priorities property page* if your bank offers data communication facilities over the Internet using the EPFT, MCFT, FTP or EBICS Comms. method (cf. Chapter 3.2: *EPFT/MCFT*, 3.4: *FTP* or 3.5: *EBICS*).

To be able to communicate over the Internet, WINSOCK.DLL must be installed on your system. You must also have access to the Internet through a service provider, for instance T-Online, AOL, CompuServe, etc. or a local service provider.



You have two possibilities to communicate via TCP/IP:

1. TCP/IP direct connection over a leased line

If you are using this permanent line there is no need to set any further parameters.

2. TCP/IP dial-up connection via Internet Provider

To use the dial-up connection to your Internet Provider please configure the communications network of Windows first and make necessary adjustments using the specification supplied by your provider.

Comms. network:

If you are successfully connected to the internet via comms. network (**Use dial-up networking**), enter your **connection** as well as **user** and **password** here. Additionally you can set the number of re-diallings aswell as the break in seconds between the repetitions. Further you can determine whether the system has to terminate the connection after the transmission. During initialization you will be first connected to your internet provider and afterwards to the bank.

Proxy settings:

If you **use a Proxy server**, highlight the corresponding checkbox. Subsequently, you can enter for this the **address** (IP address like nnn.nnn.nnn.nnn or host name, e.g. proxy.xyz.de; no URL entries) and **port** of the **proxy** server and a **user name** and **password**.



Please note ...

With EBICS the standard port for SSL/TLS connections (443) is used. With other procedures (e.g. MCFT) the banks define special ports for the connection establishment. If in your proxy outgoing ports are restricted, they need to be activated additionally if necessary. You find the port data in the BPD file of the respective bank and/or in the letter with the access data.

Since communication to the banks usually is executed automatically, the access data need be stored in the proxy parameters, in order that they are always available for the communication processes. If your proxy is awaiting an authentication, we recommend to set up a special identification for the Electronic Banking communication, whose password should be preferably also temporally unrestricted. This is not a security risk, since the access data are stored in encrypted form.

For special cases, in which only MCFT should not be used via proxy, this can be switched off using an entry in the CSUB.PRO configuration file.

The proxy settings are administered separately for each PC in the network and stored in an encrypted way. Thus, an individual user identification together with the appropriate proxy password can be stored here for each PC (or its user), so that there is no need to enter it again for each Comms. order. Thus, also an unattended mode of communication is possible.

In order to simplify the use of the Electronic Banking system, it can also be useful to create a special proxy user whose password does not expire.

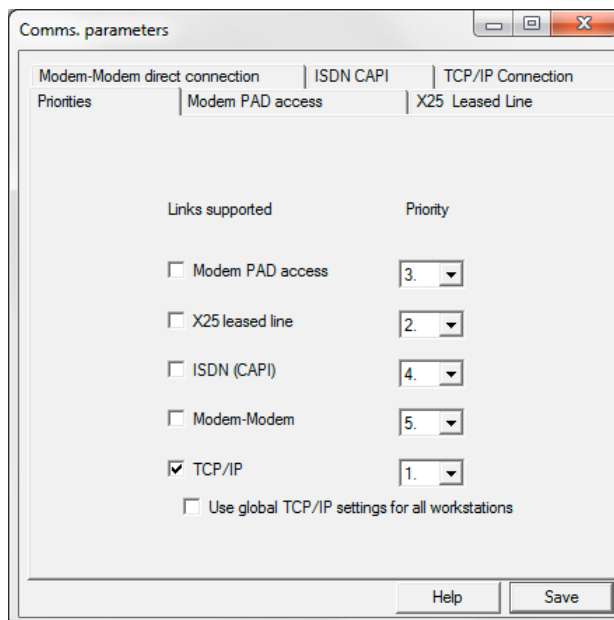
The following proxy authentication protocols are supported:

1. Basic
2. Digest
3. NTLM (Microsoft® ISA-Server)

No special settings need to be made for this, since the Comms. modules negotiate the favored protocol automatically with the proxy during connection establishment.

2.7 Priorities property page (Comms. procedures)

Use the *Priorities property page* to define the sequence (priority) in which the communications methods you have configured should be used.



With TCP/IP the following characteristic exists, that by ticking the **"Use global TCP/IP settings for all workstations"** check box it can be defined, that the TCP/IP parameters (see Chapter 2.6) should be valid globally. In this case TCP/IP need to be activated only once on any computer and the proxy parameters also need to be entered only once. Then they are used by all computers in the network.

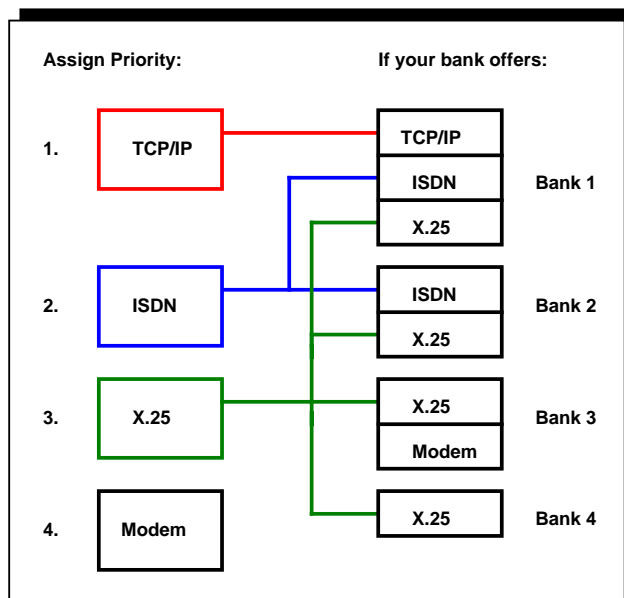
The configuration of transmission paths to your banks (e.g. via ISDN) is specified in the various BPDs (Bank Parameter Data files). If access to a bank changes, you will be notified accordingly and you should then modify the corresponding BPD. Details relating to this are contained in Chapter 3: *Define Bank Parameter Data files*.

Priorities 1 - 5 can be specified for each Comms. method in the list box.

If you have an ISDN line, you should allocate this Priority 1 or 2. If you can also use X.25, allocate this Priority 2 or 3.

If you use a variety of communications methods, the program checks which banks use the method you have allocated top Priority. Sessions for these banks awaiting processing are processed first. The program then moves on to the Comms. method with the next priority and processes those sessions with the specified method.

The procedure is illustrated in the diagram below:



In this example, the program first establishes a connection with Bank 1 over the Internet (= TCP/IP) and processes all pending sessions.

It then connects to Bank 2 using ISDN. All pending sessions are processed. Because all sessions have already been sent to Bank 1 over the Internet, this bank is no longer called, unless transmission over the Internet was not successful.

In the next step, a connection is established to Bank 3 and Bank 4 using X.25, and the remaining sessions are transmitted. Comms. sessions with Priority 1 (Internet) and 2 (ISDN) have already been processed by now, so X.25 is only used for Banks 1 and 2 in the event of errors (Internet and ISDN communication failure).

Because Bank 3, which offers modem-modem communications in addition to X.25, has already been called in the Priority 3 session (= X.25), there is no modem-modem transmission unless: you modify the priority list and assign modem-modem communications a higher priority than the Priority 4 assigned in the example.

2.8 AT Commands

Modems are controlled using the AT instruction set, which has become a de-facto standard. However, the modems available on the market differ in the way they handle this instruction set and the number of instructions they use. In some modems, the commands must all be written in CAPITALS.

A modem can only interpret and process AT commands if it is in the command mode (after switching on or before transmission).

In transparent mode, on the other hand (during transmission), no characters sent to or received from the remote station are interpreted.

Each AT command line must start with the prefix "AT" or "at". "AT" refers to "Attention Code". This code tells the modem to expect one or more commands.

Several commands can be linked together to form a single command line, which must end with a <CR> character. The commands are separated by spaces.

The total number of characters in a command line may not exceed **40** (including AT prefix, commands, spaces and the <CR>).

Example for AT-standard modem:

The following settings are constant for all AT modems.

Transmission type	300 Baud	:	or 1200, 2400 / 9600 / etc.
	Modem	:	
Baud	300	:	or 1200, 2400 / 9600 / etc.
Parity	None	:	
Bits	8 Bit	:	
Port	COM1	:	or COM2, COM3, ..., COM8
PSN ID	xxxxxxx	:	NUI from your network provider
PSN password	xxxxxxx	:	Password from network provider
Modem Init	AT&C1&D2!~~~~	:	
NUA prefix	ATDP	:	
Number	xxxxxxx	:	Tel.No. PSN node
AT standard	[x]	:	"Check"

Init. string

The text in the "Init str." box should be as follows for most AT modems:

```
AT&C1&D2V1!~~~~
|  |
|  | DTR shows whether a connection still exists
DCD shows the carrier
```

If you receive error message "No dial tone" when dialling, change the Init string as follows:

```
AT&C1&D2V1!~~~~ATX1!~~~~
```

Dial string

Structure of the dial string: **ATDabb**

Replace the digits as follows:

- a** = "T" for Tone dial access lines
 "P" for Pulse dial access lines

In PBXs, the outside line may be accessed from the extension with "0W", with "0" standing for the number used by the telephone to access an outside line. "W" tells the modem to Wait until the outside line has been established.

AT Commands (selection):

- **ATZ**
 Reset.
 Corresponds to switching the modem off and on.
- **ATMn**
 Loudspeaker control.
 "n" may have the following values:
 - 0 = always off
 - 1 = on during dialling and connection
 - 2 = always on
 - 3 = on when waiting for answer tone
- **ATLn**
 Loudspeaker volume.
 "n" may have the following values:
 - 0 = off
 - 1 = quite
 - 2 = loud
 - 3 = very loud
- **ATSO=O**
 Autoanswer off
- **ATE**
 Echo off
- **ATD**
 Dial a number:

 Special dialling characters:
 - T = Tone
 - P = Pulse
 - > = Outside line via earth key
 - W = Wait for dialling tone
 - , = 1 second pause before processing next dialling signal (max. 3 "," in succession)

Example: ATDT0W06920251
 Tone , 0 for outside line, W for wait, Dialling tone, telephone no., PTT PAD

Example: ATDP0W06920251
 Pulse, 0 for outside line, W for wait, dialling tone, telephone number, PTT PAD

- **ATQn**
Acknowledgement.
"n" may have the following values:

0 = Acknowledgement on
1 = Acknowledgement off
- **ATVn**
Type of acknowledgement.
"n" may have the following values:

0 = Acknowledgement as number
1 = Acknowledgement as text
- **ATX1**
Report CONNECT 1200 or 2400.
- **ATX3**
The modem does not wait for a dialling tone before dialling. This is particularly important for PBXs.
- **AT&C1**
complies with V22bis to V25bis; DCD shows the status of the Data Carrier of the remote station.
DCD ON status shows valid connection.
- **AT&D2**
If the DTR signal from the PC is set to OFF, the modem disconnects and returns to command mode.
- **AT&Sn**
Data Set Ready signal.
"n" may have the following values:

0 = Data Set Ready signal always on.
1 = Data Set Ready signal OFF in command and text modes.
- **AT&W**
Writes current settings to the modem memory so that they are active the next time the modem is switched on or the ATZ command is entered.

Table of Contents: Chapter 3

	Page
3 Define Bank Parameter Data files	3-2
3.1 Create BPD	3-3
3.2 EPFT / MCFT	3-5
3.2.1 Import MCFT BPD.....	3-10
3.2.2 Export MCFT BPD	3-12
3.3 FTAM.....	3-13
3.4 FTP	3-17
3.5 EBICS.....	3-19
3.6 HBCI.....	3-27
3.7 HBCI+.....	3-32
3.7.1 Maintain period (HBCI and HBCI+)	3-35
3.7.2 Maintain TAN list (HBCI+).....	3-36
3.8 ETEBAC3.....	3-37
3.9 WOP	3-41

3 Define Bank Parameter Data files

BPD files are **Bank Parameter Data** files..

A Bank Parameter Data file saves key data for accessing one of your banks. BPDs are needed to install or lock the transmission paths and to execute Comms. sessions.

You need a separate BPD for **each** bank with which you want to communicate.

If you

- are using the standard **EPFT** communication method, you will receive a "bank disk" from your bank containing the necessary access data in the form of a BPD. The file name normally consists of an abbreviation of the bank's name plus the standard extension *.BPD.
(File name in brackets behind).
You can accept this file using the selection dialog to open using the [**Copy EPFT-BPD**] button from any directory to the program (copy).
- you use the enhanced EPFT procedure with Electronic signature (**MCFT**), you have possibly received from your bank for each employee authorized to sign a diskette with a BPD file which you accept using the selection dialog to open using the [**Import MCFT-BPD**] button from any directory to the program (import).
This creates a "**Multi-user BPD**" containing an entry for each user authorised to enter an Electronic Signature.

From the MCFT bank parameter file dialog, individual user entries can be removed using the [**Export bank parameter file**] button from a Multi-User-BPD and saved (exported) using the selection dialog in any directory as individual BPD file.



The bank parameters, the NUA to be used and the external and internal user of EPFT and MCFT BPDs can only be edited. New BPDs for these communication methods cannot be created.

You must create BPDs manually for all other communication methods. Your bank will provide instructions and relevant details.

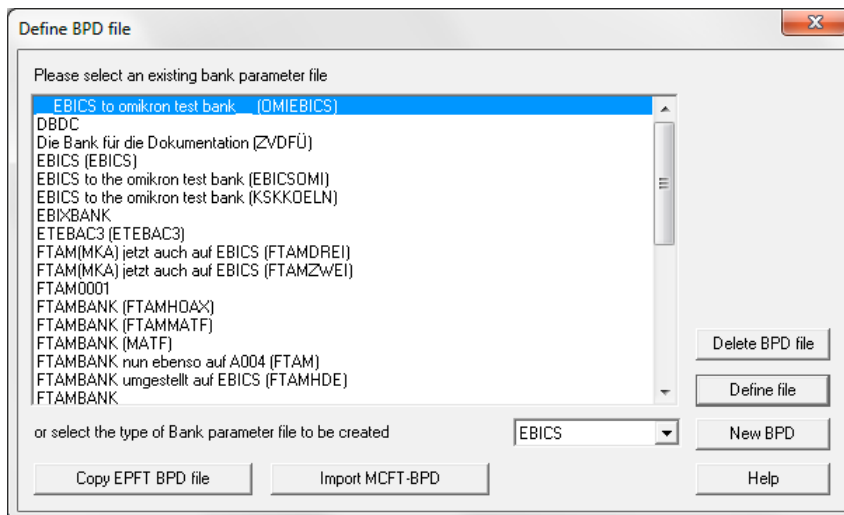
In the current program version, you can create BPDs for

- FTAM
- FTP
- EBICS
- HBCI
- HBCI+
- ETEBAC3
- WOP

The procedure for creating BPDs is identical for all the communication methods listed above. The only differences relate to the type and scope of parameters to be defined.

3.1 Create BPD

The procedure for creating BPDs is identical for all the communication methods listed above. The only differences relate to the type and scope of parameters to be defined.



Follow these steps to create a BPD:

1 Select menu item –Communication- / - BPD files-

If no diskette with a BPD is inserted in the disk drive for the ES, a message asks you to enter the diskette with the BPD file. Press [**Yes**] to access the inserted disk. Press [**No**] to bypass this option and view a list of all BPD files saved on the hard disk in directory ...MCCWIN\DAT. You can also close this step by pressing [**Cancel**]. Files in drives are marked by a drive letter in brackets behind the file name.

2 Select the BPD to be created or edited

After selecting this menu item a dialog box appears which displays all existing Bank Parameter Data files and allows you to select a BPD to be created from a list box showing all supported Comms. methods.

If you

- want to create a new BPD for a particular communication method, select the type of BPD to be created and confirm by selecting the [**New BPD**] button. A list box shows all BPDs that already exist in directory ..\DAT. Enter the name of the file to be created. The extension ".BPD" is automatically added by the program.



Please note ...

The internal BPD file name may have max. 8 digits and may consist only of characters (A-Z,a-z,0-9,-, _).

The extension ".BPD" will be automatically attached by the program and the corresponding entry dialog will be opened.

- want to view and/or edit an existing BPD, position the cursor on the file using either the mouse or the arrow keys and confirm with [**Define file**] button. Double-click the entry in the list to open also the entry dialog.

3 Entering the BPD name / the parameters

The layout of the dialog box for entering parameters differs depending on the communication method on which the selected BPD is based. Enter a name for the BPD file. A maximum of 30 characters can be used.

Information on parameter entry can be found under

- EPFT / MCFT
- FTAM
- FTP
- EBICS
- HBCI
- HBCI+
- ETEBAC3
- WOP

4 Save your entries with [Save].

Click on [Save] to save the settings to the appropriate Bank Parameter Data file.

Please note:

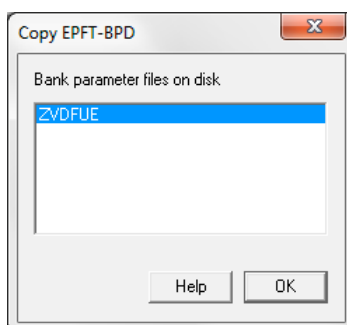
The bank parameters, the NUA to be used and the external and internal user of EPFT and MCFT BPDs can only be edited. New BPDs for these communication methods cannot be created.

Incidentally:

EPFT BPDs can be copied from the disk to the hard disk directory ..\MCCWIN\DAT using the [Copy EPFT BPD file] button i.e. this means that EPFT BPDs can also be saved on a disk.

If, however, you wish to save the EPFT BPD from disk to hard disk, you will be asked to insert the disk with the EPFT BPD file into the drive for the ES after you have clicked on the [Copy EPFT BPD file] button.

After inserting the disk and confirming with [OK] all the BPDs on the disk will be displayed in a list box. Select the BPD to be copied by correctly positioning the cursor and confirming with [OK] or double-clicking.



If the BPD is already saved on the hard disk, you will be asked whether you wish to replace the existing BPD with the new BPD. If yes, confirm with [OK]. Otherwise, click on [Cancel].



If your bank offers communication using MCFT, your bank will provide you with a fully configured Bank Parameter Data file on disk for each person in your organisation authorised to send data to and receive data from this bank. The **MCFT** BPDs **have to** be imported. To do so, use the [Import MCFT BPD] button. Further details can be found in Chapter 3.2.1: Import MCFT BPD

You can delete again bank parameter files by choosing the corresponding BPD file, then click the [Delete BPD file] button and answer the following security prompt with [Yes].

3.2 EPFT / MCFT

EPFT (Electronic Payment File Transfer) is the communications method supplied as standard with the Core module. EPFT features:

- Verification of error-free data transmission
- Compression
- Encryption
- Syntax check (validation) of the data to be transmitted
- Authorisation during transmission
- Guaranteed protection against manipulation

You can use X.25 (Datex-P), ISDN and the telephone network to transmit data using EPFT. If you use EPFT, each bank with which you have signed an agreement for electronic banking services provides you with a BPD. The file name of this BPD is normally an abbreviation of the bank's own name and the extension ".BDP".

If there are any changes to the communications method used by the bank (for example a different NUA), you can modify the BPD accordingly. In such cases, your bank will inform you of any changes to be made.

The extended EPFT method with Electronic Signature is known as **MCFT** (= **M**ulti**C**ash **F**ile **T**ransfer). It features the same full functionality as the EPFT method, but also supports the Electronic Signature described in Chapter 6 for authorising payment orders. In contrast to FTAM, the signature is verified during file transfer itself, providing you with the result of the Comms. session, including signature verification, immediately after data transmission by means of the Return Codes (cf. Chapter 5.4: *Return Codes*).



Do not make any changes to the BPDs without prior instructions from your bank. Unauthorised changes could prevent you from accessing your bank. An exception to this involves the fields with the "internal" and "external names" of users of the MCFT method (described below).

The dialog box for a EPFT BPD contains the following entries:

- BPD description
- User number
- Customer no.
- Bank parameters
- X.25 NUA
- ISDN call no.
- Modem number
- TCP/IP address and port
- Connection information for dial-up networking

Key to the boxes:

Description of bank parameter file

Enter an explanatory description in this box. The description you select will then be shown in all cases instead of the BPD file name.

User number

Customer no.

The entries in the "User number" and "Customer number" boxes are defined by the bank and cannot be changed by you.

Connection information of bank:

X.25 NUA

ISDN call no.

Modem number

The access numbers for X.25 (Datex-P), ISDN and/or modem communications need only be entered if the corresponding bank parameter fields have been set (= "J"). These are fields 6 (X.25 (Datex-P) = "J" or "N"), 7 (ISDN = "J" or "N") and 8 (Modem = "J" or "N"). If the corresponding field in the bank parameter line has been deactivated (= "N"), it is not necessary to enter the corresponding access number.

The program bases its communication with the bank using the relevant Comms. method on the access number/NUA from the BPD. The bank will notify you of the access number(s). In the case of Datex-P, you can specify an area code in the first of the two boxes.



Do not make any changes to the access numbers/NUAs **unless you receive instructions from your bank.**

TCP/IP

If your bank has an Internet gateway, you can use the Internet for all transmit (e.g. payment orders) and download sessions (e.g. account data). In this case, the "IP address" and "Port no." fields already contain the correct entries when you receive your BPD. Instead of using the IP address ("dot notation") the addressing can be made using a **DNS name**. This simplifies the change of addresses because of removal or change of the provider.

To be able to communicate over the Internet, WINSOCK.DLL must be installed on your system. You must also have access to the Internet through a service provider (e.g. T-Online, AOL, etc. or a local service provider).



Do not change IP addresses, port IDs or DNS names **unless you receive instructions**

from your bank.

Dial-up networking (RAS connection):

To use the dial-up connection to your Internet Provider please configure the communications network of Windows first and make necessary adjustments using the specification supplied by your provider. Enter your **connection** as well as **user** and **password** here.

Bank parameters

The "Bank parameters" box is a character string consisting of a combination of letters and numbers.

Please note that the bank parameter field describes the parameters supported by the bank, i.e. the customer can only use ISDN communications with a bank if a "J" is entered in the corresponding field of the bank parameter character string.

Key to the individual fields of the bank parameters:

X	N	X	X	X	X	X	X	X	X	
										PUB session with ES (J [Yes] or N [No]) using MCFT/FTAM/FTP
										Parameter for distributed ES (only for FTP):
										N = no distributed ES
										V = distributed ES without bank distribution list (list defined by customer)
										A = distributed ES with bank distribution list
										Parameter for Internet use (J [Yes] or N [No])
										Parameter for modem use (J [Yes] or N [No])
										Parameter for ISDN use (J [Yes] or N [No])
										Parameter for X.25 use (J [Yes] or N [No])
										Parameter for encryption (H [= hybrid procedure] or N [No]) using FTAM/FTP
										Parameter for ES (N, A, B or C, where A = ES type A002, B = ES type A003/M001, C = ES type A004/M002)
										Parameter for compression (N or F, where F = compression with FLAM) using FTAM/FTP
										Parameter for the internal file name (e.g. A3)

A typical **EPFT** bank parameter line, for example, has the following structure:

A3NNNJJNNNN

- the internal file name starts with **A3**
- No separate compression, no separate encryption are needed because these functions are automatically incorporated in EPFT, no Electronic Signature is available
- for communication with the bank, either X.25 (Datex-P) or ISDN can be used
- The bank does not support modem or Internet communications.
- the Distributed Electronic Signature is not supported by the bank
- the bank does not support PUB orders with Electronic Signature

A typical **MCFT** bank parameter line, for example, has the following structure:

A3NBNJJNJNJ

- the internal file name starts with **A3**
- no separate compression is required because this is already incorporated in MCFT
- the data to be transmitted are protected by an Electronic Signature version M001
- no separate encryption is required because this is already incorporated in MCFT
- for communication with the bank, either X.25 or ISDN can be used.
- the bank does not support modem communications
- the bank does support Internet communications.
- the Distributed Electronic Signature is not supported by the bank
- the bank supports PUB orders with Electronic Signature

Changes are normally necessary only in the four parameters for communications access (X.25/Datex-P, ISDN, modem and Internet).



You should only make changes to these parameters **if instructed to do so by your bank.**

Matching Internal User and Bank user no.:

User number (external name)

In the case of **MCFT**, the BPDs are supplemented by the table with "internal" and "external" names. The table is used to allocate the internal names (User names) to the User numbers at the bank.

Up to 512 approved signatories can be saved in a BPD file.

Internal name	External name	Save comms pass...	Current ES version
3 (Henk Lauwers)	99999900	No	M006
2	10001001	No	No

The "User numbers" (external names) defined by the bank are supplied by your bank (with the BPD). Several User numbers may be assigned to each Customer ID.

You can use the list box which displays all the users registered in the system to assign the User numbers. The program checks whether the **user names** generated in menu item -User- / -Users- are identical to the entries under "**internal name**".

Only the Users entered under "Internal name" who have been allocated a User number can exchange data with the bank using MCFT.

Double-click the list or use context menu entry -Maintain record- (right mouse button) to open the list of the available users (internal name).

Export bank parameter file

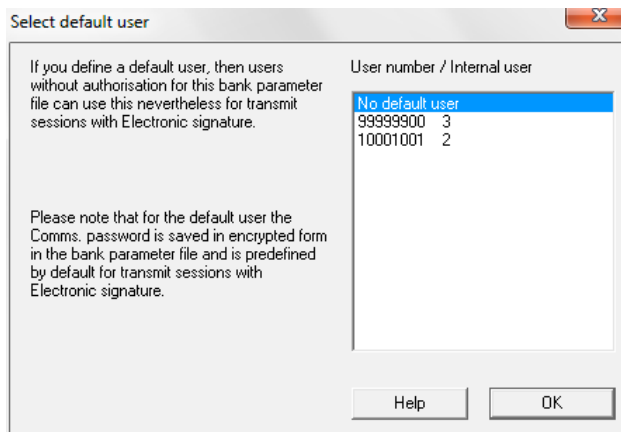
Select the [**Export Bank parameter file to disk**] (cf. Chapter 3.2.2: *Export MCFT BPD*) to remove individual user entries from a multi-user BPD (see Chapter 3.2.1: *Import MCFT-BPD*) and save them as individual BPDs.

Define default user

Using the [**Define default user**] button you can define a so called default user. Users without authorisation for this bank parameter file can still use this to prepare orders with electronic signature. Confirm your entry with [**OK**] finally.

**Please note:**

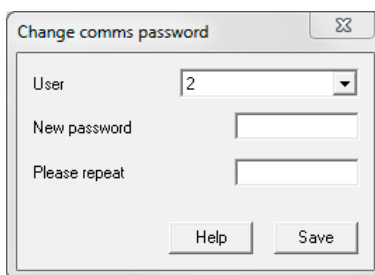
After the definition of a standard user, an administrative order type like INI or PWA has to be accomplished with the standard user first. The comms. password for the default user is then stored in the bank parameter file in encrypted form and is added as default for sending orders with electronic signature.

**Change Comms. password**

Click on [**Change Comms. password**] to change the Comms. password, which is stored in the BPD. (The password, which is known by the bank, is not changed hereby! Therefore the session type PWA must be used or the password has to be changed on the bank computer using the menu item -Communication- / - Change Comms. password- [wizard]).

Select any user from the bank parameter file. Simply enter the new password. 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 for your own protection.

Then confirm your entries with <Return> or by clicking on [**Save**].



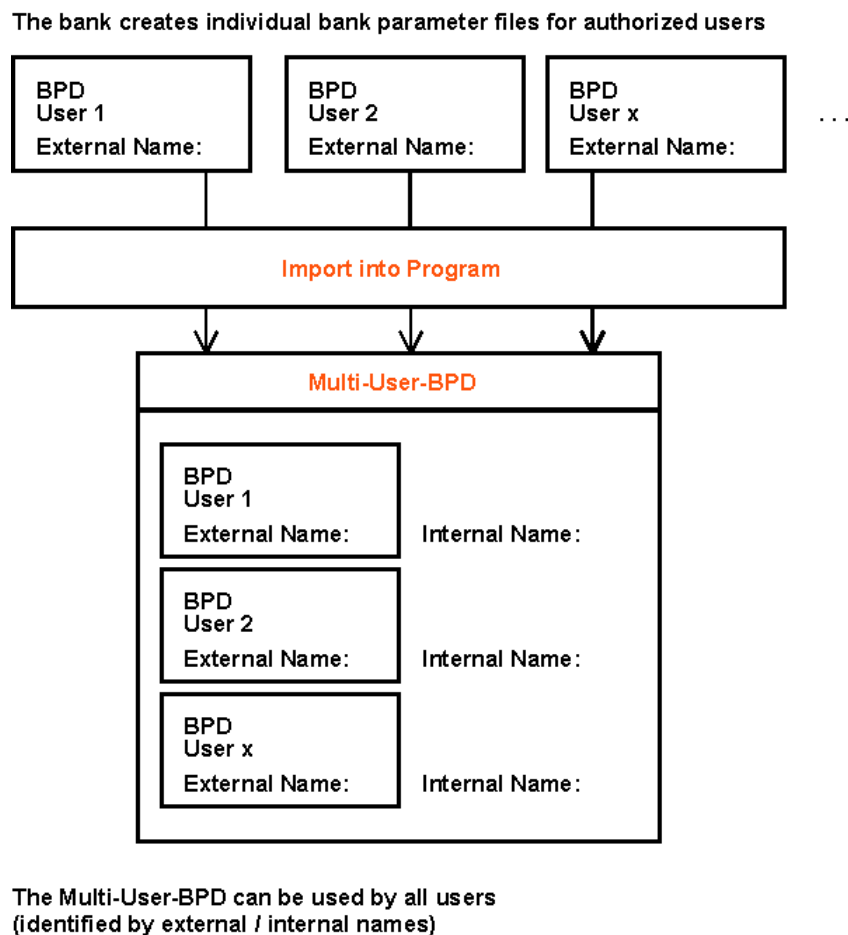
3.2.1 Import MCFT BPD

If your bank offers communication using **MCFT** (cf. Chapter 1.2.2: *MCFT*), they will supply you with a fully configured Bank Parameter Data file on disk for each person in your organisation authorised to send data to and receive data from this bank. You can merge the Bank Parameter Data files on each of these disks to form a "**Multi-user BPD**". You can also use the BPDs separately.

What is a "**Multi-user BPD**"?

The bank has specified that several users can access an account to transmit and download data. An "external name" (User number) has been saved at the bank for these users. All users for whom the BPD contains an "external name" can use this BPD. This means that there does not have to be a separate BPD for each user.

The relationships are explained in the diagram below:

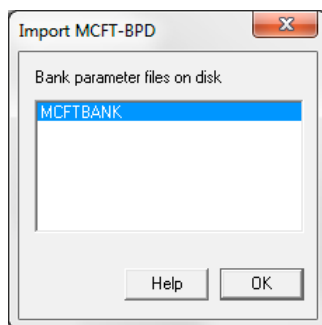


Select the button [**Import MCFT BPD**] to generate a single "Multi-user BPD" from a variety of individual BPDs before defining the BPD file (cf. Chapter 3.1 *Create BPD*). This "Multi-user BPD" can only be saved on the hard disk: it cannot be copied to a diskette.

The advantage of "Multi-user BPDs" is that when Comms. sessions are started, **all** users need only access a **single** BPD to communicate with a **single** bank. This one BPD can be assigned a unique name to identify the relevant bank.

The following steps are necessary to **import a MCFT BPD** or to create a "Multi-User-BPD":

- 1** Select the [**Import MCFT BPD**] button.
- 2** Select the folder where the individual BPD is located on your computer.
- 3** Select the MCFT bank parameter file from which user data is to be transferred from an overview of the bank parameter files available in the chosen folder. Select the appropriate bank parameter file by positioning the cursor or by clicking with the mouse and confirm with [**OK**].

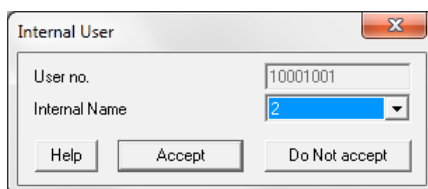


- 4** Allocating the **User number** ("external name") to an internal User. Select the user name (= **internal name**) of the user who will be one of the users of the new "Multi-user BPD" from the list box which lists all users registered in the customer system. Confirm your selection by clicking on the [**Accept**] button. In the event of there being several users, the process will be repeated until all the users have been allocated to internal users. If you do not wish to import a particular user, click on the [**Do not accept**] button



Please note:

When importing a BPD, the "Internal name" box always contains the name of the current user.



Incidentally:

When creating a new "Multi-user BPD" or modifying an existing one, "pairs" are always formed from the "external" name defined by the bank and an "internal" name. This means that an "internal" name is allocated to an "external" bank name.

You can view the "external" and "internal" name pairs contained in a "Multi-user BPD" at any time in -Communication- by choosing menu item -BPD files-. More detailed information is contained in Chapter 3.1: *Create BPD*

3.2.2 Export MCFT BPD

The "**Multi-user BPD**" merged from several individual BPDs using the [**Import MCFT BPD**] button can be split back into individual BPDs using the [**Export Bank parameter file to disk**] button in the dialog box "MCFT-Bank data". The individual BPDs are "exported" to a diskette.

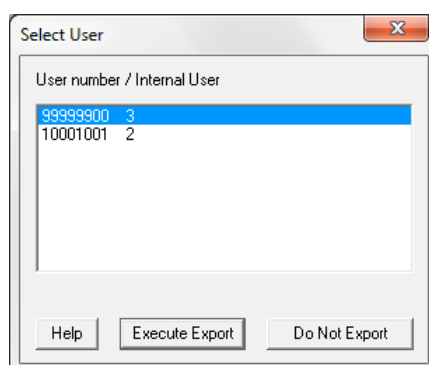
It may be necessary to "export" individual BPDs if a user saved in a "Multi-user BPD"

- leaves the company or organisation and the transmission path for this individual must be deleted
- moves to another department or branch office and will continue to use the transmission path originally defined for this user
- etc.

In the first case, the individual BPD "exported" to diskette must be deleted. In the second case, the user takes his or her individual BPD saved on diskette to their new workplace where they can continue to use it as before.

The following steps are necessary to **export individual BPDs** from a "Multi-User-BPD":

- 1** Select the MCFT "Multi-user BPD" from which the individual BPD will be exported
- 2** Click on the [**Export BPD file to disk**] button.



- 3** Select the user (identified by User number and "internal" user names) whose BPD will be exported. Select one or several users to be exported by positioning the cursor or with a mouse click and then press the [**Execute Export**] button
- 4** Choose target directory for export from the directory structure and confirm with [**OK**]
Insert a medium where required (the individual BPD exported from the "Multi-user BPD" will be written to this medium.)

3.3 FTAM

FTAM (**F**ile **T**ransfer **A**ccess **M**ethod) is a standardised method of transferring files of any kind. FTAM enables access to the contents and attributes of a file in a networked open system.

With FTAM communications, you must **create a separate Bank Parameter Data file for each bank**. In contrast to EPFT/MCFT, your bank does not send you a BPD for FTAM.

FTAM - Bank parameter file

Description of bank parameter file

Connection information of bank

X.25-NUA 45447658765743

ISDN NUA 54568678676769

ISDN call command

Encryption information

No encryption

No encryption bank-side

Single DES 64-Bit

Automatic retrieval of PTK files

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

Information on bank

Customer ID FTAMUSER Host name FTAMHOST Bank parameter A3FBJJNN

Conversion to ES version A004

Not started Started on Maximum length of conversion phase 0

Matching Internal user and Bank user no.

Internal name	External name	Save Comms. pass...	Default user	Sig.class
1	ICH	Yes	Yes	
KUNDE 1	MEIER	No	No	
KUNDE 2	MÜLLER	No	No	
KUNDE 3	MOLL	No	No	

Convert this bank parameter file for using FTP

New user Change Comms. password Session types Sender-ID EDIFACT Help Save

The following boxes are available for generating an FTAM BPD:

Description of bank parameter file

In this field, enter a meaningful description of the BPD file (max. 30 characters) which is used in the further program run instead of the BPD file name.

Connection information of bank:

The information needed to configure the fields listed above will be supplied by your bank. One exception is the "BPD description" field, in which you should enter an explanatory BPD description yourself. The description you select will then be shown in all cases instead of the BPD file name.

- X.25 prefix (Country ID)
- **X.25- NUA**
- **ISDN NUA**
- **ISDN call command** (e. g. PBX, provider number etc.)

Encryption information:

"**Encryption information**" provides information on whether customer or bank encryption has been specified in menu item -Communication - / -Encryption- (see Chapter 4.5) and which key has been selected for encryption. If no encryption between the customer and the bank has been

agreed, the status is: "No customer or bank encryption". After adding the session types VPK or VPB, the status changes to "Customer or bank encryption ready". Once the keys have been exchanged, the status changes to "Customer or bank encryption active".

Automatic retrieval of PTK files:

If you enter a number of minutes in the field "**How many minutes after sending a file?**", an automatic collection of the corresponding log files starts the appropriate time **after** sending a file. If you set this parameter to "0" no automatic collection of *.PTK files takes place.

Information on bank:

The **Customer ID** defined by the bank identifies the customer in all Comms. sessions. The bank computer will only accept Comms. sessions if you have a Customer ID at your bank.

The **Host name** and the **bank parameters** will be provided by your bank.

The "Bank parameters" box contains a character string consisting of a combination of letters and numbers.

Please note that the bank parameter field describes the parameters supported by the bank, i.e. the customer can only use ISDN communications with a bank if a "J" is entered in the corresponding field of the bank parameter character string.

Key to the individual fields of the bank parameters:

X	N	X	X	X	X	X	X	X	X	
										PUB session with ES (J [Yes] or N [No]) using MCFT/FTAM/FTP
										Parameter for distributed ES (only for FTP):
										N = no distributed ES
										V = distributed ES without bank distribution list (list defined by customer)
										A = distributed ES with bank distribution list
										Parameter for Internet use (J [Yes] or N [No])
										Parameter for modem use (J [Yes] or N [No])
										Parameter for ISDN use (J [Yes] or N [No])
										Parameter for X.25 use (J [Yes] or N [No])
										Parameter for encryption (H [= hybrid procedure] or N [No]) using FTAM/FTP
										Parameter for ES (N, A, B or C, where A = ES type A002, B = ES type A003/M001, C = ES type A004/M002)
										Parameter for compression (N or F, where F = compression with FLAM) using FTAM/FTP
										Parameter for the internal file name (e.g. A3)

A typical **FTAM** bank parameter line, for example, has the following structure:

A3FCHJJNNNJ

- the internal file name starts with **A3**
- files can be compressed using the FLAM procedure
- the data to be transmitted are protected by an Electronic Signature version A004
- an encryption is possible (hybrid procedure)
- for communication with the bank, either X.25 or ISDN can be used
- the bank does not support modem communications
- the bank does support Internet communications.
- the Distributed Electronic Signature is not supported by the bank
- the bank supports PUB orders with Electronic Signature

Changes are normally necessary only in the parameters for communications access (X.25/Datex-P, ISDN, modem and Internet).



You should only make changes to these parameters **if instructed to do so by your bank.**

Conversion to ES version A004:

Under "Conversion to ES version A004" you will find information on the status of the ES conversion process (not started, can be started, started, ready), on the start of the conversion and on the max. length of the conversion phase (60 days by default). For more information see Chapter 6.3: *Convert signature version*.

Matching Internal User and Bank user no.:

In addition to the customer ID, you should define internal and external names for the individual users allowed to use the respective BPD. Up to 512 authorized signatories can be stored in one BPD.

The "**external names**" defined by the bank are supplied by your bank's Customer Service dept. Several external names may be assigned to each Customer ID.

You can also assign the external names to specific users. The program checks whether the user names defined in menu item -Users- are identical to the entries under "**internal name**". Only users entered under "internal name" who have been assigned an "external name" can use FTAM to communicate with a bank.

Double-click the list or use context menu entry -Maintain record - (right mouse button) to open the list of the available users (internal name). Then you can enter the external name. Use the context menu entry -New entry of user - to add new users (from the one available on the PC) to the BPD file (new record). Use -Delete- and confirm the security prompt with [**Yes**] to remove user entries from the BPD file.

In addition, it can be defined for each user whether the Comms. password shall be saved in the bank parameter file. To do so, choose either "Yes" or "No" from the list in the column "**Save Comms. password**".

The Comms. password is saved in the BPD file and automatically added to the Comms. session for transmit sessions with an Electronic Signature. This eliminates the need to enter the Comms. password manually for each bank even if encryption is activated - as long as it is validated by an Electronic Signature .

After starting the BPD session type "Fetch Bank Parameter Data file", the signature category defined for you by the bank is entered in the "**Sig. class**" box:

N	No signature required
E	Permission for single signature up to maximum amount
A	Permission for single signature with any ES permission up to the maximum amount
B	Permission only for second signature up to max. amount

In the context of the enhancement of the signature keys to a length of 1024 Bit the allocation area was extended by a column with the **current ES version** of each user (A003 or A004).

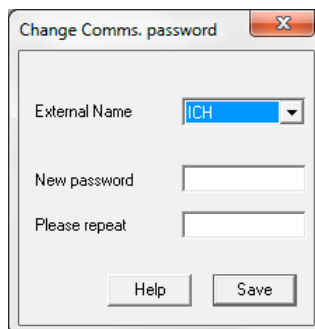
Click on [**Change Comms. password**] to change the Comms. password, which is stored in the BPD.

(The password, which is known by the bank, is not changed hereby! Therefore the session type PWA must be used or the password has to be changed on the bank computer using the menu item -Communication- / - Change Comms. password- [wizard]).

This function has to be used, if a FTAM BPD was restored from backup, the check box "Save Comms. password" was set and the password has changed between the backup and the restoring.

Select any user from a list of external names. Simply enter the new password. 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 for your own protection.

Then confirm your entries with <Return> or by clicking on [**Save**].



Change Comms. password

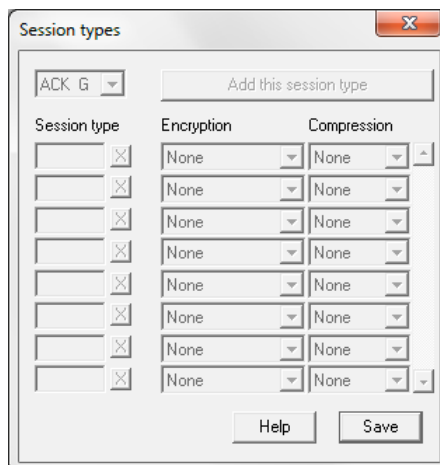
External Name: ICH

New password:

Please repeat:

Help Save

Finally, click on [**Session types**] to define the session types for which encryption and/or compression using FLAM will be enabled. The information is entered via BPD session type "Fetch Bank Parameter Data file", but you can edit this information if you wish. Select the session type you are looking for from the list box containing all possible session types. Add this session type to the table below by clicking on [**Add this session type**]. Continue doing this until you have entered all the session types you want in the table. You can then specify for each session type whether encryption should be activated or not, or whether the data should be compressed using FLAM. Confirm your entry with [**Save**].



Session types

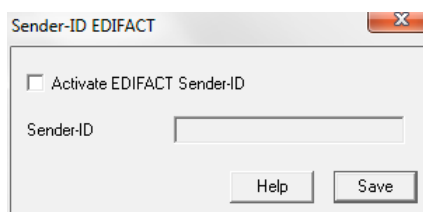
ACK G Add this session type

Session type	Encryption	Compression
	None	None
	None	None
	None	None
	None	None
	None	None
	None	None
	None	None
	None	None
	None	None

Help Save

When sending an EDIFACT file, select the [**Sender ID EDIFACT**] button to validate the file with a Sender ID.

Some banks require a signature in accordance with the General Safety Agreement EDIFACT in the case of EDIFACT transmissions. Should this be the case, check the option box "Activate Sender ID" and enter the Sender ID in the appropriate field. Having done this, transmit the public key to this bank again (Session type PUB). Please note that either an EDIFACT-ZV-module or the EDIFACT support must be installed for EDIFACT transmissions.



Sender-ID EDIFACT

☐ Activate EDIFACT Sender-ID

Sender-ID:

Help Save

Internet communication using FTAM is not possible at present.

Click on [**Save**] to save the settings to the appropriate Bank Parameter Data file.

3.4 FTP

FTP (**F**ile **T**ransfer **P**rotocol) is an Internet protocol which supports data interchange across the Net.

Files are generally transferred in binary mode. They cannot be transferred in ASCII because all files are transferred in encrypted form.

The FTP BPD dialog box is generally similar to the FTAM BPD dialog box (see Chapter 3.3). Also, up to 512 approved signatories can be saved in a BPD file (assignment as for FTAM).

Instead of the Datex-P NUA or ISDN NUA, all you need to do is enter the **IP address** of the bank host computer, **Data port** (on bank side) and **FTP port** (on your side) as "Connection Information on bank". The addressing can be made using a **DNS name** instead of using the IP address ("dot notation") This simplifies the change of addresses because of removal or change of the provider.

There are additional options for dial-up networking:

To use the dial-up connection to your Internet Provider please configure the communications network of Windows first and make necessary adjustments using the specification supplied by your provider. Enter your **connection** as well as **user** and **password** here.

The other data you need to enter in the boxes will be notified by your bank.

In the context of the enhancement of the signature keys to a length of 1024 Bit the allocation area was extended by a column with the current ES version of each user (A003 or A004). Under "Conversion to ES version A004" you will find information on the status of the ES conversion process (not started, can be started, started, ready), on the start of the conversion and on the max. length of the conversion phase (60 days by default). For more information see Chapter 6.3: *Convert signature version*.

FTP - Bank parameter file

Description of bank parameter file

Connection information of bank

IP-Address: 123 123 123 123

DNS name:

Data port: 0 Cmd port: 0

Encryption information

No encryption

No encryption bank-side

Single DES 64-Bit

RAS connection

☐ Use Dial Up Networking

Connection:

User:

Password:

Automatic retrieval of PTK files

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

Information on bank

Customer ID	Host name	Bank parameter
FTPKUNDE	FTPHOST	A3FCHNJNJWJ

Matching Internal User and Bank user no.

Can be started Begun on Max. duration of conversion phase 60

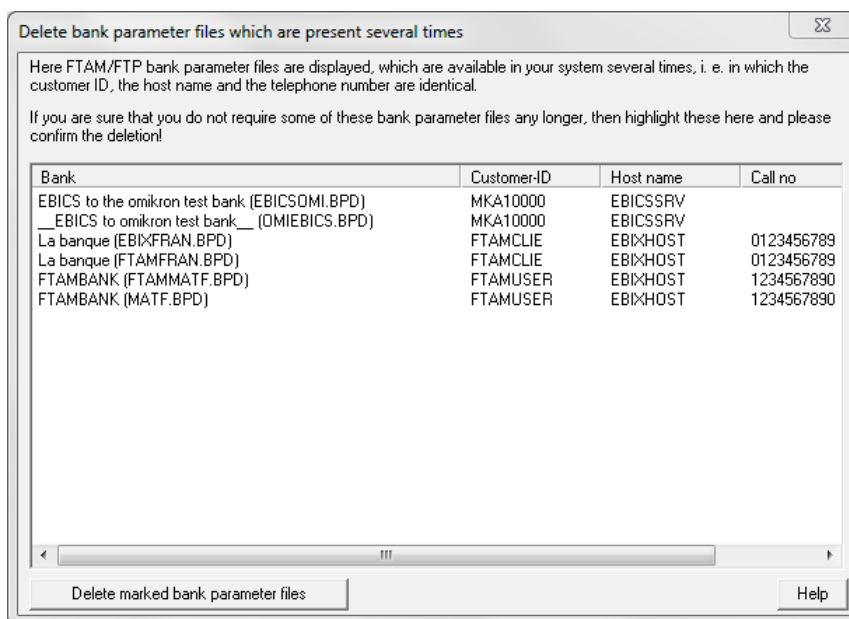
Allocations internal user and user no. at bank

Internal name	External name	Save Comms. pass...	Default user	S class	Current B
1	FTP_USER	No	No		

New user Change Comms. password Session types Sender-ID EDIFACT Help Save

Delete several times available bank parameter files

If a FTAM or FTP bank parameter file will be detected in your system, which is available several times, that means which is different by name, but identical by customer ID, host name and the call number, these bank parameter files are displayed in a special window after a new installation. You can remove these no longer needed bank parameter files from the system by pressing the [**Delete marked bank parameter files**] button.



3.5 EBICS

EBICS (**E**lectronic **B**anking **I**nternet **C**ommunication **S**tandard) is a standard procedure for the communication via internet provided by all German banks starting from 2008. Starting from November 2009, EBICS is supported also by all banks in France (only version 2.4).

As it is with the FTAM/FTP communication, you have to generate **a separate bank parameter file (BPD) for each bank**.

If you want to convert an existing FTAM/FTP access to EBICS, please use the migration wizard under - Communication- / - Convert FTAM/FTP bank access to EBICS- (Chapter 4.6) for this.

EBICS - Bank parameter file

Description of the bank parameter file: EBICS with bank data

Bank connection details: ? Address (URL): https://r-ufa3.tr.omikron.de/EBICS/ Check access Authentication status of the bank: Ready

Information regarding the bank: Customer-ID: EBC323KK Host name: EBICSUFA Operation mode: Standard EBICS-Protocol version: H004

Automatic collection of PTK files: How many minutes after sending a file (0=Never)? 0

Internal name	External na...	Save Comms. passw...	Default user	Current ES version	EBICS status
3	EBC323T3	No	No		New
2	EBC323T2	No	No		New
1	EBC323TT	No	No	A006	Ready

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

In an EBICS bank parameter file, the following fields are available:

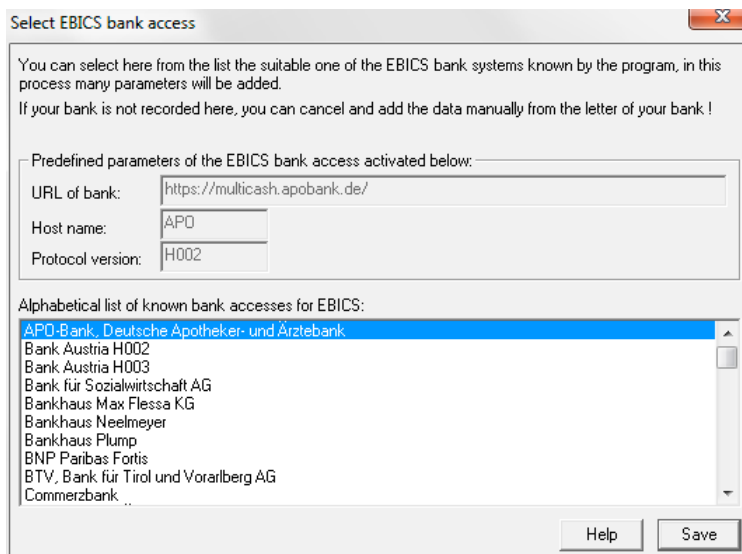
Description of bank parameter file

In this field, enter a meaningful description of the BPD file (max. 30 characters) which is used in the further program run instead of the file name of the BPD file.

Connection information of the bank:

The required details are notified to you by your bank. Enter here the internet **address (URL)** of the bank server (DNS name or IP address) for the EBICS access.

Use the [?] button in front of the connection information to open a list of known EBICS access data.

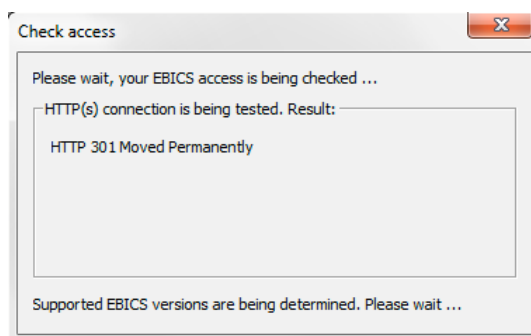


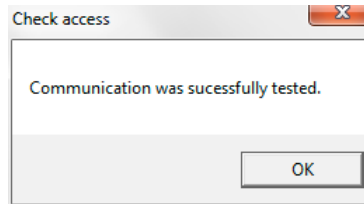
If a suitable access is contained in the alphabetical list, you can choose it and add the access data to the bank parameter file by clicking on the [**Save**] button.

Using the [**Check access**] button you can test the connection to the bank host. After pushing the button the result of the EBICS URL check is displayed accordingly. Close the boxes via [**OK**] button respectively.

The following messages can be displayed:

1. In the case of a wrong certificate:
E_TLS_INVALID_CERTIFICATE- Communication cannot be established
2. In the case, that the proxy is addressed with the wrong port:
E_TLS_INVALID_SERVER_HELLO - Communication cannot be established
3. In the case, that proxy or server cannot be found:
E_HTTPCLIENT_CONNECT_FAILED - Communication cannot be established
4. In the case, that the server can be found, but the start page is wrong:
HTTP 404 Not Found- Communication was successfully tested
5. In the case, that everything runs successfully:
HTTP 301 Moved Permanently - Communication was successfully tested





At the same time a **HEV request** is started, which retrieves the EBICS protocol version (see further below) supported by the bank system (e.g. with EBICS 2.4 the protocol version H003). If this request is successful, the protocol version is set in the BPD and the field "Protocol version" is blocked, since from this point the bank computer defines the highest EBICS version to be used (see also EBICS parameters further below).

Using the [**Check access**] button already existing bank accesses can be updated manually. This request can be accomplished also from subscribers not yet initialized and so it is possible without authentication signature. The HEV request is also executed, if a newly entered EBICS BPD is stored.

Authentication status of the bank:

Here you find details regarding the "**Authentication status of the bank**", the corresponding details regarding the user status can be found beneath in the area of the user allocation. You find here first the status display "New" (before requesting the bank keys). After successful verification of the keys the display changes to "Ready". A failure of the verification is displayed by "Verification defective".

Bank information:

The **Customer-ID** defined on bank side is used for all communication jobs for the identification of the customer. The bank server only accepts your communication jobs if you have a Customer-ID from your bank. Information on **host name** is provided by the the bank, e.g. Standard, France T (Transport ES), France TS (individual ES), Switzerland UBS..

The field **Operation mode** specifies, which EBICS variant is used by the bank.

Under **EBICS protocol version** the protocol type supported by the bank is displayed. After a HEV request the protocol version supported by the bank system is entered here.

This ensures, that the initialization is accomplished with the highest protocol version supported by both systems. If the request fails, the version H002 is entered in the BPD (since this always has to work).

Automatic retrieval of PTK files:

If you replace here the presetting 0 by a number of minutes in the field "**How many minutes after sending a file?**", an automatic retrieval of the corresponding log files starts the appropriate time **after** an EBICS transmit session. If the parameter is set to "0" no automatic retrieval takes place.

For the type of customer log the following applies:

Session type	Protocol version	Operation mode	Remark
PTK	All	All	To some extent not supported completely in France.
ACK	H003	France T and TS	If the parameter "Payment Status Report instead of customer logfile?" is set in the EBICS parameters (see below), ACK is automatically executed for H003.
HAC	Starting from H004	All	If the parameter "Payment Status Report instead of customer logfile?" is set in the EBICS parameters (see below), HAC is automatically executed for H004

			(customer logfile in XML format).
--	--	--	-----------------------------------

Allocations internal user and user number at the bank:

In addition to the Customer-ID, define internal and external names for the individual users who may work with the respective BPD file. Up to 512 approved signatories can be saved in a BPD file.

You receive the "**external names**" defined on bank side from your bank. To each Customer-ID several external names can be allocated.

The external names can be allocated by you to defined users. Under "**internal name**" you can choose the user names defined in menu item -Users- using a list box. Only the users entered under "internal user", to which an "external name" has been allocated, can exchange data with a bank via EBICS.

Using the [**New user**] button or context menu entry -New entry of user- when clicking with the right mouse button on an already entered user, new users (from the users available within the computer) can be chosen and added to the BPD file (a new record is created). By clicking with the left mouse button in the list or using context menu entry -Maintain record- (right mouse button) existing records can be edited. Using -Delete- and confirming the security prompt with [**Yes**] user entries can be deleted from the BPD file.

In addition to the external name, you can define for each user whether the Comms. password shall be saved in the bank parameter file. To do so, choose in the column "**Save Comms. password**" from the list either "Yes" or "No". Furthermore, you can define whether the entered user shall be a "**Default user**". More detailed information can be found in the text for the migration wizard, where you can define within the framework of the conversion a user as default user (technical user) (see Chapter 4.6: *Convert FTAM/FTP bank access to EBICS: Define default user*).

The information on the used Electronic Signature (**current ES version**; EBICS requires at least signature version A004) and on the **EBICS status** for each user (for the authentication status of the bank, see above) is updated within the context of the data exchange with the bank. Possible states for the user are:

New - before initialisation

Partially initialised (INI) - only if INI has been executed successfully

Partially initialised (HIA)- only if HIA has been executed successfully

Ready - if INI and HIA have been executed successfully

Disabled - if a SPR order has been executed successfully

Further functional buttons:

Use the [**Change Comms. password**] button to change the password which is saved in the BPD file. For this, each user can be chosen from a list of **external names**. You simply enter a **new password**. 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.

Confirm finally your entries with <Return> or by clicking [**Save**].

With the monthly HPD retrieval (Receive bank parameter data) also a **HKD request** (Receive customer and user information) is accomplished. The received data are stored for each bank parameter record and can be displayed using the [**Bank data**] button. If the retrieval is made manually via file manager, the data are displayed there [also for **HTD requests** (Receive user information)]. The manual update is also possible there at any time.

The screenshot shows a window titled "DAT\HKDA000.DSP" with the following sections:

Address:
Name and address
Ebits BR 323

Information on bank:
Host name

Account data:

Currency	Account id	Bank	A/c. number
EUR			
EUR			
EUR			
EUR			
EUR			
EUR			

Session types:

Session type	Direction	ES required	Description
ACK	Download		EBICS-Protokoll (PSR)
ATZ	Upload	2	Österreich IZV V3
AZV	Upload	2	Auslandszahlungsverkehrsdatei
C2C	Upload	2	SEPA Firmenlastschrift Container
C52	Download		CAMT Saldenreport/Vormerkposten
C53	Download		CAMT Tagesauszug
C54	Download		CAMT Sammelbuchungsdatei/Avise

The [**Hash values of bank**] button is used to display the last entered hash values (**Authentication hash of the bank (X0??)** / **Encryption hash of the bank (E0??)**) for the reconciliation with the keys collected from the bank (session type HPB). The hash values are notified to you by the bank.

It is no need to enter all values. Normally, a few digits are sufficient for the authentication. All values entered by you are reconciled with the transmitted values. Quit the entry by pressing the [**Save**] button.

The screenshot shows a dialog box titled "Hash values of bank" with the following sections:

Authentication hash of bank (X0??)

Digits 1-8: [][][][][][][][][]

Digits 9-16: [][][][][][][][][][][][][][][][][]

Digits 17-24: [][][][][][][][][][][][][][][][][]

Digits 25-32: [][][][][][][][][][][][][][][][][]

Encryption hash of bank (E0??)

Digits 1-8: [][][][][][][][][]

Digits 9-16: [][][][][][][][][][][][][][][][][]

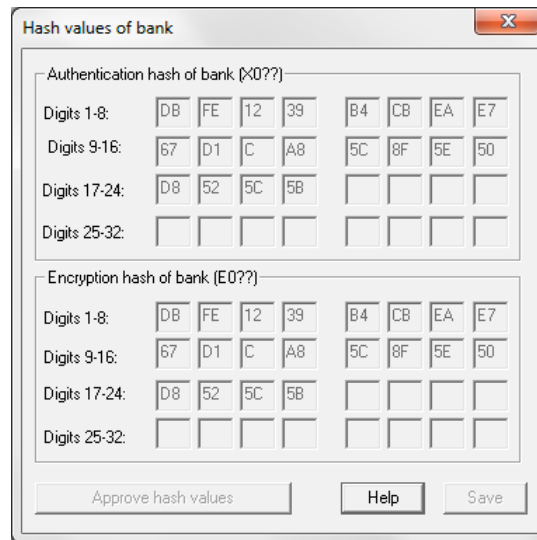
Digits 17-24: [][][][][][][][][][][][][][][][][]

Digits 25-32: [][][][][][][][][][][][][][][][][]

Buttons: Approve hash values, Help, Save

More detailed information can be found in the text for the migration wizard where you can already enter the hash values within the context of the conversion (see Chapter 4.6: *Convert FTAM/FTP bank access to EBICS: Enter hash values of bank keys*).

After collection of the bank keys by means of HPB session type the hash values of the bank are entered here and the mask is no longer capable for editing.



Hash values of bank

Authentication hash of bank (X0??)

Digits 1-8:	DB	FE	12	39	B4	CB	EA	E7
Digits 9-16:	67	D1	C	A8	5C	8F	5E	50
Digits 17-24:	D8	52	5C	5B				
Digits 25-32:								

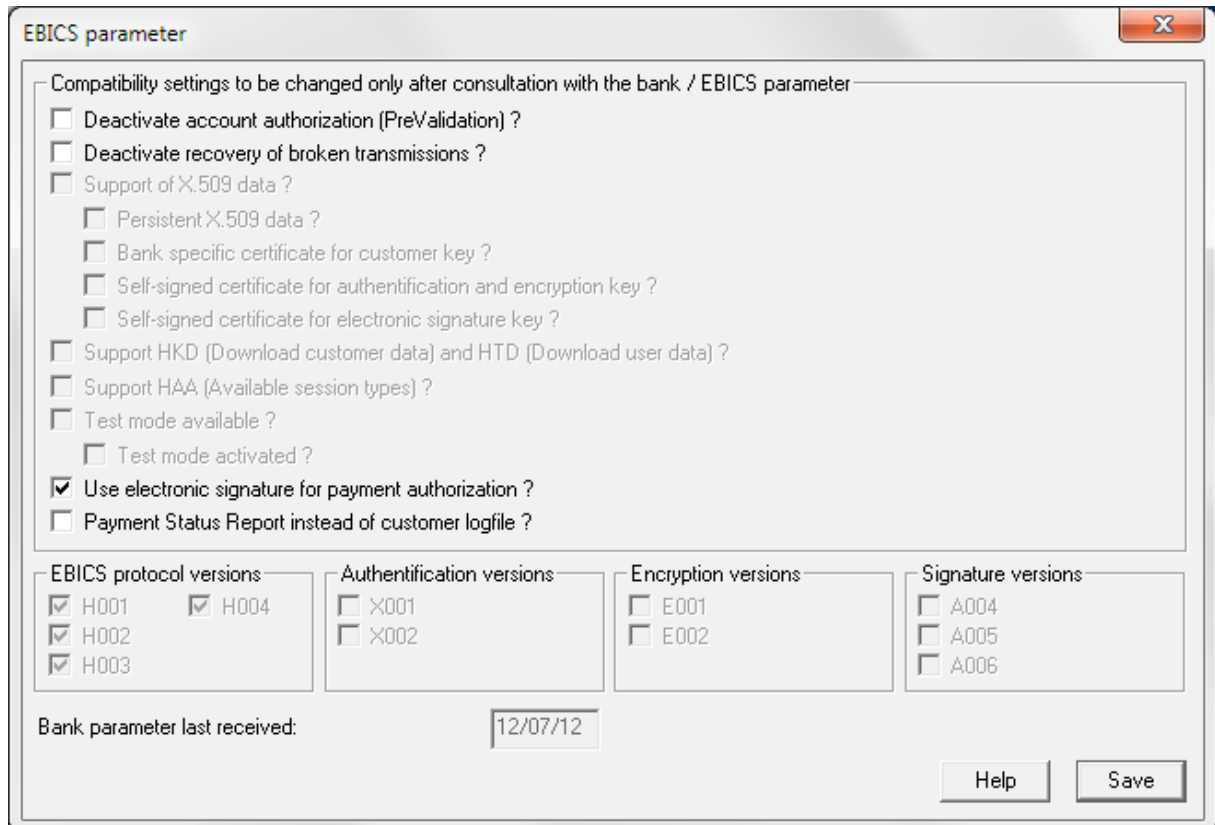
Encryption hash of bank (E0??)

Digits 1-8:	DB	FE	12	39	B4	CB	EA	E7
Digits 9-16:	67	D1	C	A8	5C	8F	5E	50
Digits 17-24:	D8	52	5C	5B				
Digits 25-32:								

Approve hash values Help Save

If the alignment of the hash values was not successful, these values remain editable and can be approved after manual alignment using the **[Approve hash values]** button.

Using the **[EBICS parameters]** button you can switch to an overview, where the compatibility settings/parameter information supported by the bank is summarized.



EBICS parameter

Compatibility settings to be changed only after consultation with the bank / EBICS parameter

- ☐ Deactivate account authorization (PreValidation) ?
- ☐ Deactivate recovery of broken transmissions ?
- ☐ Support of X.509 data ?
 - ☐ Persistent X.509 data ?
 - ☐ Bank specific certificate for customer key ?
 - ☐ Self-signed certificate for authentication and encryption key ?
 - ☐ Self-signed certificate for electronic signature key ?
- ☐ Support HKD (Download customer data) and HTD (Download user data) ?
- ☐ Support HAA (Available session types) ?
- ☐ Test mode available ?
 - ☐ Test mode activated ?
- ☒ Use electronic signature for payment authorization ?
- ☐ Payment Status Report instead of customer logfile ?

EBICS protocol versions <input checked="" type="checkbox"/> H001 <input checked="" type="checkbox"/> H004 <input checked="" type="checkbox"/> H002 <input checked="" type="checkbox"/> H003	Authentication versions <input type="checkbox"/> X001 <input type="checkbox"/> X002	Encryption versions <input type="checkbox"/> E001 <input type="checkbox"/> E002	Signature versions <input type="checkbox"/> A004 <input type="checkbox"/> A005 <input type="checkbox"/> A006
---	--	--	--

Bank parameter last received: 12/07/12

Help Save

Compatibility settings / EBICS parameters:

Attention! The settings in this section are only to be changed after consulting your bank:

The **"PreValidation"** function effects, that always all information required for a pre-validation of the ES, the account authorization and the limit is transmitted. If the bank system supports the "PreValidation" function, the reply from the bank server, if pre-validation fails, is displayed in the File Manager. The order can then be edited again.

By ticking the **"Deactivate account authorization (pre-validation)?"** check box, this function can be deactivated on customer side if necessary.

The **"Recovery"** function enables to continue the transmission of an order after a communication abort, without need to transfer all already successfully sent order data segments again. If the bank system also supports the "Recovery" function, on repeating it the communication is automatically continued at the restarting point.

By ticking the **"Deactivate recovery of broken transmissions?"** check box, this function can be deactivated on customer side if need be.

If the bank supports the use of certificates, the **"Support for X.509 data?"** box is checked. In France, certificates for customer and bank are mandatory.

Additionally, the **"Persistent X.509 data?"** check box can be ticked.

Further options are:

"Bank specific certificate for customer key?". Using this option it is possible to support one certificate per bank.

"Self-signed certificate for authentication and encryption key?". In this case no CA is necessary (default in France).

"Self-signed certificate for signature key?" In France with variant T.

If the bank supports the "ClientDataDownload" function, the appropriate check box is marked. With this, the session types **HKD (download customer data)** and **HTD (download subscriber data)** are used.

If the bank supports the request of session types, the **"HAA support"** check box is ticked (Collect retrievable session types).

If the bank supports the EBICS test mode option, the check box **"Test mode available?"** is ticked (default in France). The test mode is activated/deactivated using the following check box **"Test mode activated?"**.

Further options are:

"Use electronic signature for payment authorization?"

This option controls, whether for this bank electronic signatures should be used for payment authorization. If this parameter is not activated, the file indeed can be signed in the payment module, but is added to the file manager with attribute T (transport signature).

"Payment Status Report instead of customer log file?"

If this option is checked, depending on the protocol version (see above) a Payment Status Report (session types ACK or HAC) is collected instead of a customer log file (session type PTK).

EBICS protocol versions:

The EBICS protocol version supported by the bank is displayed here. With the EBICS version 2.4/2.5 a new protocol version (H003/H004) was introduced.

Authentication versions:

The version of the authentication procedure supported by the bank is displayed here. With the EBICS protocol version H003 also a new version of the authentication procedure (X002) was introduced.

Encryption versions:

The version of the encryption procedure supported by the bank is displayed here. With the EBICS protocol version H003 also a new version of the encryption procedure (E002) was introduced.

Signature versions:

The signature version supported by the bank is displayed here. With the EBICS protocol version H003 the new ES versions A005 and A006 were introduced newly.

The update of the supported features of the bank is accomplished all 30 days automatically by means of a **HPD request** (Download bank parameters). The date of the last HPD request is stored in the BPD and is shown here in the "**Bank parameters received last time:**" box. With each communication it is checked, whether the last HPD request lies one month or longer back. If this is the case (or still no last request date is stored), a HEV and a HPD request are accomplished automatically before the pending order and the date is registered here.

**Please note ...**

If you would like to accomplish a HPD request outside of this fixed 30 days range, for example upon call of the bank, then this is possible at any time in the file manager by creating a collection order.

By confirming finally with the [**Save**] button the settings are added to the EBICS bank parameter file.

3.6 HBCI

Using the HBCI procedure (Homebanking Computer Interface) you work with an individual digital key on a personal diskette or chipcard. You insert this into the disk drive or into a special chipcard reader while working with the program. With the data on the diskette or on the chipcard, your orders to the bank are encrypted after entering a password/a PIN.

To be able to use HBCI, whichever security medium you may use, you have to take care of the fact that

- the "HBCI communication module" has been installed.
- the "TCP/IP connection" procedure has been ticked on the *Priorities property page* on menu item - Communication- / -Comms. parameters-. On the *TCP/IP connection property page*, you have to decide whether the connection is made using dial up networking or LAN.

If you want to use the HBCI procedure *with chipcard*, you have to ensure additionally that

- the chipcard reader driver has been installed,
- the connected chipcard reader has been tested using menu item –Chipcard reader- in the Windows control panel.

After clicking the [**New BPD**] button under -Communication- /-Bank parameter files-, selecting the "HBCI" procedure using the list box and entering a name for the bank parameter file, a dialog opens to enter the account details and the selection of the key medium.



Please note ...

The internal BPD file name may have max. 8 digits and may consist only of characters (A-Z,a-z,0-9,-,_,.).

Please enter first in the two text boxes your account details consisting of the bank code (**BLZ**) and the **a/c. number**, for which you wish to use the HBCI procedure. Subsequently, choose the medium for saving the keys by clicking on the appropriate radio button.

The further procedure is a little different depending on **diskette** or **chipcard** usage:

Option A: You want to use a key diskette...

After confirming the selection with [**OK**], enter the following in the next dialog successively:

- the **drive** (the drive letter) for your HBCI key diskette
A key pair consists of a Private Key and a Public Key. The Private Key can only be written to a diskette. Therefore, the entry of "A" or "B" is only allowed in the first text box. The Public Key is saved on the hard disk and is sent then to the bank via Comms.
- the **password** which can be used immediately (PIN / pass phrase)
Using the PIN / pass phrase you access the Private Key stored on diskette for each interaction with the bank (key change, sending payment orders, collecting account data, etc.).

Confirm with [**OK**] to open the dialog box for the data of the bank parameter file.

Option B: You want to use a chipcard...

- After confirming the selection with [**OK**] and after being prompted by the program, insert your chipcard into the **chipcard reader**.
- Subsequently, enter your **password** (PIN / pass phrase).
Using the PIN / pass phrase you access the Private Key stored on the chipcard for each interaction with the bank (key change, sending payment orders, collecting account data).

If you have received a chipcard already configured from your bank, a further prompt follows to allow the data import.

After selecting an contact and confirming with [**OK**], the corresponding data has already been entered in the following dialog box of the HBCI bank parameter file.

After the respective selection of the key medium and logon using the password, the dialog box for the data of the HBCI bank parameter file opens:

If you want to store the access data on diskette, you receive a document (first access letter) from your bank, containing the essential data for your HBCI access. An example for this can be found at the end of this chapter. When a chipcard is sent, this document can be omitted (field entries are read from the chipcard) or can show only a part of the information contained in the example (to be added to the entries already imported).

Enter the data sent to you in the fields of the dialog box; in the case that such written information is not available accompanying your chipcard, the complete information is contained on your chipcard. In this case, confirm the dialog box simply by using the [**OK**] button.

**Please note ...**

As a matter of course, several users can also be authorized to access an account (further entries under MC user name and user-ID). In this case, the corresponding user data must also be deposited and each user entered additionally has to log on to the system at a later time again, has to select the HBCI file under -Communication- /-Bank parameter files-, has to log on and has to execute the procedure described below with his own security medium.

For new key media, the [**Generate key**] button is only activated initially.

Enter then the details for your HBCI access notified by the bank in the corresponding fields and start the key pair generation for the current user (!) by clicking the [**Generate key**] button then.

Incidentally:

During the creation of the signature and encryption key, the respective bank is contacted simultaneously. The bank keys made available there, which are also required for the communication, are collected – if they have not already been saved on the chipcard – and are then available for further usage in the program.

If the Public Key of the bank has been successfully received, you have to compare the hash value displayed in a further dialog subsequently with the data on the written bank message (an example for this can be found at the end of this chapter) and confirm the match with **[OK]**.

After successful key pair creation and exchange of the Public Key of the current user, now the further buttons in the dialog box of the HBCI bank parameter files are activated. Using the **[Print INI letter]** button you should now print the INI letter (with your Public Key) (file: PINBRIEF.TXT), which you have to sign and to send to the bank for the release of your HBCI access.

Example: INI letter of the user

INI LETTER

```
User name      1
Date          30.09.03
Time          13:47
Beneficiary    87654321
User-ID       MKAC1U01
Customer ID    MKAC0001
Key number     1
Key version    1
HBCI version   210
```

Public Key for the Electronic Signature

Exponent

```
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
```

Modulo

```
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
00 00 00 00 - 00 00 00 00 - 00 00 00 00 - 00 00 00 00
B6 9C FE 78 - 20 6B 93 47 - 10 D3 F2 8F - 41 20 E6 DF
30 FF 4B B1 - 98 AF A5 06 - 15 BD 1B 0f - C9 BB 1C 96
F3 35 62 4B - 8E E8 E7 8B - 3A 41 22 67 - 85 AC B8 CD
65 32 D8 88 - F0 D3 07 8A - A7 03 CD 5D - 39 80 A6 58
00 B7 3A 0e - EF 47 3C B7 - CD CB F4 BE - E7 4A F2 38
53 0d 4E 4E - DF 97 38 3D - D6 DA 7E E7 - 76 CB A9 75
```

```
Hash          5B AD 1C 27 - 3B 68 7C 83 - 6C 15
              34 21 69 C7 - 1A AA 2B B5 - 98 0E
```

The above Public Key will be hereby confirmed for the Electronic Signature of the user authorized under the above User-ID.

Town/Date

Signature

If required, you can change then your keys, block or delete them in the dialog box of the HBCI bank parameter file using the corresponding buttons **[Change key]**, **[Block key]** or **[Delete key]**.

Using the [**Change password**] button you can change the password for accessing your key medium. For this, enter the new password in the appropriate field. In the field "check entry" repeat your entry for security reasons once again.

Using the [**Maintain period**] button you can change the collection period as well as the "Start" statement number of account statements according to HBCI⁺ (see Chapter 3.7.1: *Maintain period*), if required.

A "period maintenance" is only then required if you want to change the default settings of the program system.

After pressing the [**Maintain period**] button, a dialog box opens in which the field "First day" contains the current system date - 1 month and the field "Last day" contains the current system date; the field "statement number" is predefined with 1.

If you want to collect the account data at another starting time and/or with another "Start" statement number, you have to change the default value accordingly.

Entering the starting time is only then required if you have not received so far any account data from your bank.

In the further program process, the date in the field "Last day" is always set to the current system date. In the field "First day" the last statement date + 1 day will be entered. (Exception: In the last collection procedure, it has been determined that the collected account data is not complete. In this case, the program leaves the date "First day" unchanged in order that the data still missing can also be received in the next collection session.)

If a statement for the bank code entered in the BPD file has already been saved with the statement number entered manually by you in the databases of the Cash Management module, thus this statement will be overwritten. For this reason, please pay always attention to the correct entry of the "Start" statement number.

In the further program operation, the statement number will be increased by 1 after each collection process.

(Exception: In the last collection process, it has been determined that the collected account data is not complete. In this case, the program leaves the statement number unchanged in order that the data still missing can also be received in the next collection process.)

Include your settings by clicking the [**Save**] button.

To be able to use the HBCI communication process, you have to ensure that you have allocated the generated HBCI bank parameter file on the *Banks property page* under –Reference tables- / -Banks- to the appropriate bank (see Chapter 7.1.1). You have to do appropriate allocations in the payment modules used.

Example: HBCI first access letter

Cologne, 23rd October 2003

F I R S T A C C E S S L E T T E R

Mrs.
Monika Mustermann
In der Lohn 43

12345 Musterstadt

OMIKRON HBCI Test bank
Von-Hünefeld-Straße 55
50829 Cologne

Phone : 0221 / 59 56 99 - 0
Fax : 0221 / 59 56 99 - 7

Dear customers,

To configure a new HBCI access, you require the following information

```
User-ID                UMCC0001
Customer ID           KMCC0001
Connection port:      3000
Internet address      123.456.789.012
```

Enclosed you receive the INI letter about the Public Key
of the bank for the Electronic Signature.

After successful initialization, please send your INI letter signed to the adress listed above in order that we are able to release your HBCI access.

This notification will not be signed.

Example: INI letter of the bank

Bank:

Key version	0
Key number	1
HBCI version	currently 2.01/2.10/2.20

Public key for the Electronic Signature:

[illegible]

Modulo										0768									
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
1B	D1	9E	2F	70	30	70	9D	9E	A1	66	99	57	A9	70	82				
07	2A	65	D7	BC	34	6E	94	23	BC	B5	61	A3	EB	00	63				
E5	D3	9C	3D	2D	E4	C8	41	CF	0D	5C	BC	49	1B	C9	8A				
8B	00	5B	DD	02	66	CF	06	20	28	37	BE	BA	47	E1	17				
1E	13	1F	E5	5B	70	7E	9C	5A	ED	56	9C	DA	A1	CD	7A				
F1	FD	02	4E	10	FD	74	A5	00	30	57	62	80	EC	CC	E7				

```
Hash
3A F3 85 0F BE 83 AD 76 2A E5
B7 4E 3B 71 2D 1E 8A D9 D2 24
```

3.7 HBCI+

For the communication with **HBCI+** (= HBCI with PIN/TAN extension) bank parameter files are also needed. The bank parameter files thereby are set up by you; the necessary data will be received from the banks, which provide this communication access. This flexible procedure, which works without further installations (like smart card readers and appropriate driver software), combines the security of a single use password (TAN) with the approved 128 bit transport encryption (SSL) of your browser.

To be able to use HBCI+, you have to take care of the fact that

- the "HBCI Plus communication module" has been installed,
- the "TCP/IP connection" procedure has been ticked on the *Priorities property page* on menu item - Communication- / -Comms. parameters-. On the *TCP/IP connection property page*, you have to decide whether the connection is made using dial up networking or LAN.

After clicking the [**New BPD**] button under -Communication- /-Bank parameter files-, selecting the "HBCIPLUS" procedure via list box and entering a name for the bank parameter file, a dialog opens to enter the access data.



Please note ...

The internal BPD file name may have max. 8 digits and may consist only of characters (A-Z,a-z,0-9,-,_,.).

Enter the received data similarly to HBCI into the fields of the following dialog box and confirm with [**Save**] afterwards.

Using the [**Change PIN**] button you can change the PIN of your HBCI+ access. For this, enter the new PIN in the appropriate field. In the field "check entry" repeat your entry for security reasons once again.

According to this you can [**Block PIN**] or [**Reset PIN block**] using the appropriate buttons in the HBCI+ access data dialog box. Additionally you can [**Maintain TAN list**], [**Order TAN list**] or [**Block TAN list**]. Using the [**Display TANs used**] button you can show all the TANs already used. With some banks it is necessary that you activate your TAN list. You can do this with the [**Activate TAN list**] button.

Your TAN list provided by the bank for an individual account using the [**Maintain TAN list**] button. With several users only the currently logged user can maintain its own TAN list. Further information can be found in Chapter 3.7.2: *Maintain TAN list*.

After pressing the buttons mentioned above you have to authorize yourself first by entering your account PIN (= your access password).

Some of the actions must be authorized by TAN entry. Please enter a valid TAN in the appropriate field and then confirm with [**OK**].

Results of the actions are shown in each case in a message window during communication.

If an action is not successful or the function is not supported on bank side, corresponding error messages will be shown.

Furthermore there are the following options in HBCI⁺:

Use TAN list of another bank parameter file?

Tick this check box if for several accounts of a bank only one TAN list was handed out and if this TAN list was stored for another account than the current account, for which you want to specify the access data.

From the selection list behind the check box you select the bank, for which a TAN list is already stored, which should also be used for the current account.

Use second TAN for transmission of payment orders?

If you tick the appropriate check box, the transmission of payment orders is authorized by input of a second TAN. The access to the second TAN is linked to a second user (with a second PIN). This means that in the user administration at least two users have to be registered, who have the right to send a payment order.

In the dialog box mentioned above you have to add the name of the second user from the user administration in the left column "MC user name" and the "User ID" in the right column. (The user ID of the second user normally is identical to the user ID of the first user.) Finally the data is stored in the program system by pressing [OK].

Each user has to store its own TANs, if it does not want to enter the TANs manually during a transmission.

Each user has only access to its own TANs, i.e. the user "1" from the example above will see only its own TANs when clicking the [**Maintain TAN list**] button. The user "2" only has access to its own TANs if it logs on accordingly and then clicks on the [**Maintain TAN list**] button .

How to send a payment order authorized by a second TAN?

For the first user nothing changes, i.e. after sending e.g. by clicking on [**Send file**] in the file manager its PIN will be prompted (and, if not stored, its TAN too).

As soon as the user 1 confirms its PIN entry with [OK], a new dialog box will be shown and the user 2 is prompted to enter its user name and its PIN.

If for everyone of the users the TAN list is stored and contains still a sufficient number of TANs, there will be no prompt for manual TAN entry. Even if both or only one TAN list are not sufficiently filled, the user-dependent dialog box for manual TAN entry appears. Enter a valid TAN and confirm with [OK].

Only if all conditions are fulfilled, the payment orders will be sent.

Using the [**Maintain period**] button you can change the collection period as well as the "Start" statement number of account statements (see Chapter 3.7.1: *Maintain period*), if required.

A "period maintenance" is only then required if you want to change the default settings of the program system.

After pressing the [**Maintain period**] button, a dialog box opens in which the field "First day" contains the current system date - 1 month and the field "Last day" contains the current system date; the field "statement number" is predefined with 1.

If you want to collect the account data at another starting time and/or with another "Start" statement number, you have to change the default value accordingly.

Entering the starting time is only then required if you have not received so far any account data from your bank.

In the further program process, the date in the field "Last day" is always set to the current system date. In the field "First day the last statement date + 1 day" will be entered.
(Exception: In the last collection procedure, it has been determined that the collected account data is not complete. In this case, the program leaves the date "First day" unchanged in order that the data still missing can also be received in the next collection session.)

If a statement for the bank code entered in the BPD file has already been saved with the statement number entered manually by you in the databases of the Cash Management module, thus this statement will be overwritten. For this reason, please pay always attention to the correct entry of the "Start" statement number.

In the further program operation, the statement number will be increased by 1 after each collection process.
(Exception: In the last collection process, it has been determined that the collected account data is not complete. In this case, the program leaves the statement number unchanged in order that the data still missing can also be received in the next collection process.)

Finally confirm your data in the HBCI+ access data dialog box with the **[Save]** button.

To be able to use the HBCI+ communication process, you have to ensure that you have allocated the generated HBCI+ bank parameter file on the *Banks property page* under –Reference tables- / -Banks- to the appropriate bank (see Chapter 7.1.1). You have to do appropriate allocations in the payment modules used.

The key to the **[Maintain period]** and **[Maintain TAN list]** buttons can be found in the corresponding Chapters on Definition of download periods and on Define TAN lists.

3.7.1 Maintain period (HBCI and HBCI+)



You need **only** define periods if you want to change the default settings assigned by the program.

After selecting the [**Maintain period**] button a dialog box appears which contains the fields "**First day**" and "**Last day**" which show the current system date; the "Start **statement no**" contains the default value 1 .

Change the default values correspondingly if you want to download account information at another start date and/or with another start statement number.

You need only enter a start date if you have not previously downloaded account information from your bank.

The date in the field "Last day" is always set to the current system date from now on. The last statement date + 1 day is always entered in the "First day" field.

(Exception: this is not the case if the system established during the last download that the account information downloaded was incomplete. In this case, the program keeps the "First date" unchanged, so that the missing data can be downloaded during the next session.



Any statement for the Sort Code entered in the BPD with the statement number you have entered manually in the databases of the Cash Management module will be overwritten. Please ensure that the **Start statement number is entered correctly**.

The statement number is increased by 1 after each download session from now on.

(Exception:

this is not the case if the system established during the last download that the account information downloaded was incomplete. In this case, the program keeps the statement number unchanged, so that the missing data can be downloaded during the next transmission.

Click on [**OK**] to save your entries.

3.7.2 Maintain TAN list (HBCI+)

"TAN" is the acronym for **Transaction number**. Entering a TAN protects your data from unauthorised changes and access by third parties during transmission. Together with your BTX PIN, TANs constitute your access rights for the T-Online host computer. One TAN is used up each time you transfer payment orders. No TAN is needed to download account data.

Your bank sends you TANs, normally 50 at a time, by post.
TANs are allocated to a particular bank and thus to a particular **Bank Parameter Data file**.

You can save your transaction numbers (TANs) in your system.
After selecting the [**Maintain TAN list**] a small dialog box opens in which you can enter your PIN.

For additional security, the TAN list for the BPD can only be opened if you enter the PIN assigned when the BPD was created. Then click on the [**TAN list**] button.

The first time you edit a TAN list, the table displayed can hold up to a maximum of 100 TANs.

Only a few bank data centres require you to assign a **TAN list number**. Your bank will notify you in such cases.

Each **TAN** consists of a 6-digit number.



Please ensure that all TANs are entered correctly as incorrect TANs can result in the Comms. session being cancelled.

Save the TANs you have entered by clicking on [**Save**]. If your bank has sent you more than 100 TANs, page to the next TAN entry page with [**Next page**].

3.8 ETEBAC3

Most French banks use the ETEBAC3 communication method for data transfer. ETEBAC3 is used to send payment orders to the bank and download account data.

Select the relevant menu item to edit the BPD file needed for ETEBAC3. The information you need to configure the ETEBAC3 BPD will be notified by your French bank.

You can only use ETEBAC3 for data transfer if you have installed the corresponding ETEBAC3 module.

For more information refer to

- Create ETEBAC3 BPD file
- Configure ETEBAC3 parameter cards



Please note:

The data you need to create an ETEBAC3 BPD will be supplied by your French bank on request (normally by fax). Before creating an ETEBAC3 BPD, you should therefore contact the customer services department at your French bank.

Incidentally:

The statements downloaded from the French bank using ETEBAC3 are saved in the main directory `..MCCWIN` under the name of the corresponding backup file (*.STA) as well as in the original format with the extension *.AFB.

Create ETEBAC3 BPD file

You must enter the appropriate data into the following boxes to create an ETEBAC BPD:

Description of BPD file

Enter an explanatory description of the BPD in the this box. The description you select will then be shown in all cases instead of the BPD file name.

User ID

Use this box to enter the Customer ID with which you must log in to some banks. The User ID will be supplied by your French bank (always in upper case).

Account

Enter the account number for your account at the bank in this box. The payment orders sent by online transfer are processed through the account number you enter here. You can also only download account data for the account you enter here. In some cases, an access number for the Electronic Banking service notified to you by the bank should be entered here instead of the account number. Your French bank will provide details.

TRANSPAC NUA

The program uses the Transpac Number (= Bank computer NUA) you enter here to establish a connection with the bank's gateway computer.

ISDN direct connection

Here you can decide via list box whether your connection to your bank is a ISDN direct

connection or not. If you choose "Yes", ISDN number of the bank can be given in the next field "ISDN no. of the bank". If it is set to "No", the indirect connection using a french PAD is chosen and two other fields have to be filled (see below).

ISDN no. of the bank

If the field "ISDN direct connection" is set to "Yes", this field appears, where you have to enter the ISDN number of your bank for point to point connection.

ISDN no. of TRANSPAC

If the field "ISDN direct connection" is set to "No", this field appears, where you have to give the ISDN number of the french PAD (TRANSPAC: 08 36 08 64 64).

X25 NUA of the bank (X25 B-canal)

If the field "ISDN direct connection" is set to "No", this second field appears, where you have to enter the X25 NUA of the bank. This is the same number as in the field "TRANSPAC NUA".

Bank dialog

The ETEBAC3 diskette provides predefined dialog files for communication with the French banks. The available dialogs are contained in the "Bank dialog" list box. Double-click to select the appropriate dialog from the list.

(The file name consists of an 8-digit abbreviation of the bank name.)

Transmission no.

Some banks require each Comms. session to be assigned a consecutive number related to the current date. Starting with the number "0", this value is increased by 1 after each successful transfer.

If your bank requires transfers for each day to start with a particular transfer number, enter the relevant start value in this box. Transfer numbers are then increased automatically. In such cases, you must reset the transfer number to the start value every day before starting a Comms. session.



For your information, the program enters the date on which the last successful transfer was made using the corresponding BPD in the "Last transmission on" box.

Last transmission on

The date of the last transmission is shown here.

Character set

Use the list box to select the character set which will be used for data transfer.

Choose between:

- EBCDIC (default)
- ASCII

Data interchange with French banks normally uses EBCDIC.

Comms. mode

Use the list box to specify whether a separator (<CR><LF>) must be inserted between individual records.

Choose between

- With pause (no <CR><LF>, default)
- With separator (<CR><LF>)

Data interchange with French banks normally takes place without <CR><LF>.

Pause after Comms

Depending on the bank involved, you can define pauses between the individual Comms. sessions. The figure you enter relates to a pause of 1/20 of a second (for example: if you enter a "5", this means that there will be a pause of 5/20 = 0.25 seconds).

The default pause is 5/20 second.

PCV

This field is only valid for X.25 connections and within France: Communication fees can be paid by the bank. To do this set parameter to "Yes" via list box.

User data field

Up to twelve alphanumeric characters can be entered here for your own purposes.

If necessary, click on [**Parameter cards**] to define specific data – if necessary - for file transfers.

If you have already found and configured an existing entry in the "Bank dialog" box for data interchange with a bank, it is not normally necessary to make changes in the parameter cards. You should only change the parameter cards if instructed to do so by your bank or if you are configuring a new bank using the Bank dialog.

Save the settings by clicking on [**Save**].

Configure parameter cards

The parameter cards supplied with each dialog type contain valid settings. Modifications will only be required in particular (exceptional) circumstances.

Parameter cards describe communication between the bank and customer systems for the various session types (e.g. transfer orders, direct debits, etc.). A parameter card contains exactly 80 alphanumeric characters which must be entered as specified by your bank. It is important that the entries are made at the specified positions, e.g. exactly at Position 11, 22 or 65, etc.

To improve transparency, the parameter description is split across 3 lines, whereby a max. of 40 characters can be entered in the first and third lines. The second line facilitates the exact positioning of the values to be entered. Enter the values needed for Positions 1 to 40 in the first line, and for Position 41 to 80 in the third line.

You can enter variables for the following values in the parameter cards:

- User ID
- Account no.
- Password
- Transmission no.

A key to which variable is used for which function is shown in the last line in the dialog box. At present, the

User ID	can be defined by	uuu ... uu
Account no.		aaa ... aa
Password		ppp ... pp
Transmission number		nnn ... nn

Once variables have been entered in the corresponding sections of the parameter cards, the entries in the first dialog box for creating ETEBAC3 BPDs are automatically transferred to these positions during data transfer.

**Please note:**

The variable "p" for defining the Comms. password is an exception to the arrangement described above. This variable must **always** be entered in the parameter card as specified by your bank. During the Comms. session, this variable will be replaced by the password which you enter.

In the current program version, parameter cards can be defined for

- Account statements
- Domestic transfers
- Direct debits
- LCR collections (computerised bill of exchange statements)
- International payments
- Receive log file
- Send free text
- Receive free text
- Collect return clearing information
- Collect LCR payment statement (computerised bill of exchange statements)
- Send LCR statement answer
- Send VSOT
- Collect clearing status

Open the following parameter cards each by clicking on [**Next**] on the first page of the parameter cards dialog box or at the bottom of the parameter cards. Finish scrolling on the last parameter card by pressing [**OK**].

3.9 WOP

WOP (**Web Ongum Portal**) is a procedure used in the savings banks group for the file transfer via Internet.

The information needed to configure the WOP BPD file will be supplied by your savings bank. One exception is the "**Bank parameter data file description**" field, in which you should enter an explanatory BPD file description. This description will then always be shown instead of the BPD file name.

The following boxes are available for generating an WOP BPD:

Proxy server:

Usually the access to the Internet from local firm networks is made by a proxy server. If an existing proxy server should be used, tick the "**Use proxy server?**" check box. If this check box is activated, you can add "**Address**" and "**Port**" of the Proxy server in the next fields.

Encryption information:

"Encryption information" provides information on whether customer or bank encryption has been specified

Connection information of bank:

Use the "**URL of the bank**" field to enter the Web address of the bank server or of the server in the associated IT centre.

Information on bank:

The **Customer ID** defined by the bank identifies the customer in all Comms. sessions. The **Host name** and the **bank parameters** will be provided by your bank. The "Bank parameters" box contains a character string consisting of a combination of letters and numbers (cf. Chapter 3.3: *FTAM*).

Matching Internal User and Bank user no.:

The matching of "**Internal**" user (within the system) and "**External**" name (at bank) should be made as described for FTAM. Also up to 512 authorized signatories can be stored in one BPD file.

Use the [**New user**] button or the context menu entry –New entry of user – to add new users (from the available ones on the PC) to the BPD file (a new record will be created). Click the list or use the context menu entry –Maintain record - (right mouse button) to open the list of available users. Use -Delete- and confirm the security prompt with [**Yes**] to remove user entries from the BPD file.

In addition, it can be defined for each user whether the Comms. password should be saved in the bank parameter file. To do so, choose either "Yes" or "No" from the list in the column "**Save Comms. password**".

In the "**S**(ignature) **class**" column that signature class is entered by the bank side, which was defined there for the respective customer.

After successful initialization the ES version used by the respective customer is shown in the "**Current ES version**" column.

Click on [**Change Comms. password**] to change the Comms. password, which is stored in the BPD (cf. *FTAM*).

Then confirm your entries by clicking on [**Save**].

Use the [**Session types**] button to define the session to be available and/or whether an encryption should be enabled. The information is used for the creation of Comms. batches. Select the wanted session type from the list box containing all possible session types. Add this session type to the table below by clicking on [**Add this session type**]. Continue doing this until you have entered all the session types you want in the table. You can then specify for each session type whether encryption should be activated or not. Confirm your entry with [**Save**].

Click on [**Save**] to save the settings to the Bank Parameter Data file.

Table of Contents: Chapter 4

	Page
4 Special communication functions	4-2
4.1 Change Comms Password (Session type PWA)	4-3
4.2 First initialization of bank access (Session type INI)	4-5
4.3 Reset EPFT/MCFT communication access (Session type RES)	4-10
4.4 Block a Comms. access (session type SPR)	4-13
4.5 Encryption for FTAM/FTP transmissions	4-15
4.5.1 Activate encryption with banks	4-16
4.5.2 Encryption return codes	4-21
4.6 Convert FTAM/FTP bank access to EBICS	4-22
4.7 Exchange EBICS authentication keys	4-26
4.8 Change EBICS Comms. password	4-31
4.9 Key media administration wizard	4-32
4.10 Manage certificates	4-34
4.10.1 Generate system key and certificate	4-35
4.10.2 Generate TLS key and certificate	4-36
4.10.3 Generate certificate request	4-39
4.10.2 Import certificate	4-41
4.10.3 Assign certificate	4-42

4 Special communication functions

The special functions for the Comms. parameters comprise functions only used occasionally for the administration of your Comms. access such as

- Change Comms Password
- First initialisation of bank access(INI)
- Reset bank access(RES)
- Block a Comms. access.

You can use the

- Encryption

option if you are using FTAM or FTP for dial-up communication.

For EBICS -besides some functions, which are integrated in the common wizards (First initialization, Blocking)- some special functions are available in separate menu items:

- Convert FTAM/FTP bank access to EBICS
- Change EBICS authentication keys
- Change EBICS Comms. password

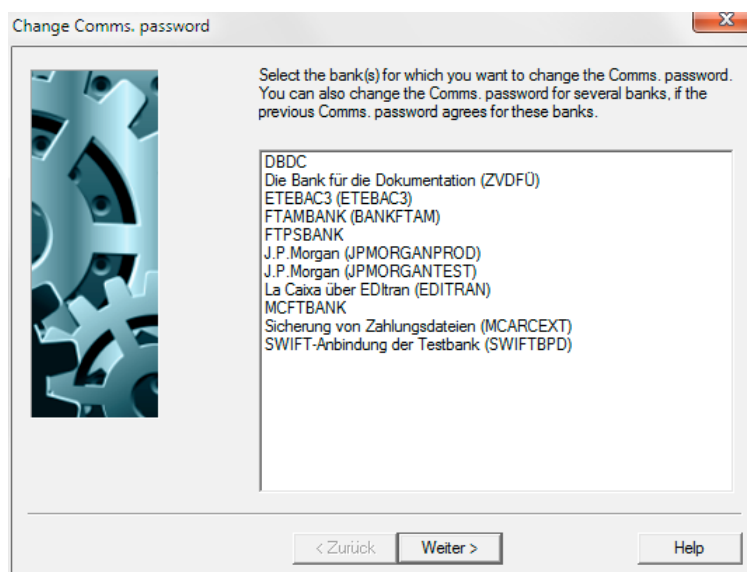
4.1 Change Comms Password (Session type PWA)

Select the menu item -Change Comms Password- in the Communication menu to change an existing Comms. password.

A wizard will guide you through the steps that need to be taken when changing the Comms. password:

1 Select the bank(s)

All the banks that are saved in the system which allow you to change your password are shown in a list. Click on the bank for which you want to change the Comms. password. You can change the Comms. password for several banks, if, for example, the current Comms. password is the same for these banks. Then press **[Next >]**.



2 Enter current and new password

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 change of password.

Use the TAB key to jump to the next box and then enter the new password. This will be used for future communication sessions after it has been successfully sent to the bank.

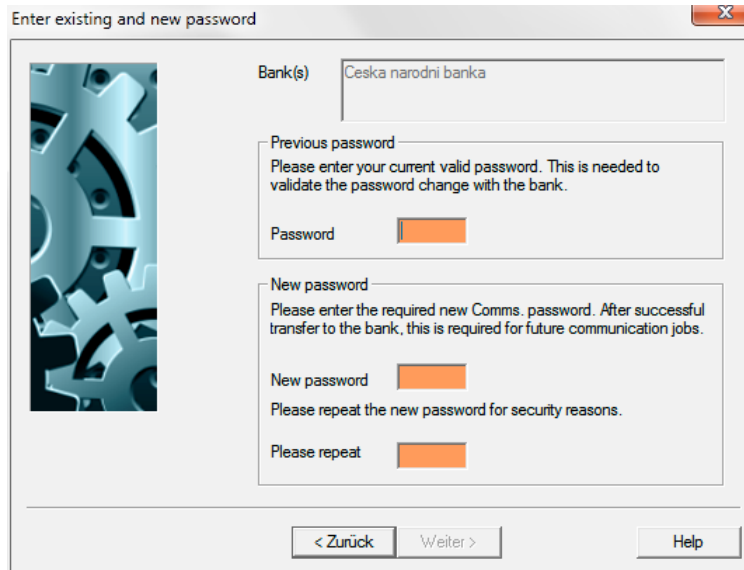
Because password definition is concealed, i.e. when you press a key you only see an * (asterisk) on the screen, you must repeat the new password in the appropriate field for your own protection.



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.

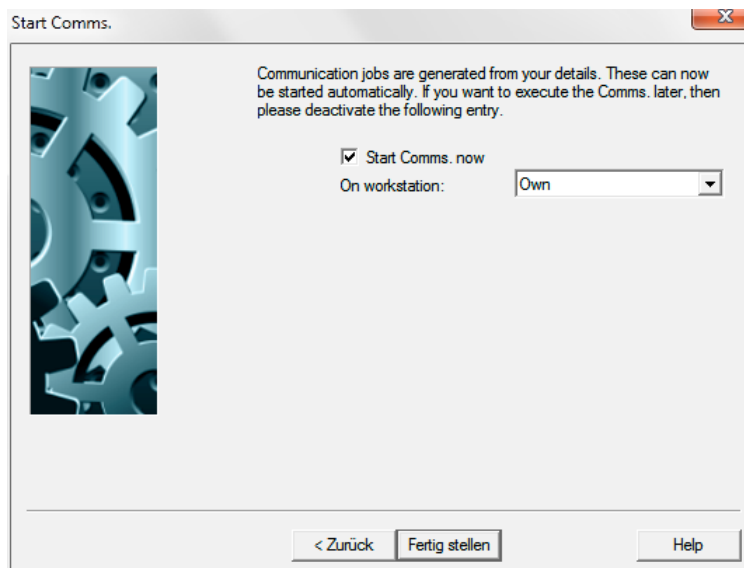
Close password definition by clicking on **[Next >]**.



3 Start communication

A Comms. session file is generated from your entries. Comms. can be started automatically during this last step if you confirm the default entry using the [**Complete**] button. If you do not wish to start the Comms. immediately, you will have to deactivate the entry "**Start Comms Now**".

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.



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

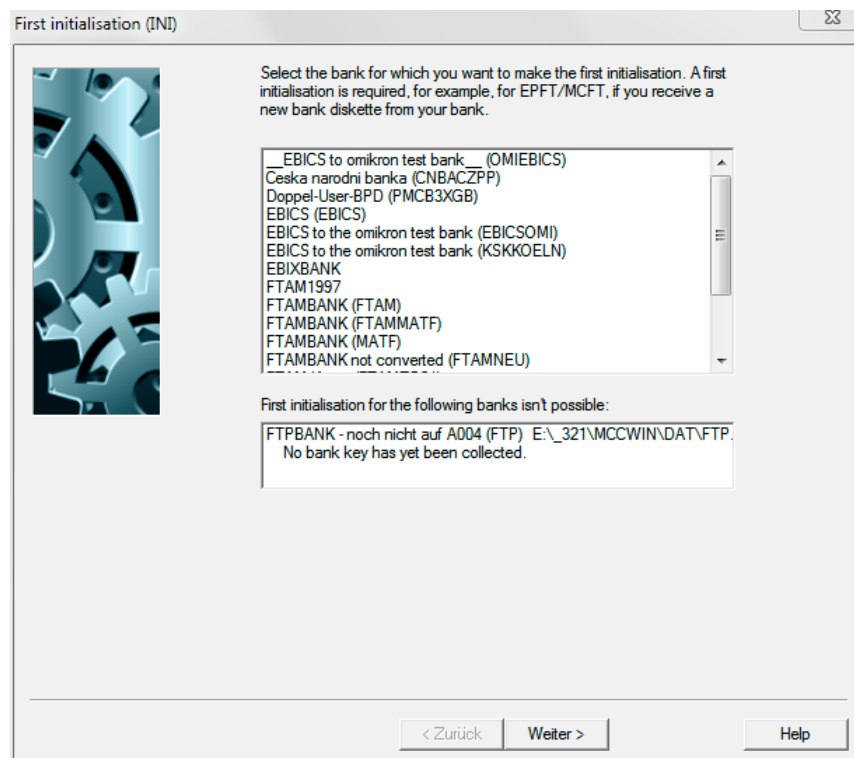
4.2 First initialization of bank access (Session type INI)

Select the menu item -First initialisation (INI)- in the Communication menu to initialise access for the first time. First initialisation is, for example necessary for EPFT/MCFT when your bank provides you with a new bank disk.

A wizard will guide you through the steps that need to be taken to carry out first initialisation. A message asks you to insert the appropriate bank disk.

1 Select the bank(s)

Click to select the bank(s) from the list for which first initialisation is to be carried out. Then press [**Next >**].



Banks, for which a first initialization is not yet possible, appear in a second list together with a notice on the cause, e.g. "No bank key has yet been collected".

2 Enter current and new password

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 initialisation.

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. If necessary a second password must be entered and its new entry must be repeated likewise.

**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 [**Next >**].

Enter previous and new password

Bank(s)

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

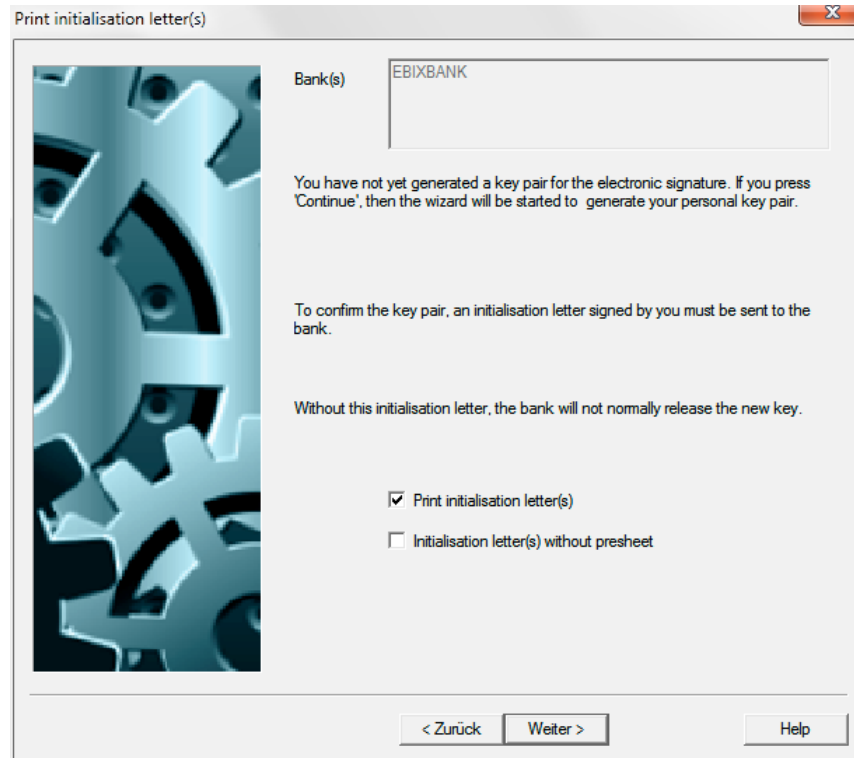
< Zurück Weiter > Help

only for EBICS:

If the user status deviates from "New" or "Disabled", a warning appears here for EBICS. Otherwise, step 3 follows directly.

3 Print initialization letter(s)

You will have to send a signed initialization letter to your bank (or several banks) to confirm a (already generated) 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 INI letters to be printed, leave the default box **"Print INI-Letter(s)"** checked.



Print initialisation letter(s)

Bank(s) EBIXBANK

You have not yet generated a key pair for the electronic signature. If you press 'Continue', then the wizard will be started to generate your personal key pair.

To confirm the key pair, an initialisation letter signed by you must be sent to the bank.

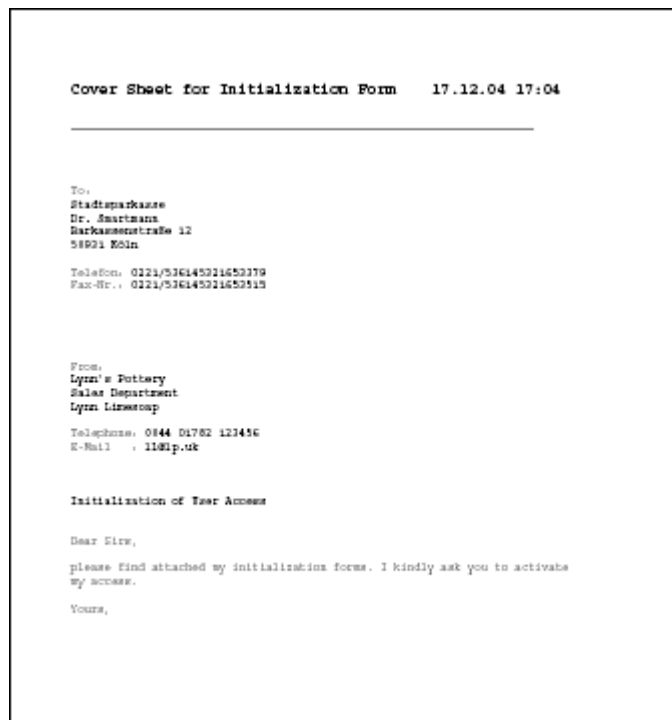
Without this initialisation letter, the bank will not normally release the new key.

☒ Print initialisation letter(s)

☐ Initialisation letter(s) without presheet

< Zurück Weiter > Help

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



Cover Sheet for Initialization Form 17.12.04 17:04

To:
Stadtsparkasse
Dr. Smartmann
Barkassestraße 12
50921 Köln

Telefon: 0221/53614531653379
Fax-Nr.: 0221/53614531653319

From:
Lynn's Pottery
Sales Department
Lynn Limescop

Telephons: 0844 01782 123456
E-Mail: l1@ip.uk

Initialization of User Access

Dear Sirs,

please find attached my initialization forms. I kindly ask you to activate my access.

Yours,

If the cover sheet should not be printed each time for the same bank at the first initialization of several users, you can inhibit the generation by ticking the **"Print INI-Letter(s) without cover sheet"** check box additionally.

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

If you have not generated a keypair yet, first the wizard for keypair generation is started afterwards (see Chapter 6.1: *Generate / Send ES keypair*).

If you have not generated any key pair for the bank-specific signature, subsequently to this the wizard/dialog for the key pair generation or for the import of the public keys from the signature medium is started first (see Chapter 6.1: *Generate / Send ES key pair*).

4 Generate signature keys

If you have not generated any key pair for the bank-specific signature, subsequently to this the wizard/dialog for the key pair generation or for the import of the public keys from the signature medium is started first (see Chapter 6.1: *Generate / Send ES key pair: Key generation*).

Generate EBICS authentication keys (only for EBICS)

If you have not generated any A- and V-keys, you can do this on this page. In the dialog box, the checkbox "**Generate new authentication key**" has already been highlighted. If you want to generate a new key pair for the EBICS authentication, unchange this presetting.

If, however, already existing keys (e.g. generated earlier) should be sent to the bank(s), untag the checkbox.

If, however, already existing keys (e.g. generated earlier for another bank) should be sent to the bank(s), untag the checkbox. Please enter your currently valid Comms. password for the authentication key in this case.

In case of the highlighted option, the new keys are subsequently generated. Please allocate a new password for the access to the keys. It is later used as "**Comms. password**". 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 appropriate field.

If you have highlighted the checkbox for the key pair generation, you must enter below the field for the password entry any character string consisting of exactly **32 characters**. These characters should be chosen as randomly as possible. The entry is made concealed, i.e. each entered character is displayed by an * (asterisk). This optionally selectable character string builds the basis for the creation of the key pair.

Use the checkbox "**Also collect current bank key (HPB)**" to collect the bank keys. This is only necessary if for this BPD file still no bank keys are available. If the status of the bank keys is set in the BPD file to "Ready", the checkbox for collecting the bank keys is predefined without highlight and deactivated.

Click finally on the [**Next >**] button.



Please note:

If you have ticked the "**Generate new authentication key**" check box, although already valid keys exist, a warning message appears afterwards.

If you continue here, you have to send the new key pair also to your already activated EBICS banks afterwards, otherwise you cannot continue working with these banks any longer.

You can go back here to the previous page and remove the tick from the check box if necessary.

5 Enter the hash values of the bank keys (only for 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 appropriate 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".

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.

For EBICS, the following communication jobs are automatically generated by the wizard and included in the file manager:

INI,

HIA (Transmission of the user public keys for authentication and encryption) and

HPB (Collection of bank keys)

Comms. can be started automatically during this last step if you confirm the default entry using the [**Complete**] button. If you do not wish to start the Comms. immediately, you will have to deactivate the entry "**Start Comms Now**".

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.

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

For EBICS, the communication jobs INI and HIA are immediately executed after pressing the [**Complete**] button.

The bank keys can only be collected if the user is activated on bank side. In this process, the hash values of the bank are only kept once per BPD file (i.e. not per user) and are automatically reconciled and activated as far as they have already been stored in the BPD file.

For this reason, the HPB order is included by the wizard with the status "Waits for Comms." in the file manager (only if no bank key is available) so that it can simply be executed there after the activation. An appropriate note is displayed for the user.

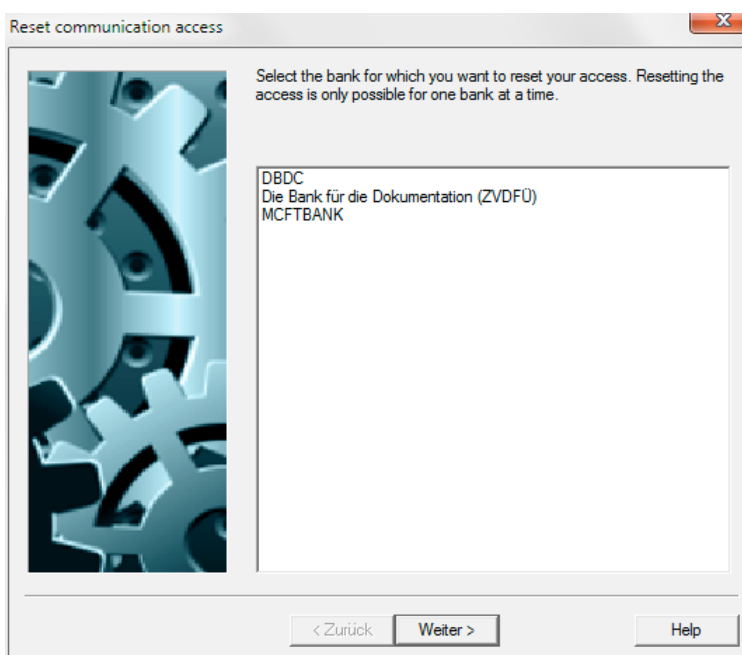
4.3 Reset EPFT/MCFT communication access (Session type RES)

Select the menu item -Reset EPFT/MCFT communication access- in the -Communication- menu to reset the bank access.

A wizard will guide you through the steps that need to be taken to reset bank access. Resetting can only be effected for one bank at a time.

1 Select the bank

Click to select the bank from the list for which access is to be reset.



Then press [**Next >**].

2 Print initialisation letter / Reset with signature

You will have to send a signed initialization letter to your bank to confirm the reset. Access will normally not be released by the bank until such time as the initialization letter has been received. Therefore you are advised to leave the option box "**Print initialisation letter**" checked.

Below this you have to enter the valid Comms. **password**. It is required to authorize the reset at the bank.

Enter the Comms. password in the corresponding field. The password entry is concealed, i. e. each key-stroke is shown by an * (asterisk).

Reset communication access

Bank: Doppel-User-BPD

To confirm the reset, an initialisation letter signed by you must be sent to the bank.

Without this initialisation letter, normally no release of the access is made on bank side.

☒ Print letter

Current password:
Please enter your current valid password. This is needed to validate the reset of your Comms access with the bank.

Password: [Orange box]

< Zurück Weiter > Help

If supported by the bank system, the **reset** can be activated directly **via signature** directly. Mark the second option for this. Then enter the **"ES password"**.

Furthermore you have to enter the new Comms. **password** for your future Comms. orders. The password must be **repeated** for security reasons.

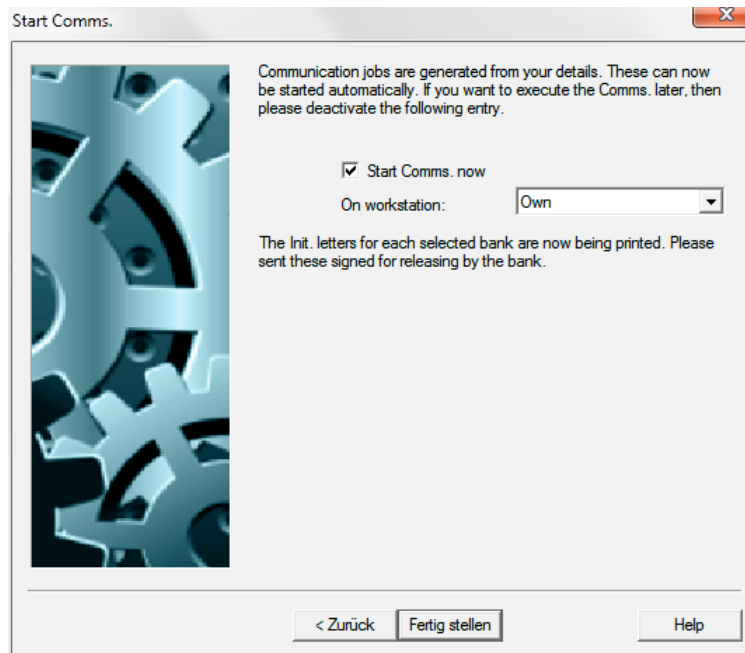
If the signature can be verified by the bank system, the keys and the new Comms. password are updated in one step, without manual interaction on bank side.

Close this page by clicking the **[Next >]** button again.

3 Start communication

A Comms. session file is generated from your entries. Comms. can be started automatically during this last step if you confirm the default entry using the **[Complete]** button. If you do not wish to start the Comms. immediately, you will have to deactivate the entry **"Start Comms Now"**.

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.



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

Initialization letters will then be printed for each selected bank. Please sign this letter and send it to your bank to release access.

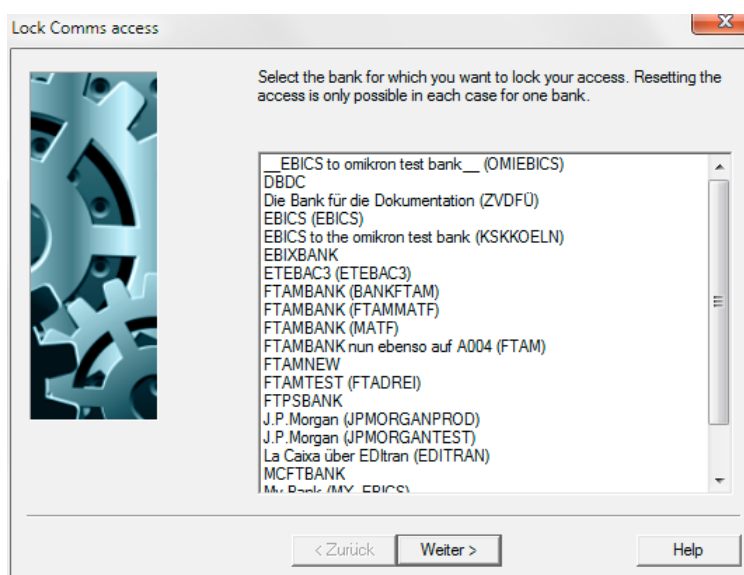
4.4 Block a Comms. access (session type SPR)

To block a bank access, choose menu item – Block a Comms. access – in menu -Communication-.

A wizard guides you through the necessary steps required to block a Comms. access to the bank. The blocking is only possible for one bank.

1 Choose bank

Choose the bank from the list by a mouse click, for which you want to block the Comms. access. Click then the [**Next >**] button.



only for EBICS:

If the user status deviates from "Ready", a warning message appears here for EBICS. Otherwise, step 2 follows directly.

2 Blocking the Comms. access

For EBICS, the blocking session must be signed by the user to be blocked. Enter therefore in the area "Signing user block" your currently valid **"ES password"** for the Electronic signature in the appropriate field. The prompt for the ES medium is made in the last step (-> **3**) of the wizard. Below the chosen bank(s) you must enter the valid Comms. **password**. It is required to log on the blocking at the bank.

Enter the Comms. password in the corresponding field. The password entry is concealed, i. e. each key-stroke is shown by an * (asterisk). Close the password entry by clicking the [**Next >**] button.

3 Start communication

Comms. batches will be generated from your entries. These can be automatically started in the last step if you confirm the predefined entry using the [**Complete**] button.

If you want to execute the Comms. later, please deactivate the entry "**Start Comms. now**".

If you work in a network environment, you can choose a PC intended specially for communication jobs using the list box "**On workstation:**" and start there the communication.

Use the [**< Back**] button to go back each time to the working steps in order to enter changes, if necessary.

4.5 Encryption for FTAM/FTP transmissions

The EPFT/MCFT procedure features automatic data encryption. You have the option of encrypting your data when transmitting it using FTAM or the data will be generally encrypted like with FTP. The encryption method used here is a hybrid method based on a combination of DES and RSA. The messages to be transferred are encrypted using DES, and the DES key used is encrypted using RSA and transferred in a message header record.

Further information on the subject of the encryption of data transmitted using FTAM/FTP is contained in Chapter 1.2.3: *FTAM*. Here will you also find a chart illustrating the encryption workflow.

A requirement for data encryption is that the recipient of the encrypted data must inform the sender of this data of the public key of his RSA encryption keypair. You must notify your bank of your public key using session type **VPK** (Transmit Customer public key).

The bank's public key is notified to you using session type **VPB** (Transmit Bank public key) by the bank.

The parameters you need to set for encryption which can be found in menu item -Parameters-, -Encryption-, are explained in the following chapter:

Chapter 4.5.2: *Activate encryption with banks*

You can find special return codes concerning encryption in

Chapter 4.5.2: *Encryption return codes*

4.5.1 Activate encryption with banks

Selecting menu item Communication / -Encryption- generates the keypair needed for RSA-encrypted transmission of the DES key in the same way as described for the Electronic Signature (see Chapter 6.1: *Generate / Send ES keypair*).

A Wizard will guide you through the steps that need to be taken to activate encryption.

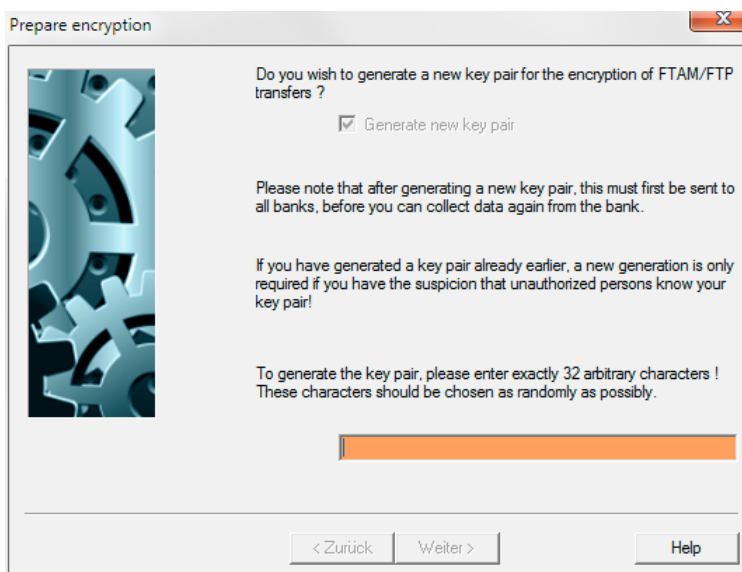
1 Generate a new keypair



Please note:

If you have already generated a keypair, it will only necessary to generate a new keypair if you suspect that an unknown third party has acquired access to your keypair.

To calculate the keypair, enter an arbitrary character string 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 freely-selectable character string forms the basis for generating the keypair and should therefore be selected as randomly as possible. A message tells you if the character string contains less than 32 characters. Confirm your entry by clicking on [**Next**].



Both key components (secret and public key) are encrypted using the internal user ID and a timestamp and saved on your hard disk in directory ..\MCCWIN\DAT. Use parameter entry (V_KEY_DRIVE) in control file CSUB.PRO to save the secret key on another drive.

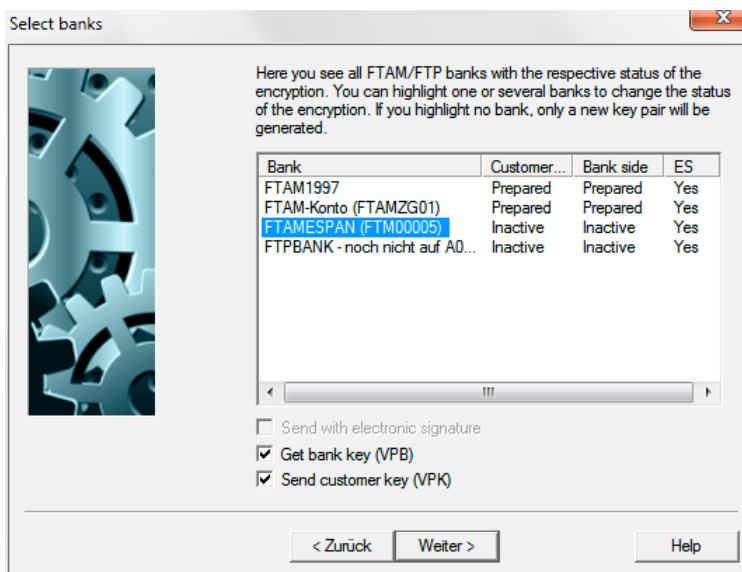


Normally, you do not need to regenerate a keypair to use the program. If you change the key, you must notify this change to all banks with which you communicate using a VPK session i.e. after generating a new keypair, **you must send it to all banks before you can download data from your bank.**

2 Select the bank(s)

A list of FTAM-(FTP-) banks is available for which a "VPK"- or a "VPB"-Comms. session should be generated automatically. The respective encryption status is shown. Triple DES is the default encryption method used with the bank.

Click to select the bank(s) from the list for which you want to generate a keypair. You can check one or more banks for the purpose of changing the encryption status. Only one keypair is generated if you do not select a bank.



You can only check "**Send with Electronic signature**" if you have also installed the **ES** supplementary module (= Electronic Signature) and want to send the data to the bank using FTAM (FTP). Information on the ES is contained in the documentation on the Comms. module (Chapter 6: *Electronic Signature*).

If you wish to sign a file before sending it, check the box in front of "Send with electronic signature" (standard setting).

The further checkboxes "**Get bank key (VPB)**" and "**Send customer key (VPK)**" are predefined according to the current encryption statuses (customer / bank side) and, however, can be adapted as and when required. This option exists only then if exactly one bank (parameter file) has been chosen. As soon as more than one bank is marked, the two check boxes are not available, since communication orders will then be generated automatically according to the status of the BPD.

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

3 Enter Comms. password

You have to enter the current Comms. password below the selected bank(s). This is needed by the bank to verify the change of key.

The file saved on the hard disk must be protected by a Comms. password so that it can be sent to your bank via Comms.

This Comms. password is known only to you and is specified on installation of the communications link between your computer and the bank.

If necessary, you can change the Comms. password at any time.

You can only specify and change the Comms. password in the Comms. program in the Core module. Information on this is contained in the Comms. module documentation (see Chapter 5.1.1: Database overview File Manager: *"Password and execution date" property page*).

If you have selected several banks, you determine by ticking the **"Use the same Comms. password for all banks"** check box, that for all banks the same Comms. password is used. Otherwise you leave this option unchecked. Then for each selected bank the current valid Comms. password is prompted afterwards.



Please note:

The bank (parameter file) can only be displayed above the password entry box if the field "Description of bank parameter file" has been filled in the respective bank parameter file.

Enter the Comms. password in the corresponding box. The password definition is concealed, i.e. when you press a key you only see an * (asterisk) on the screen. Close password definition by clicking on [**Next >**].

4 Enter ES password

As long as you have checked parameter "With Electronic Signature" (see above), entry of the Comms. password is followed by the entry of the password for the Electronic Signature.

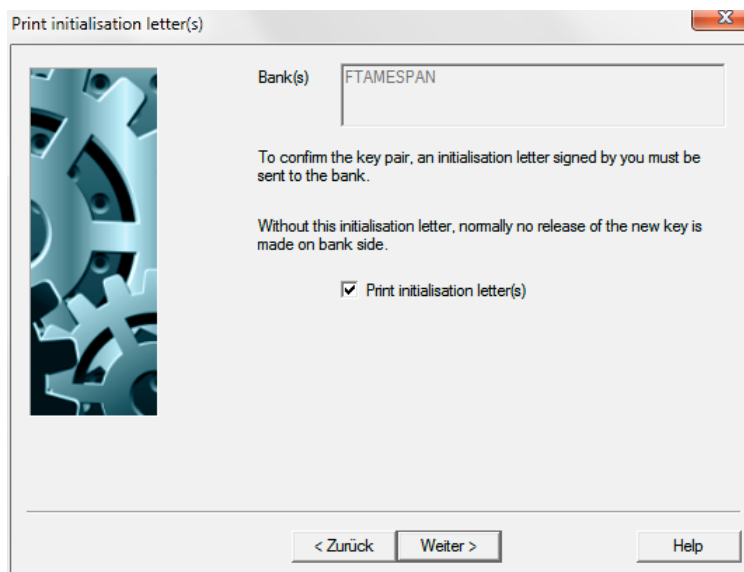
Before you enter the Electronic Signature, you are prompted to enter the ES password. You chose the **ES password** when generating the keypair for encrypting the private key on the key diskette (see Chapter 6.1: *Generate / Send ES keypair*).

Confirm your entry by clicking on [**Next >**].

5 Print initialization letter(s)

You will have to send a signed initialization letter to your bank (or several banks) to confirm a (already generated) keypair. Access will normally not be released by the bank until such time as

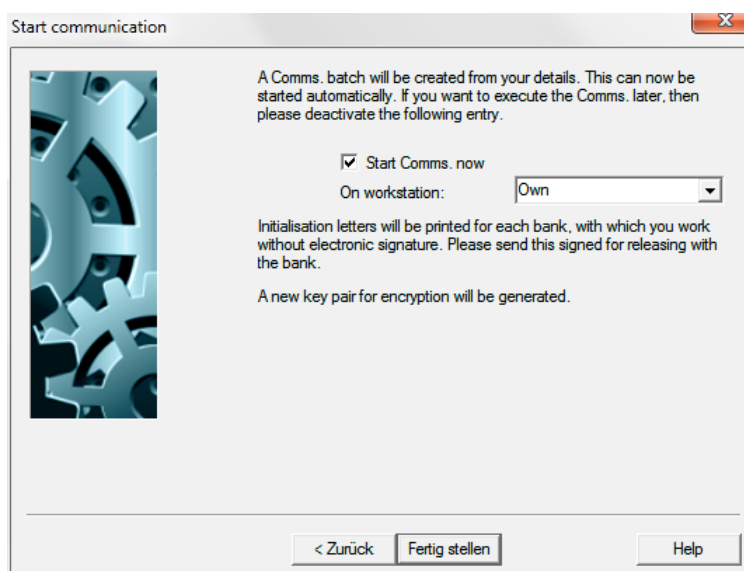
the initialization letter has been received. If you would like the INI letters to be printed, leave the default box "**Print INI-Letter(s)**" checked.



If you would like to print no initialization letter(s), please remove the check accordingly.

6 Start communication

A Comms. session file is generated from your entries. Comms. can be started automatically during this last step if you confirm the default entry using the [**Complete**] button. If you do not wish to start the Comms. immediately, you will have to deactivate the entry "**Start Comms now**". 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.



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

The new keypair for the Electronic Signature is then generated Insert a **formatted disk** and close the message with [**OK**]. If a private key has already been save on the disk, a message appears asking you if you really want to overwrite this key. Select [**Yes**] to overwrite the existing

key. Should you not want to do this, select [**No**] and insert a new disk.



Always keep the key disk in a secure place!

You are then prompted to insert the key disk into the disk drive defined when the ES module was installed so that the key disk can be verified using the ES password.

Communication starts after you have clicked on [**OK**] and have entered the Electronic Signature.

The Comms. sessions for sending public keys are generated temporarily and then deleted once the Comms. session has been completed.

As soon as the bank has been able to authenticate the (new) VPK, the data prepared by the bank is encrypted using your (new) VPK and you are released for the download sessions agreed with your bank. The bank public key is saved in the BPD file on your hard disk.

If the VPK session is not successfully authenticated, the bank sends return code 54 "Encryption code must be resent" when you try to download an encrypted session type from your bank. The bank will also contact you separately to rectify the problem.

If all sessions for activating encryption have not yet been performed (e.g. because the line is permanently busy), a message tells you to reselect the menu item -Encryption-.

Acknowledge subsequent messages (such as the creation of a Comms. batch to sent the key at a later time) by clicking on [**OK**].

Initialization letters will then be printed for each selected bank, with which ES should not be used. Please sign this letter and send it to your bank to release the keypair.



Please note:

As soon as encryption with a bank has been activated, all session types can be transmitted in encrypted form, apart from the ES files and the session types listed below. The session types which are sent in encrypted form is the subject of a separate agreement between you and your bank. This is ultimately relevant for download sessions only, as you can send transmission sessions to the bank in encrypted or unencrypted form.

The following (administration) session types are transmitted in unencrypted form:

ID	Description
INI	Password initialisation
PUB	Send public key for signature verification
PWA	Password change
SPR	Block access rights
VPB	Download bank public key for encryption
VPK	Send customer public key for encryption

4.5.2 Encryption return codes

The following encryption return codes are issued by the bank. They trigger off the actions described below on the customer computer, as long as the customer computer uses version "A3" of the application protocol in the FTAM remote file name. (Older customer systems using version code "A2" generally do not receive these return codes.)

50 Action successful - Fetch new Bank Parameter data

New Bank Parameter data is available for downloading on the bank computer. Your system automatically generates a BPD download session and tells you that the download session will be started automatically.

51 Encryption code with the bank must be updated (session type VPB)

A new public key was generated on the bank computer, which must be downloaded by your system. You are informed about this by the message "Please start menu item -Activate encryption with bank-". You cannot send any (encrypted) data to the bank until you have downloaded the new public key from the bank.

Return code 51 may also be returned by the bank if the hash value of the bank public key (VPB) used in the FTAM remote file name does not match the hash value expected by the bank. In such a case, you must also download a new public key from the bank.

52 Data must be downloaded in encrypted form

This message will only appear if you try to download data in unencrypted form despite activated bank encryption.

53 Data must be downloaded in unencrypted form

This message will only appear if you try to download data in encrypted form although it is provided by the bank in unencrypted form.

54 Encryption code must be resent (VPK)

After the VPK session and the associated validation request has been successfully sent, the customer computer assumes that the corresponding authentication has been performed by the bank with a positive result. However, if the result of the bank's signature validation of the VPK file is negative, your system receives return code 54 when you try to download encrypted session types.

55 User does not have ES permission

This message is returned by the bank computer if it emerges that the authorised signatory for a VPK file sent with an Electronic Signature does not have signature authorisation from the bank. This can also be established when the file is transferred, as the user ID of the signatory is transferred in the FTAM remote file name.

56 Encryption code not yet released

You will receive return code 56 each time you try to download encrypted session types until such time as the customer public key has been authenticated by the bank.

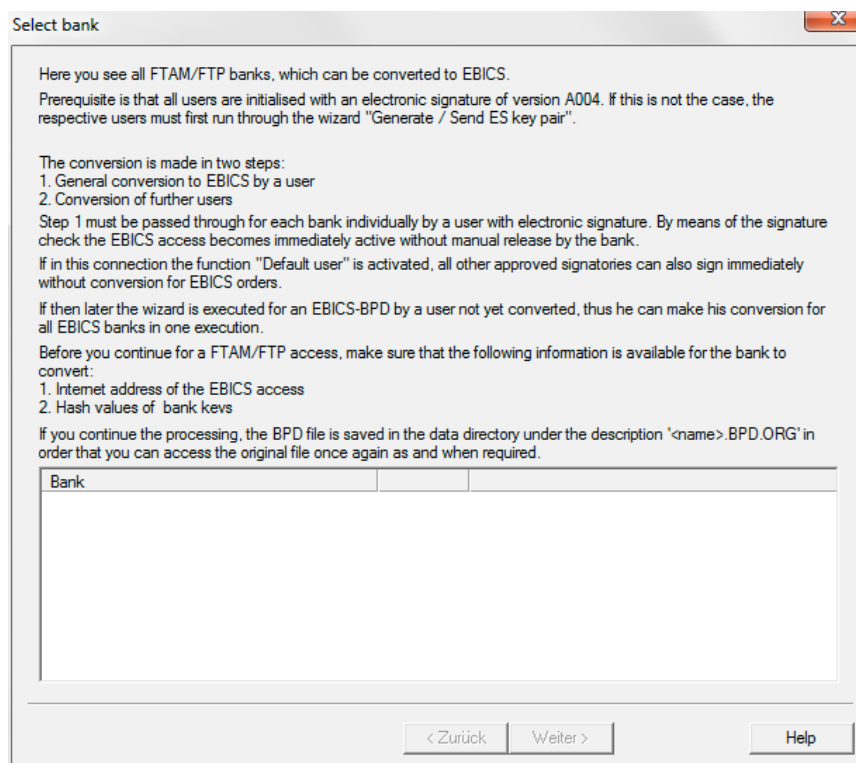
4.6 Convert FTAM/FTP bank access to EBICS

To convert an existing FTAM/FTP bank access to EBICS, choose menu item -Convert FTAM/FTP bank access to EBICS- in the -Communication- menu.

A wizard leads you through the necessary steps in order to execute the conversion. First you are prompted to choose the bank to be converted.

1 Select bank

Choose a bank via a mouse click from the list of banks which can be converted to EBICS (FTAM-/FTP-BPDs with ES version A004 as well as EBICS-BPDs with user status unequal to "Ready" or "Blocked").



The migration wizard must be passed through for each FTAM or FTP bank **individually**. If you choose more than one bank, an error message appears:



Please note:

Prerequisite for a conversion is that the respective user is initialized at the bank to be converted with **an Electronic Signature of version A004**. If a conversion to A004 has not taken place before, thus later an adequate EBICS status can only be achieved by blocking the old access and first initialization of the new access.

The conversion procedure need to be executed only by one user, provided that the remaining users accomplish signatures only. After the conversion, these users can directly continue to work. If they should become full EBICS users, i.e. they also can create communication jobs themselves, each of them has to pass through this wizard.

In this case, several already converted (e.g. by a first user) EBICS bank parameter files can be chosen.

Subsequent to this, the new authentication keys are transferred with Electronic Signature so that the access becomes immediately activated without release by the bank.

Press subsequently the [**Next >**] button. The converted bank parameter file is saved in directory ..\DAT under the description <BPDNAME>.BPD.ORG in order that you can access once again this original file if required.

2 Setup Comms. parameters (proxy settings for EBICS)

If you have to use a proxy for the access to the internet, highlight the corresponding checkbox. The necessary details on the **address** and on the **port** of the proxy are provided by your administrator. Furthermore, a **user name** and a **password** can be entered for the access to the proxy.

The proxy settings are only offered for entry if they have not yet been defined in the Comms. parameters (see Chapter 2.6: *TCP/IP connection property page*). The details entered in the wizard are saved in the Comms. parameters and are no longer prompted for the next execution of the wizard.



Please note:

If you want establish the Comms. link using a Comms. network, please cancel the wizard here and configure this first on the property page mentioned above.

Complete the entries by pressing the [**Continue >**] button.

3 Define EBICS communication address

Use the [?] button to open a list of known EBICS access data.

If a suitable access is contained in the alphabetical list, you can choose it and add the access data to the bank parameter file by clicking on the [**Save**] button.

If the bank access is not contained in the list, enter the internet address intended for the EBICS communication of the respective bank in the field "**Address (URL)**". This can be taken from documents provided by the bank.

Additionally, the **host name of the bank** (for the EBICS process) is to be entered. With older releases (before version 3.21.005) the EBICS host name is to be entered before the conversion directly in the bank parameter file, if the EBICS host name is different from the FTAM/FTP host name.

You complete the address entry by pressing again the [**Next >**] button.

4 Define default user (=technical user)

In large-scale companies, Electronic Banking specific jobs as payments entry and creation or execution of Comms. jobs as well as their authorization with ES are often executed by different persons. This organizational structure is explicitly supported in the EBICS procedure by the introduction of a "technical user" who is intended only to execute Comms. jobs.

In the program, you can label for this a user as "Default user". If in the bank parameter data a user is labeled as default user, his ID, his password and his authentication keys are used for each Comms. job which any other user can create. With it, the transport is completely separated from the current user and also users who are not entered in the BPD file can include Comms. jobs.

By ticking the checkbox "**Define current user as default user**" at the bottom of the page, you define yourself as default user. After executing the wizard, your Comms. password is saved in encrypted form and predefined for each communication job. Thereby, all other users can immediately continue to work without having to execute the conversion to EBICS themselves.

If you do not define any default user, all other users must also execute this wizard. The settings for the default user can also be later converted in menu item -Communication- / -Bank parameter files- in the bank parameter file (see Chapter 3.5: *EBICS*).

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

5 Enter the hash values of the bank keys

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".

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.

6a Generate EBICS authentication keys (for the first execution of the wizard)

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).

In the area "**Electronic Signature**" you must confirm the new key pair with your Electronic Signature. With it, the release of the key is directly authorised on bank side.

For this, enter your "**ES password**" in the corresponding field. The prompt of the ES medium is made in the last step (-> **7**) of the wizard.

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

6b Enter password (for the repeated execution of the wizard)

In case of the renewed execution the "**Password**" for your authentication key is first prompted. This is required for the authorisation of the communication job at the bank.

Subsequently, you must confirm in the area "Electronic Signature" the key pair with your Electronic Signature. With it, the release of the key is directly authorised on bank side.

For this enter your "**ES password**" in the corresponding field. The prompt of the ES medium is made in the last step (-> 7) of the wizard.

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

7 Start communication

A communication job/communication jobs is/are generated from your details. The Comms. can be automatically started in this last step if you confirm the predefined entry using the [**Complete**] button. If you want to execute the Comms. at a later time, please deactivate the entry "**Execute communication directly**".

In case you work in a network environment, you can choose a PC planned possibly especially for communication jobs using the list box "**On workstation:**" and start there the communication.

Use the [**< Back**] button to go back in each case the work steps in order to enter changes, if applicable.

At the end, the communication jobs HSA and HPB are generated and, if applicable, immediately executed.

Using the session type HSA the Public Keys are transferred to the bank signed with the currently bank-approved key for authentication and encryption. The Public Key for the Electronic Signature (ES version A004) does not need to be sent any longer to the bank, since this has already been used within the framework of the BCS-FTAM or BCS-FTP protocol and is already available on bank side. The session type HSA does not require the additional transfer of an INI letter, since the authenticity of the transmitted keys is secured by the ES of the affected user.

Subsequent to this, the collection of the bank keys is made using HPB with automatic release.

Since each EBICS communication job must be denoted with a signature, the prompt follows to enter the ES medium subsequent to pressing the [**Finish**] button. (The ES password has already been entered.)

After inserting the ES medium and confirming with [**OK**], depending on the above mentioned checkbox, the communication is started immediately or later (i. e. from the file manager).

In the lower part of the window, a display for the status of the processing then appears.

Communication immediately:

After the successful transmission, close the appearing message with [**OK**].

Close the wizard by a concluding pressing of the [**Finish**] button.

Communication later:

Confirm the appearing message with [**OK**]. Process the communication jobs with the corresponding ID-Group subsequently in the file manager.

4.7 Exchange EBICS authentication keys

To change (to generate or to send) the EBICS authentication keys (A- and V-Key) and/or to call again the corresponding keys of the bank, choose in menu -Communication- menu item -Exchange EBICS authentication keys-.

A wizard guides you through the necessary steps which are required to exchange the EBICS authentication keys.

1 Generate / Send EBICS authentication keys

After starting the menu item, the checkbox "**Generate new key pair**" is already highlighted in the dialog box. If you want to generate a new key pair for the EBICS authentication, retain this presetting.

If, however, you want to send already existing keys (e. g. generated earlier) to the bank(s), untag the above mentioned checkbox.

If you want to send the key pair generated again or the current key pair to the bank (s), thus retain also here the highlight of the checkbox "**Send key pair (HCA)**".

Use the session type HCA to send a query for changing the user keys for authentication and encryption. If you also untag this checkbox, you can use the wizard after highlighting the third option for generating a HPB communication job (see below).

For the authentication of your job / your jobs, you must enter your currently valid **Comms. password**.

Generate EBICS authentication key pair

Do you want to generate a new key pair for the EBICS authentication ?

☒ Generate new key pair

Do you want to send the new/current key pair for the EBICS authentication to the bank(s) ?

☒ Send key pair (HCA)

Please enter now your currently valid password for the authentication.

Comms. password

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

If you have highlighted the checkbox for the key pair generation (first option), you must enter below an arbitrary character string consisting of exactly **32 random characters** for the generation of a new key pair. These characters should be chosen as randomly as possibly. The entry is made concealed, i. e. each entered character is displayed by an * (asterisk). This optionally selectable character string builds the basis for the generation of the key pair.

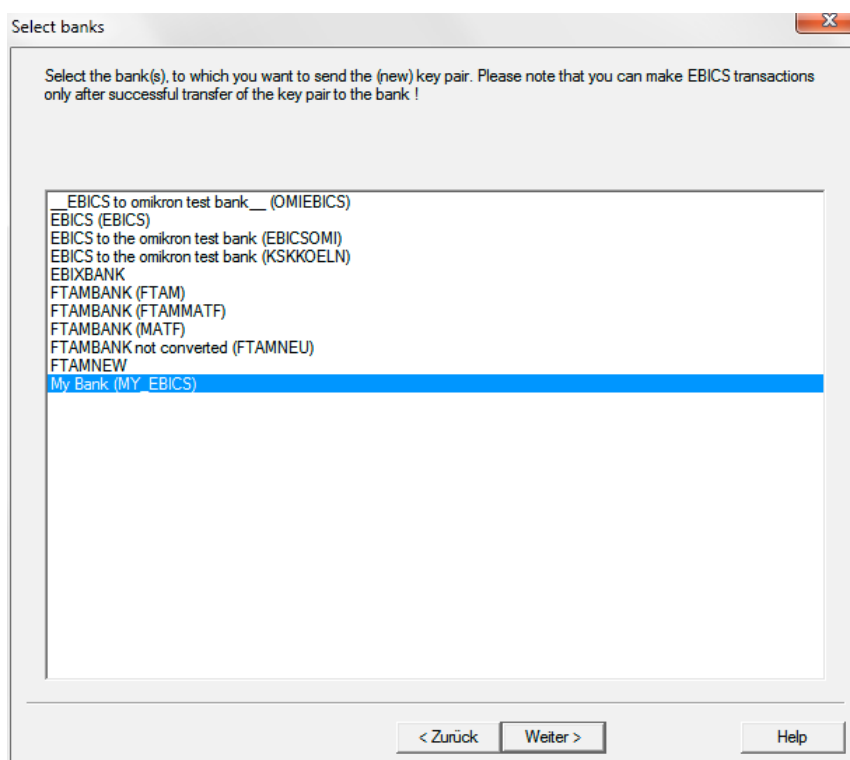
If you want to create in addition (or, if applicable, exclusively) a communication job with the session type HPB, thus you must highlight the checkbox **"Also collect current bank key (HPB)"**.

Using the session type HPB the transfer of the public bank keys is made.

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

2 Choose banks

A list of EBICS banks is offered to you. Choose the bank(s) to which you want to send the (new) key pair. Please note that you can make EBICS transactions only after successful transfer of the key pair to the bank!



Subsequently click the [**Next >**] button.

3 EBICS user status

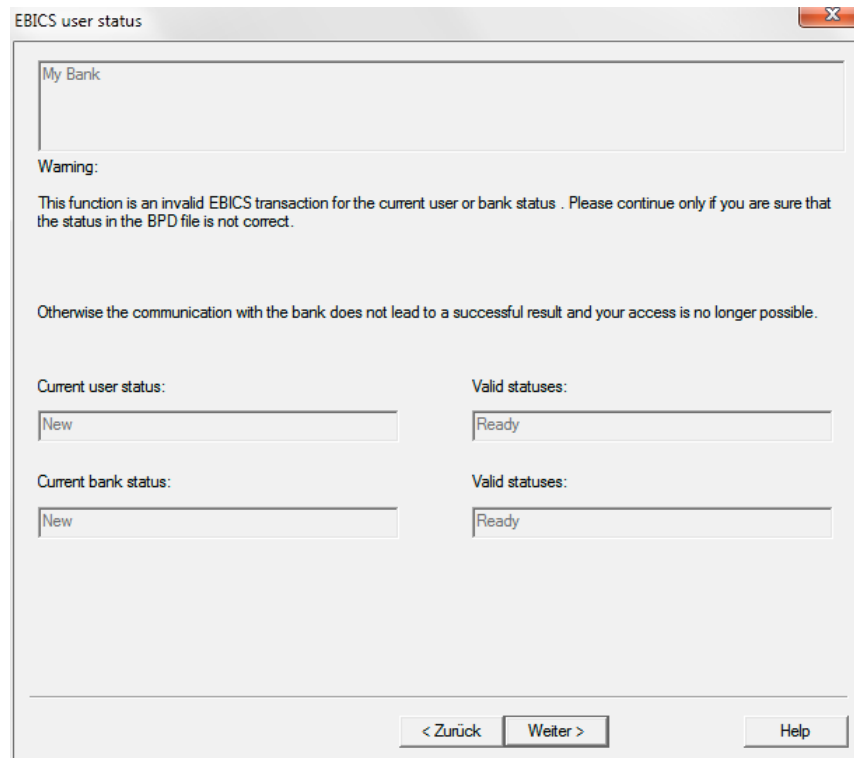
If the chosen options are invalid EBICS transactions for the current user or bank status, a warning follows. Thus e.g. in the user status "New" a key change is an invalid transaction. A valid status for such a transaction would be, for example, the status "Ready". Current and valid **statuses of the user or bank side** are displayed here for your information.



Please note:

You should proceed with the wizard in case of this warning only if you are absolutely sure that the status in the bank parameter file is not correct. Otherwise, the communication with the bank will not be successful and your access is then no longer possible.

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



EBICS user status

My Bank

Warning:

This function is an invalid EBICS transaction for the current user or bank status. Please continue only if you are sure that the status in the BPD file is not correct.

Otherwise the communication with the bank does not lead to a successful result and your access is no longer possible.

Current user status:	Valid statuses:
<input type="text" value="New"/>	<input type="text" value="Ready"/>
Current bank status:	Valid statuses:
<input type="text" value="New"/>	<input type="text" value="Ready"/>

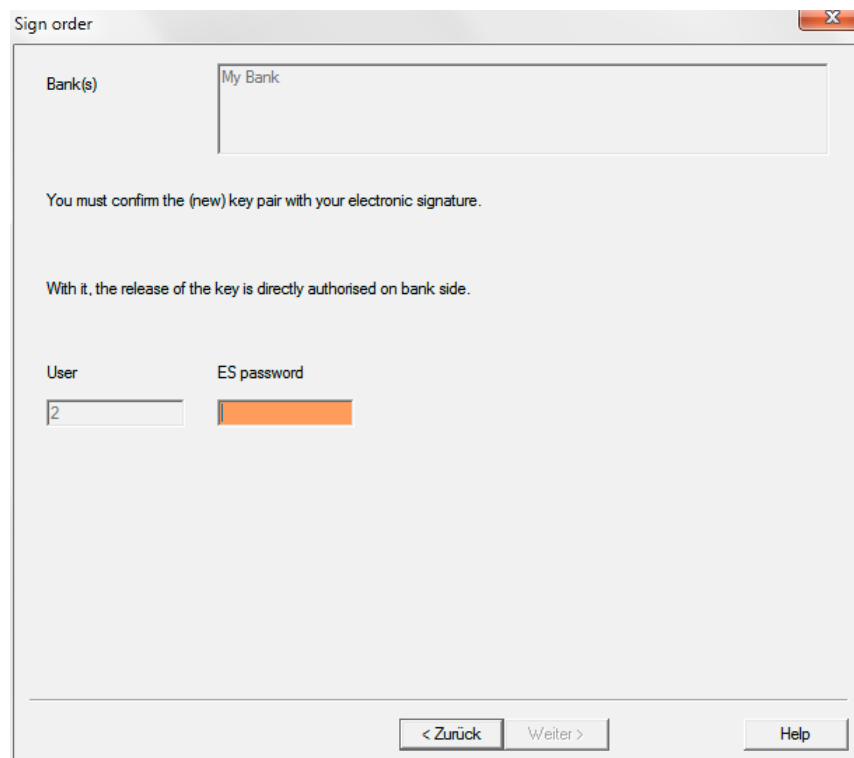
< Zurück Weiter > Help

4

Signing the order (not for the exclusive creation of HPB orders)

Subsequent to this, the (new) key pair must be clicked with the Electronic Signature in order that the release of the key is immediately authorised on bank side.

To be able to make subsequently the Electronic Signature, you are prompted to enter your **ES password**.



Sign order

Bank(s)

You must confirm the (new) key pair with your electronic signature.

With it, the release of the key is directly authorised on bank side.

User	ES password
<input type="text" value="2"/>	<input type="password"/>

< Zurück Weiter > Help

Then press the [**Next >**] button.

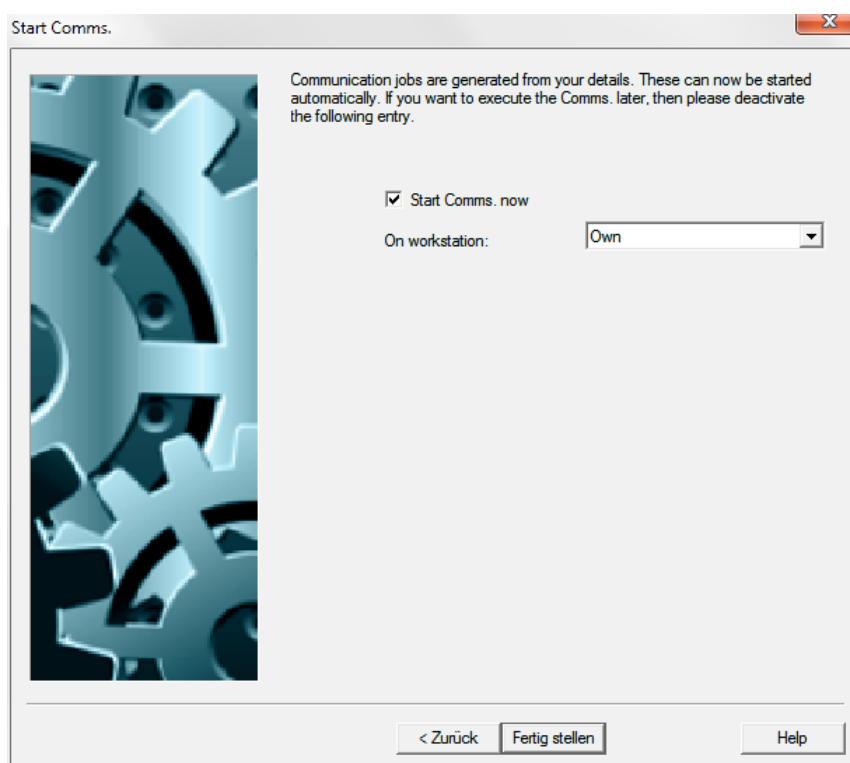
If an HPB retrieval shall be executed, subsequently the hash values of the bank keys are prompted for the automatic verification after their retrieval (This page is displayed per each chosen bank.).

Confirm subsequently with [**Next >**].

5 Start communication

A communication job/communication jobs (HCA and, if applicable, HPB) is / are generated from your details. The Comms. can be started automatically in this last step when you confirm the predefined entry using the [**Complete**] button. If you want to execute the Comms. later, please deactivate the entry "**Execute communication directly**".

If you work in a network environment, you can choose a PC planned possibly especially for communication jobs using list box "**On workstation:**" and start there the communication.



Using the [**< Back**] button you can go back in each case the work steps, if applicable, in order to enter changes.

Since orders must be denoted with a signature for the key transfer, subsequently to pressing the [**Finish**] button, the request follows to enter the ES medium. (The ES password has already been entered: step 4)

After inserting the ES medium and confirming with [**OK**], depending on the above mentioned checkbox, the communication is started immediately or later (i. e. from the file manager).

In the lower part of the window, then a display appears for the status of the processing.

Communication immediately:

After the successful transmission, close the appearing message with [**OK**].

Close the wizard using a concluding pressing of the [**Finish**] button.

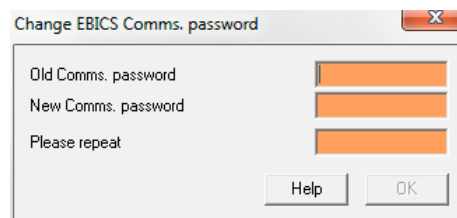
Communication later:

Confirm the appearing message with [**OK**]. Process the communication jobs with the corresponding ID-Group subsequently in the file manager.

4.8 Change EBICS Comms. password

If the necessity to change the Comms. password arises for your EBICS access (i.e. of the access password for the A- and V-Keys), thus choose from menu -Communication- menu item -Change EBICS Comms. password-.

The program prompts you in the first step to enter the **old EBICS password** used so far. Subsequent to this, enter then the **new EBICS password**. The entries are made concealed, i.e. each entered character is displayed by an * (asterisk). For reasons of security, you must **please repeat** the entry of the new EBICS password. Confirm your entries by selecting the [**OK**] button.



Confirm also a concluding message with [**OK**].

Analogously to changing the ES password, no communication to the bank is required for this.

If it is defined for you in the BPD file that the Comms. password shall be saved, thus the new password is also changed in the BPD file.

4.9 Key media administration wizard



Please note:

This key media administration function cannot be used, if you are using a chipcard as key medium.

To move private keys for the Electronic Signature and/or private EBICS authentication keys to an external medium (e.g. after having activated the parameter **"Use external medium for EBICS authorization keys"**) or between different key media, you have to use the "Key media administration" wizard. Additionally, you can delete keys with this function or backup them on another medium.

Which media can be used, e.g. for the external key storage, depends on user specific (see Chapter 5.4.1: *User property page*) and computer specific settings (see Chapter 6.1.5: *Electronic Signature property page*).

Key media administration

Please note:
This function cannot be used, if you're using a chip card as key medium!

Electronic signature

☐ Register USB-Stick for using your electronic signature on this workstation ?

☐ Move medium for electronic signature ?

Typically valid EU medium: Take over to:

☐ Delete private key for electronic signature ?

☐ Backup private key for electronic signature to another medium ?

Valid ES password:

EBICS authentication keys

☐ Move medium for EBICS authentication ?

Typically valid authentication medium: Take over to:

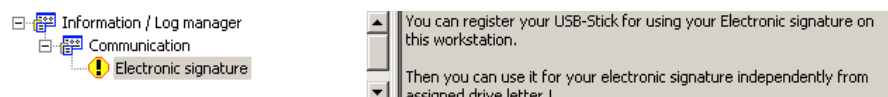
☐ Delete private key for authentication ?

☐ Backup private key for authentication to another medium ?

Valid EBICS password:

Help OK

Users, who work with USB sticks, are notified in the ILM that it is possible to register a stick.

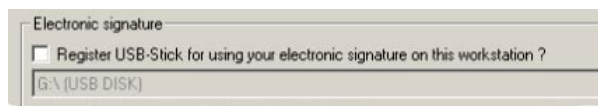


First you have the possibility here to register a certain USB stick for the Electronic Signature on a specific computer. To do this, check the **"Register USB stick for using your electronic signature on this workstation?"** check box. Then select the required stick via selection list box. After confirming with [OK] the selected stick is registered on this computer. Subsequently, a message is displayed that the selected stick is the currently registered ES medium on this computer.

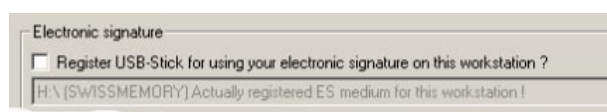
This registered USB stick is then always used for the Electronic Signature on this computer, **independently from the drive letter actually used**.

Example:

In this case the drive letter G:\ is already occupied by another USB stick.



The GUID of the USB stick can now be used to clearly identify the registered stick as the medium registered for the Electronic Signature (here the drive letter H:\ is assigned to it).



This setting need to be repeated for a user on further computers if necessary, since the GUIDs are occupied specifically for a workstation. If no USB stick is registered for the user/computer, the drive letter setting from the system parameters is used.

The next part of the wizard is used only for actions, which concern the **Electronic Signature**. Each action here is to be authorized with the current valid **ES password**.

The lower part of the wizard is used for the **authentication keys** necessary in addition with **EBICS**. Actions, which concern these keys, are to be authorized with the current valid **EBICS password**.

By ticking the appropriate options in the ES, in the EBICS or in both parts, you decide whether the actions are to be accomplished individually or at the same time.

The first option in each part is used for **moving** the private key for the Electronic Signature and/or the private EBICS authentication key from the current medium to a new target medium. To do this, select in each case the currently used medium from the available drives on the left side, the designated target medium on the right side.

After input of the ES or EBICS password and confirming with [**OK**] the key(s) is(are) moved to the target medium.

The second option in each part is used for the **deletion** of the private key for the Electronic Signature and/or the private EBICS authentication key.

After confirming with [**OK**] the key(s) is(are) deleted.

The third option in each part is used to **backup** the private key for the Electronic Signature and/or the private EBICS authentication key on a further medium. After choosing this option, a field is displayed at the bottom of the wizard, where you can enter the designated backup directory, if need be, using the folder selection via [...] button.

After input of the ES or EBICS password and confirming with [**OK**] the key(s) is(are) copied to the backup directory.

4.10 Manage certificates

If accesses to the web application with TLS encryption or with TLS encryption and client certificates shall be used, the respective certificates must be generated using the application before configuring the accesses. For this the following menu items are available:

4.10.1 Generate system key and certificate

4.10.2 Generate TLS key and certificate

What is important in these functions relevant primarily for system administrators can be found in the separate document "Quick reference for system administrators" in the Chapter: *Accesses to the web application* (File --QuickRef_Admin--.PDF in the ..\DOC directory of the installation).

4.10.1 Generate system key and certificate

Using this menu item you can create a new system key and the corresponding self-signed certificate. The system certificate will be used to sign client certificates and TLS certificates.

**Attention!**

After creating a new system key all client certificates and TLS certificates signed with the previous system key are invalid!

Generate system key and self-signed certificate

Here you create a new system key and the corresponding self-signed certificate. The system certificate will be used to sign client certificates and TLS certificates.

After creating a new system key all client certificates and TLS certificates signed using the actual system key are invalid !

☒ Generate system key ? Last generated:

☒ Generate system certificate ? Last generated:

Password of key: Please repeat password:

Key length in bits: Validity of the certificate in years:

Details for creation of certificate

Country code:

Federal state:

City:

Company:

Department:

Name:

E-Mail address:

Help OK

4.10.2 Generate TLS key and certificate

Using this menu item you generate a new TLS key and certificate for browser access.

Generate TLS key and server certificate

Here you create a new TLS key and certificate for browser access.

☐ Generate TLS key ? Last generated:

☐ Generate TLS certificate ? Last generated:

☐ Generate certificate request only for external CA and don't self-sign ?

Password of system key:

Key length in bits: Validity of the certificate in years:

Details for creation of certificate

Country code:

Federal state:

City:

Company:

Department:

On creating TLS certificates, this has to be the base URL, which is accessed by browser !

URL:

E-Mail adress:

There are two variants available:

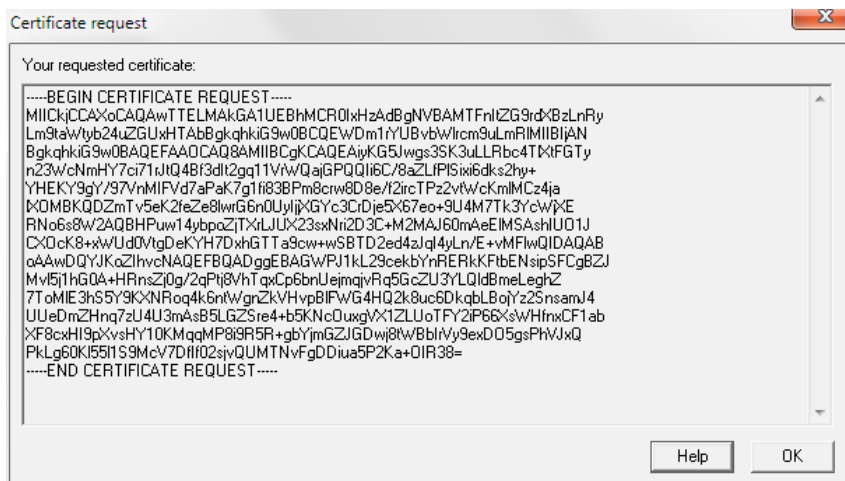
Alternative 1: Self-signed certificate

For this you have to tick the options "Generate TLS key?" and "Generate TLS certificate?". After entering the required data confirm with **[OK]**.

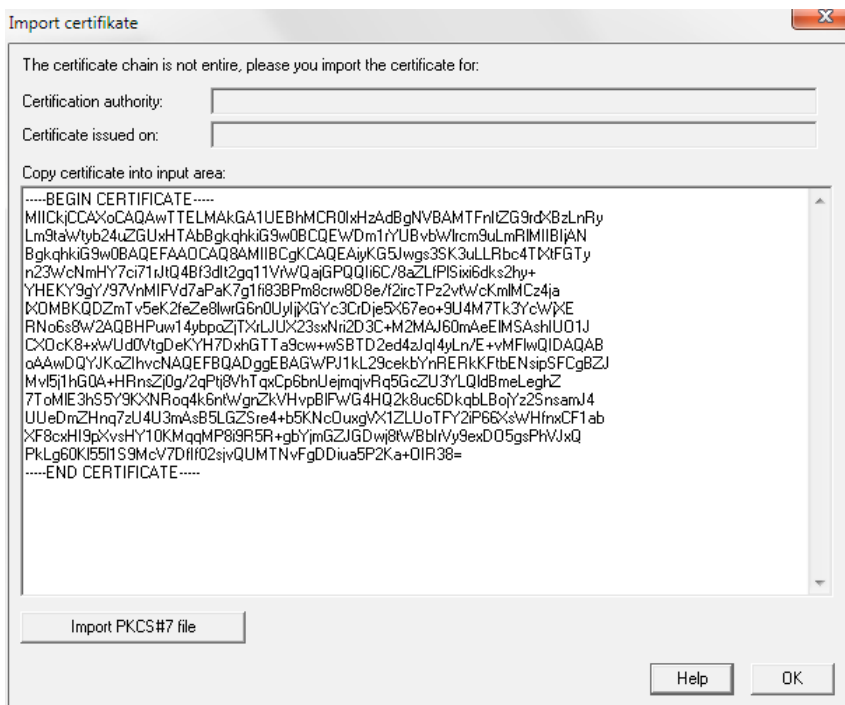
Alternative 2: Certificate of a Certification Authority (CA)

Check for this the "Generate TLS key?" and the "Generate certificate request only for external CA and don't self-sign?" check boxes.

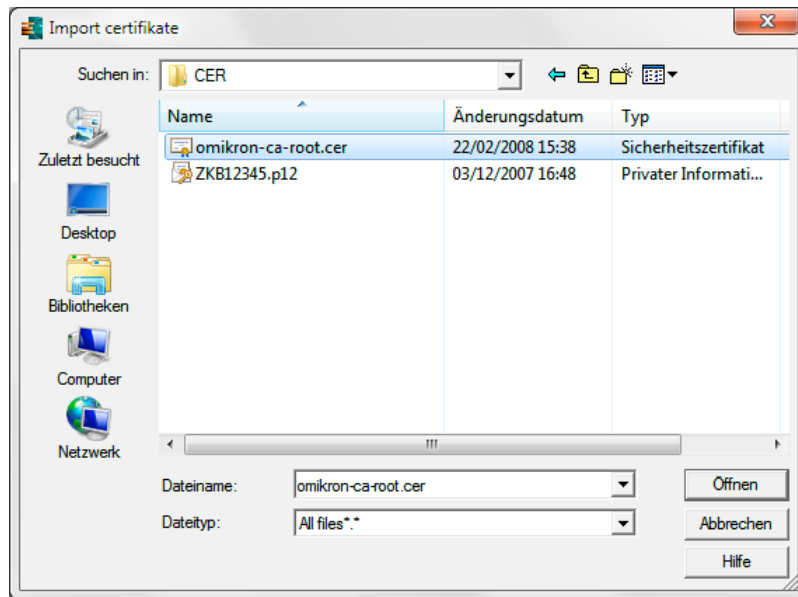
After entering the required data and confirmation with **[OK]** a certificate request is generated, which must be transmitted by you to the Certification Authority. Later you receive a certificate response from this authority.



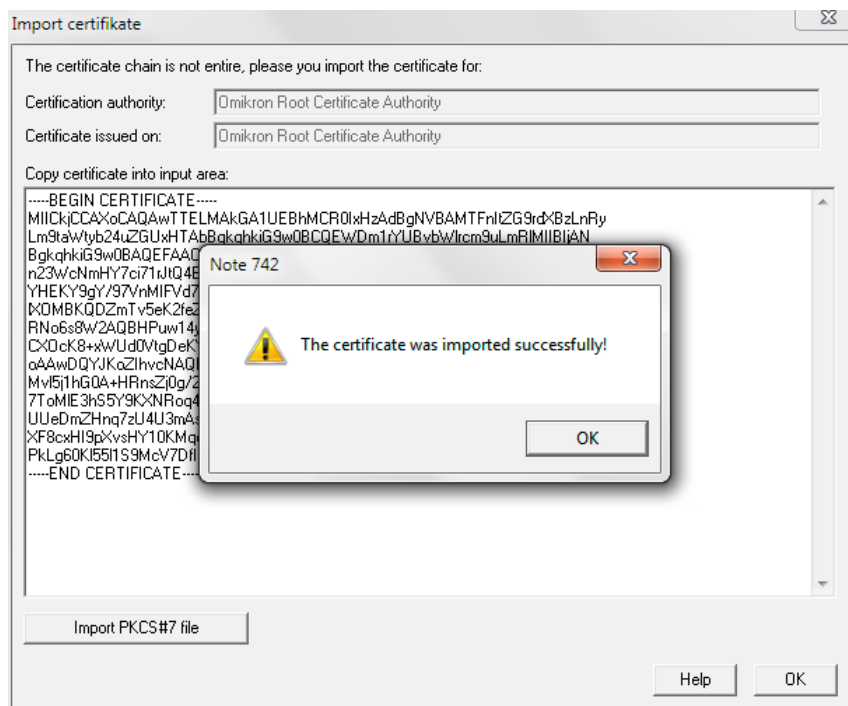
In order to import the requested certificate into the system click the [**Import certificate**] button first. Then copy the certificate response and paste it in the large text box. Confirm with [**OK**].



Alternatively you can import appropriate certificate files from other directories into the system using the [**Import PKCS#7 file**] button. Then the well-known file open box is displayed.



Using the [**Open**] button you can import the certificate file.



If the import is successful, a display shows you under “**Certification Authority**” who has issued the certificate. Under “**Certificate issued on**” also valid information is displayed.

4.10.3 Generate certificate request

Further menu items are only available, if the additional module "Certificate administration" is installed.

These are:

- 4.10.3 *Generate certificate request*
- 4.10.4 *Import / install certificate*
- 4.10.5 *Assign certificate*

After using this menu item you are first prompted to insert the appropriate ES medium:



In the following dialog some entries necessary for the creation of the certificate request must be made:

Type of private key

Password of private key

To enable the access to the key the ES password need to be entered.

Further mandatory entries are: **Country code**, **Name** and **E-Mail address**. The fields **Federal state**, **City**, **Company** and **Department** are to be filled optionally.

Generate certificate request

Type of private key: Signature key 1024 Bit (M003 A004)

Password of private key:

Information for the generation of certificate request:

Country code: GB

Federal state:

City:

Company:

Department:

Name:

E-Mail address:

Your requested certificate:

Help OK

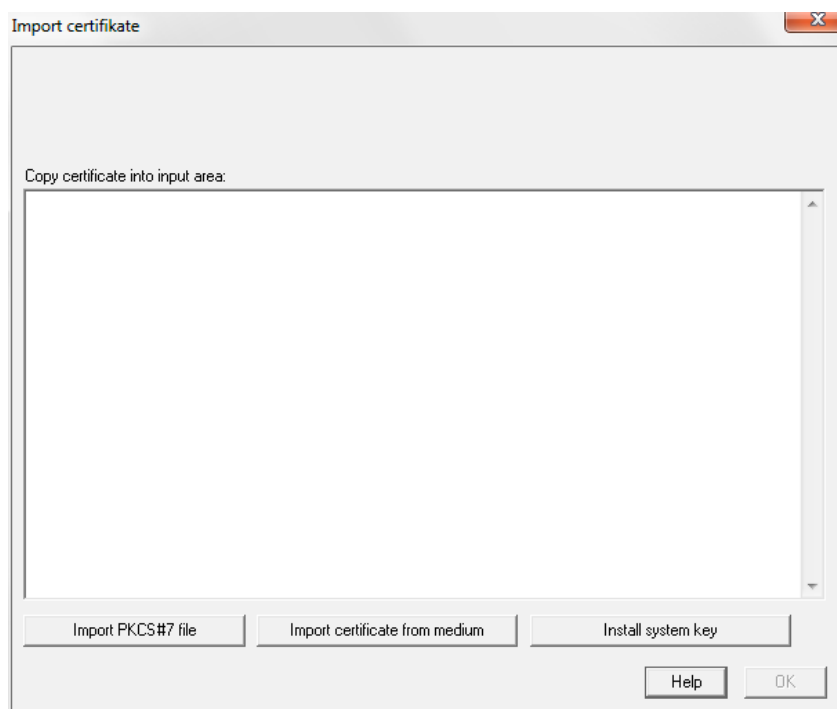
After clicking on the [**OK**] button the requested certificate appears in the large field below the entries.

4.10.2 Import certificate

In order to import the requested certificate into the system, paste the certificate copied before in the large input field and confirm with **[OK]**.

Using the **[Import PKCS#7 file]** button you can import appropriate certificate files from other directories into the system. Then the well-known box for file selection opens.

Using the **[Import certificate from medium]** button you can import a certificate file directly from a signature medium.



4.10.3 Assign certificate

Using this dialog the requested or imported certificates can be assigned to the appropriate banks (i.e. bank parameter files), which support the usage of certificates.

In the display fields suitable entries can be chosen and then linked together using the **[Assign]** button.

Using the **[Remove assignment]** button you can remove these links.

Assign certificates

Requested certificates:

Issued on	Date	Time	Type of private key
-----------	------	------	---------------------

Imported certificates:

ID	Issued on	Certification authority	Imported	Valid from	Valid until	Type of private key
----	-----------	-------------------------	----------	------------	-------------	---------------------

Assign Remove assignment

Assign here to your bank parameter files the imported certificates:

Bank	ID	Type of private key
------	----	---------------------

Help OK

Table of Contents: Chapter 5

	Page
5 File Manager / Execute Comms.	5-2
5.1 File Manager.....	5-2
5.1.1 Database overview: File Manager.....	5-3
5.1.2 File Manager: View Details	5-20
5.1.2.1 Communications property page	5-21
5.1.2.2 Post-processing and transfer parameters property page	5-23
5.1.2.3 Comms. log / ES log property page.....	5-27
5.2 Wizard for collecting data from several banks / Autodial function	5-28
5.3 Execute Comms.....	5-33
5.4 Return codes.....	5-35
5.5 Post-processing / User Exits.....	5-50
5.6 Monthly statistics (supplementary module)	5-52

5 File Manager / Execute Comms.

The file manager is the central control tool of the communication of the program, i. e. for all incoming and outgoing messages.

The function buttons in the File Manager (Chap. 5.1) and the functions described under Execute Comms. (Chap. 5.3) are available to start Comms.

5.1 File Manager

You can open the File Manager

by clicking on the icon



or

the menu item -Communication- / -File Manager-.

Controlling the communications is exclusively made using the file manager. The File Manager shows all the information relating to incoming and outgoing bank transactions. Users who make frequent use of the system can check all pending and executed Comms. sessions and control the assignment of signatures and the transmission of the files. All reference and process information is collected here.

5.1.1 Database overview: File Manager

After selecting the File Manager, a database overview opens in which you can administer all incoming and outgoing Comms. Files.

The screenshot shows the 'File manager' window with a 'Signatures' tab selected. The main area displays 'General information about the file E:_323\IDCWIN\12051005.IDC'. Below this, there is a 'Summary information on all payments' table and a main table listing sessions.

General information about the file E:_323\IDCWIN\12051005.IDC													
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	10.05.2012 37050299 AUFTRAGGEBERNAME	1 DES0370502990010203040	1.234.567,89	EUR	

Session type	Order	Status	Original file name	Bank name	Currency	Amount	Total number of payments	Attributes	ES made	ES required	ID-Group	Comms. date	Comms. Time	Hash value
<input type="checkbox"/> AZV	A000	Pending ES	E:_321\AZVWIN\12022304.AZV	EBICS...	EUR	1.565.228,51	5	T		1	ACK01092			CAB81703 (CHK2)
<input type="checkbox"/> IDC	A000	Pending ES	E:_IDCWIN\12051006.IDC	EBICS...	EUR	1.234.567,89	1	T		1	IDC19009			FAA81B05 (CHK2)
<input checked="" type="checkbox"/> IDC	A070	Pending ES	E:_IDCWIN\12051005.IDC	EBICS...	EUR	1.234.567,89	1	T		1	IDC17248			45121805 (CHK2)
<input type="checkbox"/> IDC	A000	Pending ES	E:_IDCWIN\12051004.IDC	EBICS...	EUR	1.234.567,89	1	T		1	IDC17248			45121805 (CHK2)

At the bottom, there are buttons for 'Execute order', 'Execute all due orders', 'New entry from favourite', 'Delete signature', 'Sign', 'Collect data from several banks', 'View file', 'Help', and 'New order'.

Signatures (up to six) with date and **time** of signature are displayed in the in the **display section** of the database overview with a summary of the file contents next to them.

If the internal approval function is activated (cf. parameter "Number of internal approvals" in the Core module chapter 6.1.5: *Electronic Signature / File Manager*), the IDs of persons, who made the **approvals** (up to two with date/time), are displayed. Then a signatory can check, who has accomplished the approval.

Use the list box to limit the display to defined groups of Comms. batches. So you have the choice between:

- **Display transmit sessions**
- **Display collection orders**
- **Display received files.** and
- **View all.**

If you check the control box "**Do not show successfully sent files**", all successfully sent Comms. files (Status "OK") will be excluded from the display.

You can use the control box "**Only show files pending ES**" to limit the display of files to those which still require an Electronic Signature (Status "Waiting for ES").

Using the "**Do not show files signed by yourself**" check box you can hide files signed by you as logged on user.

Using the selection list "**Stock**" you can display beside current data also historical data, if the File Manager history had been activated by the parameter "**Maintain history?**" (see Core module Chapter 6.1.5: *Electronic Signature/File Manager*). Functions like [**Select** or [**Print**] have only an effect on the data currently selected.

The **record list** of the database overview lists the individual entries using the session type, the order no. of the order attribute (see, for example, Comms. chapter 1.2.3: *FTAM*), no. of signatures required/made, of the status (e. g. Collection OK, Pending Comms. (ES), OK, error, rejected, deleted, ES check OK, ES error, Comms. initiated, Pending Comms. PIN, Waits for approval), of the file name (including drive and path entry, a grouping name (internal name), the date and the time of the Comms., of the name of the bank parameter file used for the Comms. (as clear text if available) and the total of orders (currency and amount). Use these to better identify the individual entries. The total is displayed in the original currency if all orders have the same currency. For orders in different currencies, it will be

converted into the base currency (i. e. the currency which is with rate 1 in the currency table) and then it will be added up.

The column "ID-Group" can be very simply used for a selected processing of the Comms. batches (former DAD name).

The display of the **next** execution date in the columns "Comms. date" and "Comms. time" of the overview (for comms. orders with periodical repetition cycles) always occurs if the status of the order is set on "Comms. initiated" and therefore a next execution date exists. Then the display of the next date has a higher priority as the display of the last execution date (see line 1 in the following example).

Session type	Status	File name	Bank name	ID-Group	Comms. date	Comms. Time
<input checked="" type="checkbox"/> STA	Comms. initiated	C:\...MCCWIN\BWM\DA090.STA	Mandant 100	MANUELL	21.06.06	10:32
<input type="checkbox"/> PTK	Pending Comms. R-MKA02	C:\...MCCWIN\BWM\DA010.PTK	Mandant 100	MANUELL		
<input type="checkbox"/> STA	Error	C:\...MCCWIN\BWM\DA080.STA (11,0)	Mandant 100		21.06.06	10:28

For the status "Pending ES/Pending Comms./Rejected/Deleted/Pending Comms.-PIN", the display of date and time in the overview remains empty (see line 2 of the example above).

For the status "OK/Error/ES check OK/ES error", the **last** execution date is displayed (see line 3 of the above example).

The **most recent file** (the most recent comms. job) is at the **top** of the list.

Multiple selection

If you have highlighted several Comms. batches in the database overview of the File Manager by highlighting the **checkboxes before the session type**, some functions can be executed in a "batch processing" (you can mark all orders using the context menu item -Mark all records-). Above all, this simplifies the signing, since in this case you have to enter the ES password only once.

The functions, which can be used for this processing, are on one hand the following menu items from the context menu (right mouse button):

- -Reject-
- -Reset-
- -Reactivate-

and on the other hand the following buttons from the functional area:

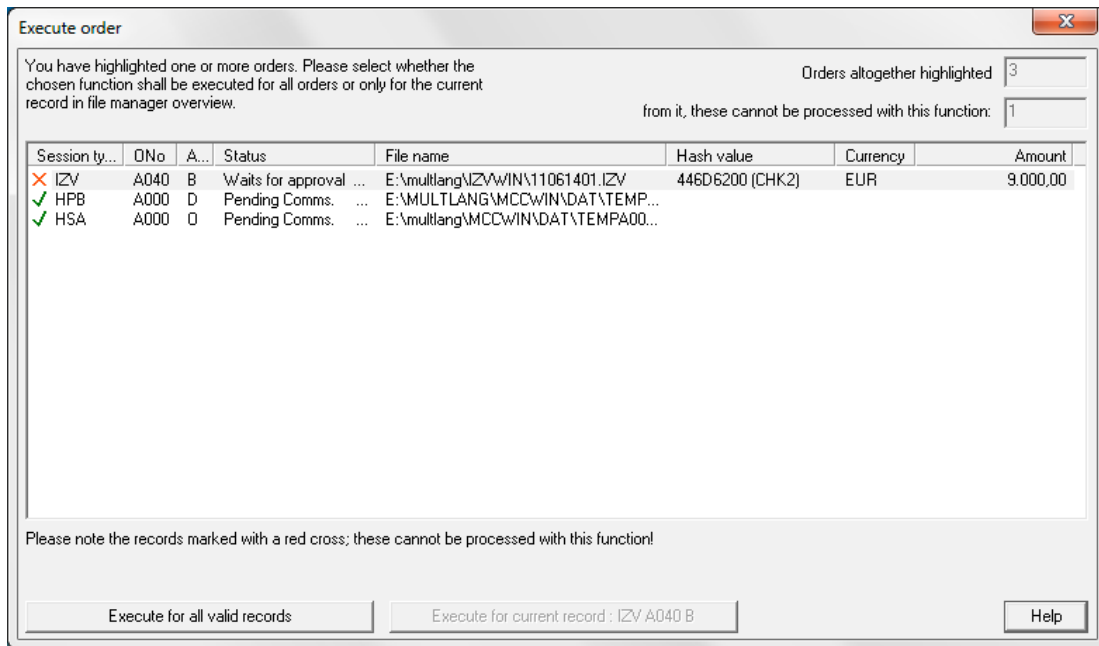
- [**Execute order**]
- [**Delete signature**]
- [**Sign**].

If several data records are marked in the file manager, a further dialog opens after selection of one of the functions specified above (in each case the selected function is shown in the title bar). The data records with ticked check box in the file manager are listed here again.

In addition symbols will show you whether the selected function can be applied to the Comms. order. A green check mark (✓) signals that the selected function is applicable to the data record. The records highlighted in the list with a red cross (✗) cannot be processed with the chosen function.

Example:

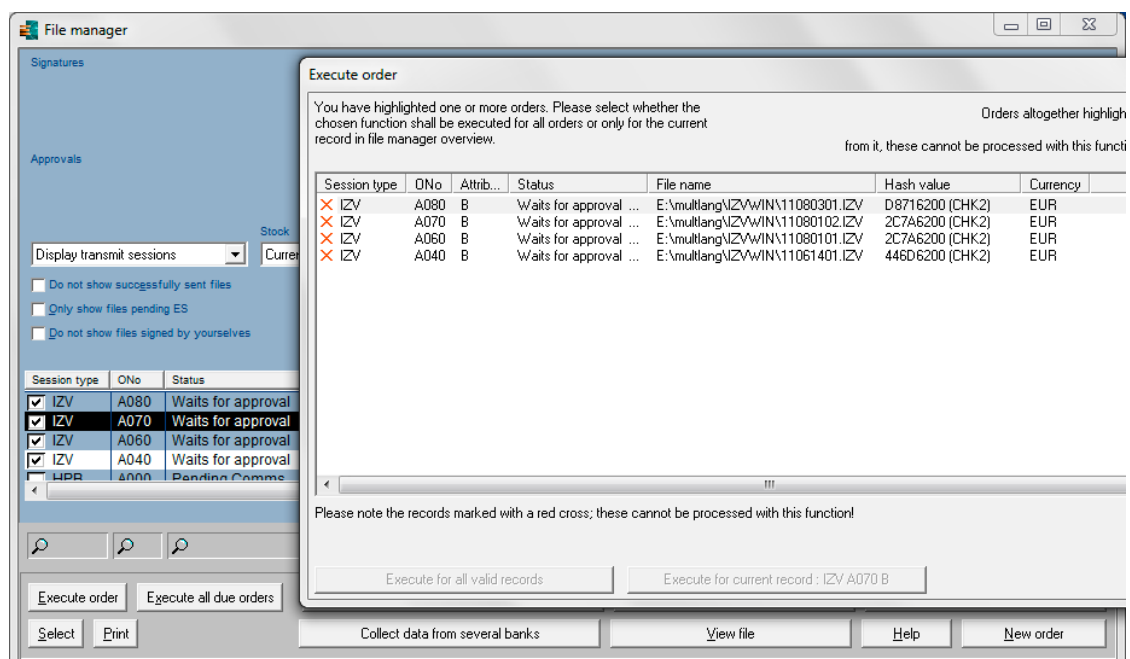
Thus in the following case three Comms. orders were marked in the file manager. The function [**Execute order**] is applicable however only to two of the data records.



The number of data records marked altogether in the file manager is indicated to your information on the top right of the dialog. In addition the number of the data records, which cannot be processed with the selected function, is indicated below this.

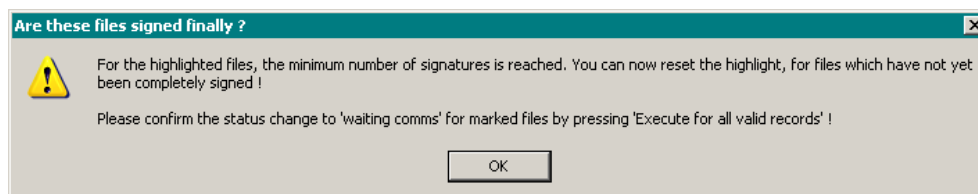
Now you can decide by selecting the [**Execute for all valid records**] button, whether the selected function can be applied to the possible (i.e. marked with a green check mark) data records. If you choose the [**Execute for current record: <ID>**] button, the chosen function is only used for the record highlighted in the file manager (!). This must not be necessarily the record highlighted in the multiple selection window. For the unique identification, the ID of the communication order highlighted in the file manager window is displayed on the button additionally. In the following example this is e.g. the record with the order number A070, not the record with the order number A080, which is highlighted in the selection window.

Example:



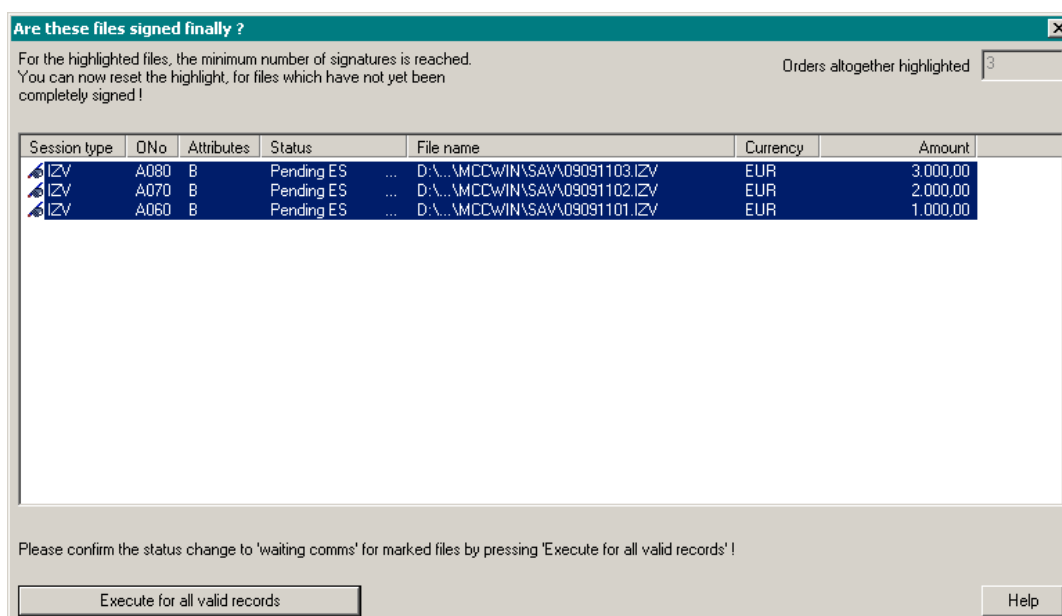
If you use the batch processing for **signing files**, then you will be prompted only once for the ES medium as well as for the input of the ES password.

If the minimum number of signatures (depending on the session type) is reached with the signature made, a prompt follows whether the file is completely signed if the corresponding system parameter "**Prompt whether signatures are complete**" is set (see Chapter 6.1.5: *Electronic Signature property page*).



Please close this message box first using the [OK] button.

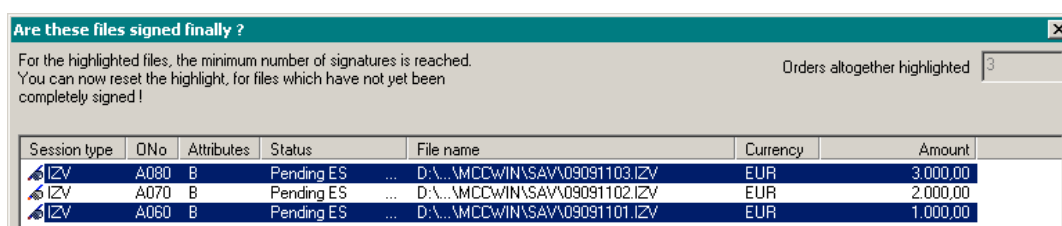
In the dialog with changed texts the files are already highlighted, for which the number of required signatures is reached (-normally- by a grey highlighting of the records).



By clicking on [**Execute for all valid records**] all files marked in such a manner would be labelled as completely signed and released for execution in the file manager (status "Pending Comms.").

To add further signatures to some files you have to reset the highlight.

This can be done by clicking on the completely signed files to highlight them explicitly, (-normally - blue cursor highlight; multiple selection with hold Shift or Ctrl key if necessary). Only for records marked like this the status will change after pressing the button mentioned above.




To reset all highlights -i.e. further signatures should be added to all files - click into the empty area below the records.

After closing the dialog using the button mentioned above the status of the non-highlighted records remains on "Pending ES" in the File Manager. For this files further signatures (second and more signatures) can be added then (using the multiple selection again if need be).

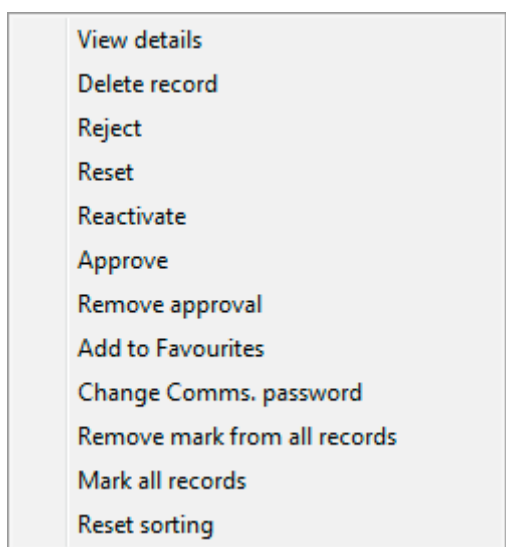


Please note when using the multiple selection for deletion:

Whereas original files of normal orders remain until the expiry of the storage period (see Core module Chapter 6.4.1), if entries are deleted from file manager, the original files of confidential payments (i.e. payments where an access class has been set) are deleted immediately for security reasons.

To prevent as far as possible an unintentional deletion of payment files with confidential payments, these files are marked with an additional exclamation mark ().

Use the **context sensitive menu** (right mouse button menu) to reach important processing functions for the individual records:



A detailed view of files belonging to an individual record can be obtained using the menu item **-View details-**.

Use **-Delete record-** to remove entries from the file manager. Before the deletion, a prompt follows in each case for security whether the entry shall be actually deleted. Only if you confirm this prompt with **[Yes]**, the corresponding action is executed.

After the deletion you are prompted additionally whether the underlying file should be deleted as well.

If you answer the prompt with **[Yes]**, the original file is finally deleted. With **[No]** this file remains and can be sent within a new Comms. session if necessary.

Files, where the entry in the file manager has been deleted (1st answer **[Yes]**), but which were not deleted here immediately (2nd answer **[No]**), will be deleted automatically after the so-called storage period, which was specified for each file type (session type, e.g. IZV) (see Chapter 6.4.1 of Core module).

For confidential payments (i. e. payments with the set access class), the original files are immediately deleted from the ..\SAV directory.

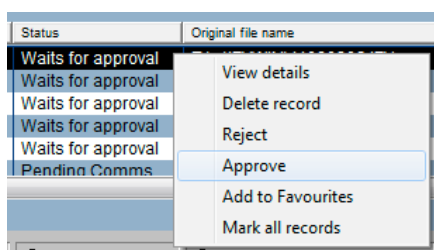
Use the item **-Reject-** to set an order to the status "Rejected", i.e. to exclude it from the Comms. In order that this action is executed, you must confirm a security prompt before with **[Yes]**.

Rejected orders can be reactivated again using the appropriate context menu entry (see below). If the status of a file in the file manager is set to "Deleted" or "Rejected", the corresponding plan data are deleted.

Use the item **-Reset-** to reset an order to a previous status. Thus you can reset, for example, an order with the status "Comms. initiated" using this entry to the status "Waits for Comms.". Also here a security prompt follows to be answered accordingly.

Use the item **-Reactivate-** to activate again orders in the status "Rejected". In principle, ES orders are thereby set to the status "Waits for ES" so that they have to be confirmed again with a signature.

If the internal approval function is activated (cf. to parameter "**Number of internal approvals**" in the Core module chapter 6.1.5: *Electronic Signature / File Manager*), newly entered files get the status "Waits for approval" first. Authorized staff can accomplish approval using the context menu entry **-Approve-**.



The approval can be revoked using the context menu entry **-Remove approval-**.

Preferred session types (transfer and collection orders) can be added to your list of Favourites by selecting **-Add to favourites-**.

If a file has been provided with a wrong or without a Comms. password, you can assign a (new) Comms. password using the context menu item **-Change Comms. password -**. Please enter the Comms. password in the appearing dialog box and confirm your entry with **[OK]**.

With missing password the status "Pending Comms. PIN" is changed to "Pending Comms" thereafter. If the order has been transferred incorrectly before, then the status will be set again to "Pending Comms.". The last return code (AC) is reset to 0.

Using the **-Insert again-** option you can resend already successfully sent files from the SAV directory. For this the original file from the SAV directory will be copied first into the \RESEND directory and then a new Comms. order for this file is added in the file manager.

If several or all orders have been highlighted for the batch processing, all highlights can be removed at once using the context menu entry **-Remove mark from all records-**. To mark all records use the context menu item **-Mark all records-**.

If a sorting of file manager data was made by clicking on one of the columns, then this sorting can be removed using the context menu entry **-Reset sorting-**.

Functions in the context of special session types:

As for the use of the Distributed Electronic Signature with EBICS (s. Chapter 1.2.5: *EBICS*) several EBICS requests are handled with the well-known session type **ESP** (Send distributed signature), several function calls exist for this session type to be called at different places in the File Manager.

Thus an ESP order can be cancelled using the context menu item **-Cancel original order at the bank-**. After selecting the item the HVS cancellation order (DES cancellation) has to be signed. After sending the cancellation order a signature is not possible any longer. Therefore a warning message is displayed, that the file is removed irrevocably from the DES processing on bank side, which you have to answer accordingly with **[Yes]** or **[No]**.

With the execution of the ESP order the retrieval of the original file up to a certain file size (usually 1 MB, adjustable) is made automatically using the EBICS request HVT (Retrieve DES transaction details), executed in the background.

If you try to display information of original files, which exceed this limit, using the **[View file]** button, then you are prompted, that the original file is not yet available, but it can be retrieved from the bank (including display of the approximate file size). If you answer this prompt with **[Yes]**, an appropriate HVT request is started in order to retrieve the original file. Select the **[No]** button, if it should not be retrieved.

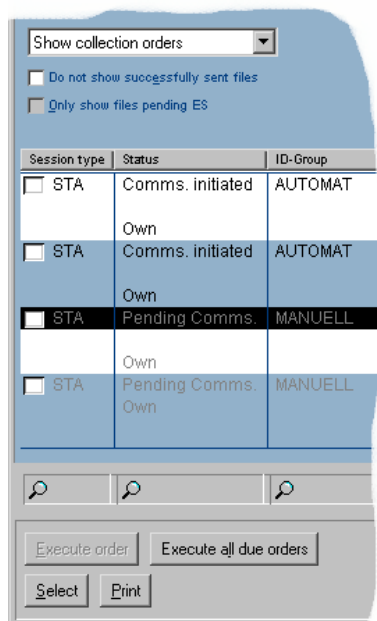
Functions relating to the Electronic Signature and to the sending of files can be found in the **button bar section** in addition to the standard functions **[Select]**, **[Print]** and **[Help]**.

Press the **[Execute order]** button to initiate the Comms. for a chosen file and send the file.

Use the **[Execute all due orders]** button to start the transmission of all due communication orders, provided that the status of the order allows this. If a selection was accomplished, all due orders are executed, which match this selection.

 **Please note:**

With collection orders to be executed manually the **[Execute order]** button is blocked and the orders will not be considered, if the **[Execute all due orders]** button is used. These orders can only be executed using the icon "Collect information from bank(s)" (see Chapter 5.2). In order to mark these orders specifically, they are displayed in the file manager overview with the color specified for deactivated fields in the system parameters, e.g. grey in the following:



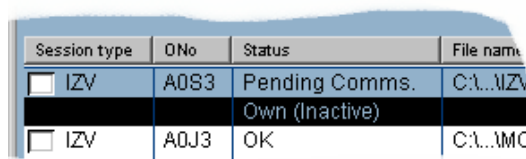
After pressing the two buttons or after choosing the corresponding buttons in the multiple selection window -if operated in a **network-**, first a dialog box opens immediately before the execution, where you select the computer for the execution of comms. orders.

You have the choice between

- Execute only due orders of selected computer or
- Execute all due orders on selected computer,

together in each case with the option to select the wanted **computer name** (if installed in a network) via list box. The selection made last is stored in each case computer-specific as default for the next selection. Computers, on which the Comms. bar of the program is not open, are marked in the selection list by an "(Inactive)" behind the computer name in each case.

Additionally the name of the Comms. computer is shown in the file manager with the "Pending Comms." or "Comms initiated" stati also marked with the label "(Inactive)", if the Comms. bar of the program is not started on this computer.



Session type	ONo	Status	File name
<input type="checkbox"/> IZV	A0S3	Pending Comms. Own (Inactive)	C:\...IZV
<input type="checkbox"/> IZV	A0J3	OK	C:\...MCC

- Execute all due orders as defined in order

is available as third option (when executing single comms. orders, only this option is available).

With the marking of the first option **"Execute only due orders of selected computer"** you determine, that only Comms. orders, which are defined for the execution on a certain computer (e.g. on the own), will be executed.

Marking the second option **"Execute all due orders on selected computer"** effects, that **all** due orders (e.g. collected for a working group) are executed on the selected computer. This is independent from what was defined as Comms. PC for each order during creation before.

If all due orders should be executed as they were defined at order creation in each case, then you should use the third option: **"Execute all due orders as defined in order"**.

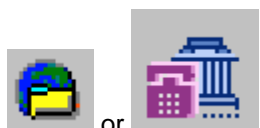
After confirming with [OK], Comms. orders are executed according to your selection (status changes to "Comms. initiated").

Click on [View file] to view the complete contents of a file in a display window. The presentation of the information depends on the display form stored for the respective session type (using parameter **Display form in file manager**; see for this Chapter 6.4.1: *Session types property page*).

Click on [Delete signature] to cancel a signature which has already been entered.

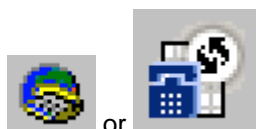
Click on [Sign] to sign the original file. Information on managing the ES can be found here.

Using the [Collect data from several bank(s)] button you can start data collection from your bank(s) as described in Chapter 5.2. The button corresponds in its function to the button for the autodial function described there:



Execute favourites

Click on the [**New entry from favourite**] when in the File Manager or the menu item -Communication- / -Execute Comms. favourite- or the icon






to carry out data communications with a simple click of the mouse if you prefer to establish a simple and direct connection to your bank.

The Comms. favourite serves thereby for pre-defining often used Comms. orders (e.g. for the sending of third-party payments).

By setting the "**Generate plan data in file manager**" parameter (see Chapter 6.4.1: *Session types property page*) for the appropriate session type, automatically the plan data creation is also available for the sending via "favourite".

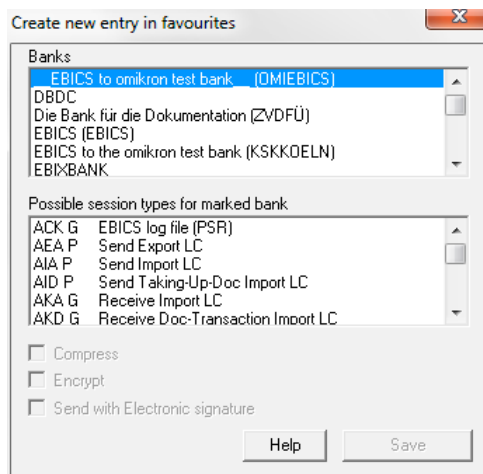
With sending orders one signature is used during the order creation. Further signatures can be carried out using the file manager if necessary.

When in the File Manager database, you can add a session to the list of preferred session types by opening the shortcut menu (right mouse button) and clicking on the entry -Add to favourites-.

After selecting the function "Execute favourite" (using the button, menu item or icon) this list will be displayed. In addition to the session type and favoured bank, small symbols indicate whether the respective session type will be carried out with encryption (), with Electronic Signature () and/or with compression ().

Favourites which are no longer required can be removed from the list using the [**Remove from favourites**] button.

You can enter a new favourite using the [**Create new entry in favourites**] button. The following dialog box will show you the available banks where you can choose your favourite. In addition you will find information regarding the possible session types for the chosen bank (incl. Angaben zu Compression, Encryption, ES).



With EBICS you have the possibility to deactivate the "Send with Electronic Signature" checkbox. Orders are then generated, which provide a transport signature only (attribute T).

	Bank name	Currency	Amount	Attributes	ES ...	ES ...
1.IZV	EBICS ...	EUR	7.777,00	T	1	1

Confirm your choice finally with [**Save**].

You can select the file to be sent using the [...] button behind the field "file". As a function of the selected session type the suitable subdirectory is offered directly (e.g. with IZV the directory..IZVWIN).

After the file selection you can enter below the path and the display of the file content the **Comms. Password** (if necessary a second) and -if need be- the **ES password** needed to issue the Electronic Signature (the field "user" is filled with the current user).

In the file manager, during the new entry in the favourite an **access class** can be allocated (see Chapter 7.8: *Access classes reference table*).

The [**View file**] button is used similarly to the button of the same name in the file manager to display the complete file content of the selected file.

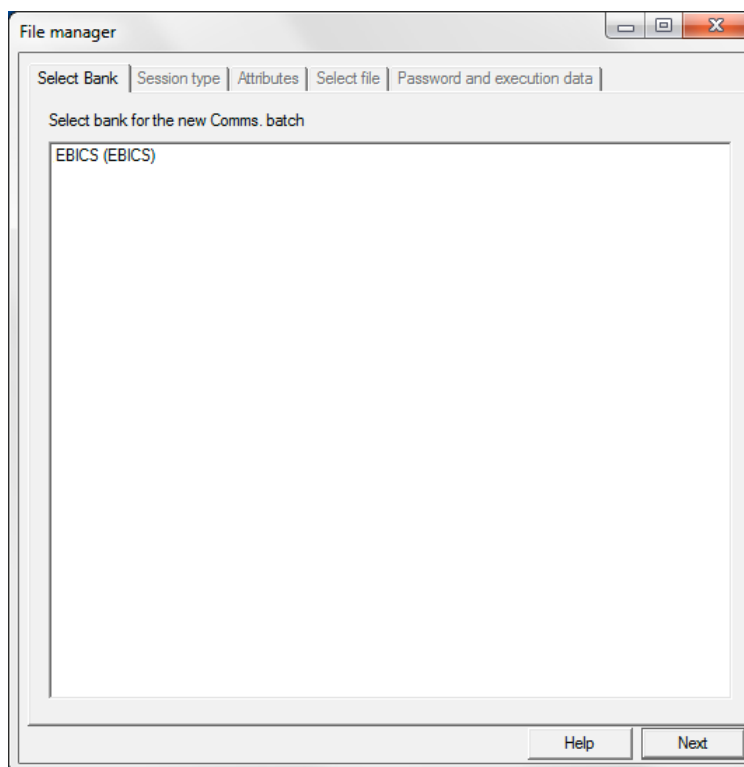
You can select the [**Save for later execution**] button to save this Comms. session for later transmission. You also use this function, if you liked to issue further signatures to the order in the file manager.

You can send it immediately as well, by selecting the [**Execute immediately**] button.

Finally use the [**New order**] button to add a new Comms. session to the file manager.

"Select bank" property page

First specify the bank related to the new Comms. session. A list box on the *Select bank* property page shows all BPDs saved in the system together with a plain text description. Position the cursor or use the mouse to select the required bank.

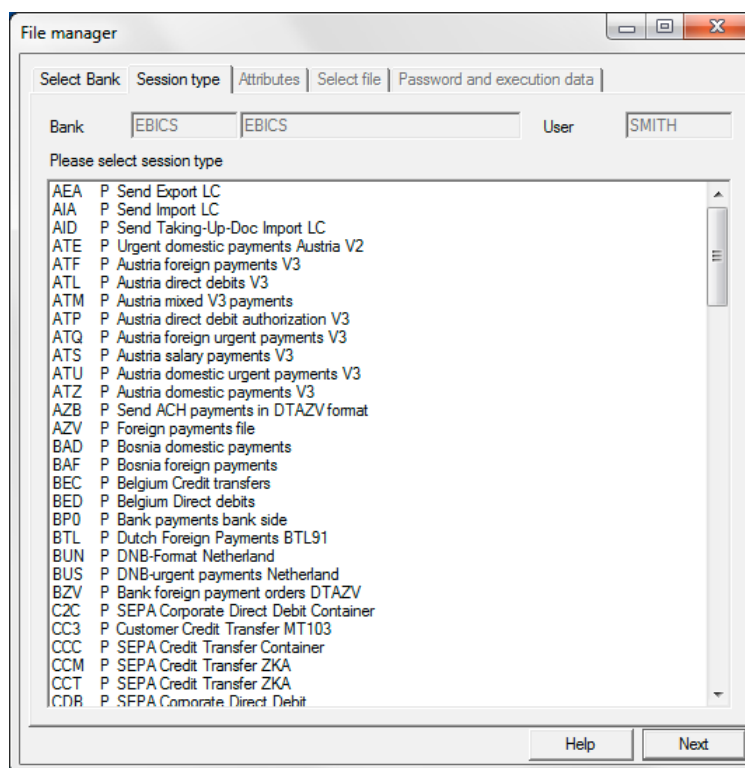


If you have set parameter "**Prompt for EPFT bank parameter files on diskette**" on the *Program property page* via menu item -Administration- / -System parameters-, the program then prompts you to insert the diskette with the BPDs in the floppy disk drive. After confirming by clicking on [**OK**], a list box then displays all BPDs on the diskette, as well as BPDs saved in directory ..\DAT in the Core module. BPDs on the disk are indicated by the corresponding drive letter behind their name. If you choose [**No**], only the BPDs saved in directory ..\DAT in the Core module will be shown.

After selecting [**Next**] (this brings you to the next property page), specify the **session type** and - if you are using FTAM to transfer the data - the **file type**.

"Session type" property page

Dependent on the display option chosen in the file manager (*Display transmit sessions etc.*) the *Session Type property page* lists all session types activated in each case accordingly (cf. Core module, Chapter 6.4: *Session types*).



Session types include:

- IZV : Send Domestic Payment (DOMPAY) orders
- STA : Collect SWIFT daily statements
- PTK : Collect logs
- etc.

Click on the session type you want to select. Selecting the session type also determines the format of the file to be uploaded or downloaded, so that formal validation checks can be carried out at a later point.

Attributes property page

To choose a **File type** from the list box click on the drop-down arrow to the right in the window to view a list of file types.

To facilitate keying on repeated new entries the last selection made here will be suggested for the "File type" field subsequently (per user and per Comms. procedure).

The following options are available in the current program version:

- Original file without signature
- Original file with signature
- Signature file
- Original / Signature together (only FTP)
- Original / Distributed signature (only FTP)
- Original file with transport signature

If you use the MCFT procedure and if you have installed the ES supplementary module, you can only send file types "Original file with signature" and "Original file without signature". Information on the Electronic Signature is contained in Chapter 6: *Electronic Signature*. Further entries are

not necessary because encryption and compression methods are inherent features of this procedure.

If you are using the FTAM procedure you can choose between

- Original file without signature
- Original file with signature
- Signature file

The screenshot shows a 'File manager' window with several tabs: 'Select Bank', 'Session type', 'Attributes', 'Select file', and 'Password and execution data'. The 'Select Bank' tab is selected. It contains fields for 'Bank' (EBICS), 'Session type' (IZV), and 'File type' (Original/Signature together). Below these are sections for 'Encryption and compression' (with 'Encryption (Hybrid DES/RSA)' selected and 'Compression' checked) and 'Customer ID for second signature FTP' (with six empty input fields and checkboxes for 'Forward original file'). A note at the bottom of the encryption section states: 'Please note that a change of these entries for collection orders may only be made after consulting your bank.' At the bottom of the window are 'Help' and 'Next' buttons.

The **Original file** is the file you want to upload or download. The original file may be saved in a particular format (DTAUS DOMPAY format, DTAZV FORPAY format, etc.) determined by the session type defined. The session type also determines the validation checks to be carried out. If you want to send the Original file using FTAM and the file involves a payment order, you must enter an **Electronic Signature** (= ES). You can enter the Electronic Signature for an original file directly when a payment order is generated in a payment module. You can also enter the ES for an original file at a later time. The Electronic Signature itself is saved in a **Signature file** which must also be transmitted to the bank.

If you have installed the FLAM supplementary module, you can achieve an efficient data compression by ticking the "Compression" check box.

With the FTP procedure you additionally have the possibility of entering the customer identifications which are -in the context of the distributed electronic signature- intended for a second signature (distribution list). Via check box you can decide in each case whether the original file is to be passed on or not. Before this, the file type "Original/Distributed signature" has to be selected.

Unlike FTAM, EBICS offers the possibility to transfer the signature together with the data in one transaction and to transmit immediately the result of the signature check to the customer. For EBICS, thus only the option "**Original/Signature together**" is valid when preparing an order to send with the Electronic Signature. If another option with signature not admissible for EBICS is chosen, it is automatically changed into the option "Original/Signature together". According to the EBICS specification it is also possible to send a file without bank-specific signature for authorizing via cover note. Unlike the procedure for FTAM or FTP, where the file

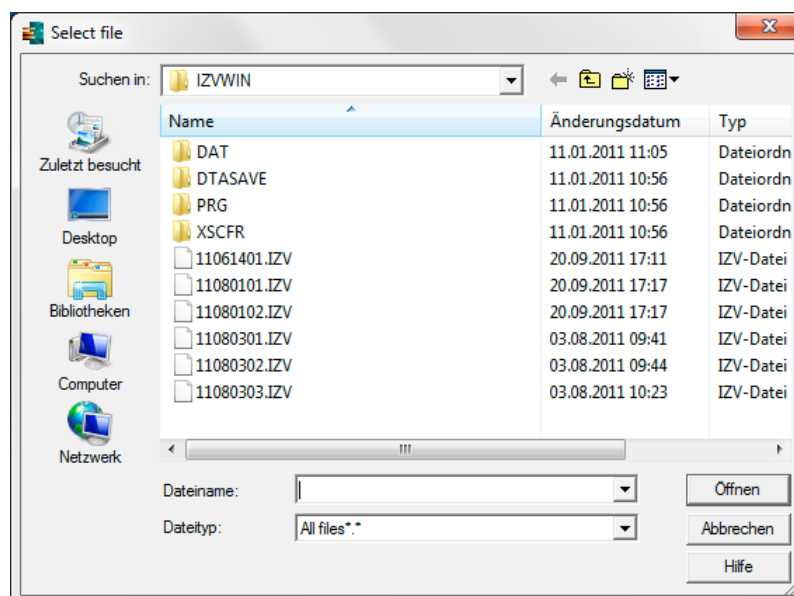
can be sent without signature, for EBICS in this case the file always has to be provided with a transport signature. For this case, the option **"Original file with transport signature"** is available when adding a new communication job. If the option "Original file without signature" is chosen, it switches automatically to "Original file with transport signature" for EBICS. For a better distinction, the order is included with attribute **"T"** and status "Waits for ES" in the file manager.

"Select file" property page

In the case of transmit sessions, the program opens the appropriate subdirectory depending on the session type selected (e.g. the directory ..\AZVWIN for session type AZV), from which you can select (session) files which are to be added to the Comms. batch.

If another sub-directory was selected, this is offered again for the next order.

Click on the required file and then select [**Open**].



The file to be transmitted is displayed in a window for control purposes. The data displayed also depends on the file format defined by the session type. The complete path will be shown in the field **"File"**.

If an error occurs after file selection, it will be shown in a separate window with a short error message.

Using the normal output functions of the window you have among others the possibility to print out this information for your files. This is useful, for example, in the case of payment orders.

For download sessions, the downloaded file will be saved in directory ..\MCCWIN under the name shown in the details dialog box for the Comms. session. The file name is formed from the constant "BWM", a code characterising the file, the 4-character session number assigned by the program and the session type as the extension.

Example:

BWMDA0A5.STA

BWM : Constant
D : File code
A0A5 : Session number
STA : Session type

The screenshot shows the 'File manager' window with the 'Password and execution data' tab selected. The 'General information about the file' section displays the following data:

File creation date	Number of logical files	Total number of payments	Currency	Sum payments
03.08.2011	1	1	EUR	66,00

The 'Summary information on all payments' section displays the following data:

Type	Value date / Ordering party	Number	Currency	Amount
Transfer	03.08.2011 37050198 MY NAME	1 0033633322	EUR	66,00

"Password and execution data" property page

The final step when creating a Comms. session is to **enter the Comms. password** (if need be an ES). The Comms. password, which depends on the bank for which the Comms. session is being created, must be entered to process the sessions. You need a separate Comms. password for each bank for which Comms. sessions are created.

The screenshot shows the 'File manager' window with the 'Password and execution data' tab selected. The 'Password' section contains the following fields:

- Bank: EBICS
- User: SMITH
- Session: IZV
- File Type: Original/Signature together
- Encryption: (Hybrid DES/RSA)
- File: E:\IZVWIN\11061401.IZV

The 'Make Electronic Signature' section contains the following fields:

- User: 2
- ES password: [empty]

The 'Other' section contains the following fields:

- ID-Group: [empty]
- Access class: [empty]
- For this file, plan data shall be generated additionally in a new way: [checked]

The 'Execution' section contains the following fields:

- Repetition: Once
- Pause in minutes before repetition?: 0
- Execute on workstation: Own
- 1. Comms: 22.09.2011
- Last Date: 22.09.2011

Password:**Password**

The Comms. password assigned by you when you added the session to the Comms. batch. The Comms. password cannot be changed for sessions added to the Comms. batch from other modules. You can change the password of Comms. download sessions.

For EBICS the log-on at the bank server is not longer made using a Comms. password, but using a signature. For the access to the Private Key necessary for this, a password is also required. For this, the "Comms. password" box -available in all necessary places in the program- is used.

Make Electronic Signature:**User name and password for the Electronic Signature**

If a procedure with Electronic Signature was selected on the *Attributes property page* for transmit sessions, then you can enter the **user**, who accomplishes the ES (default is the user currently logged in) and the **ES password** subsequently.

Other:**ID-Group**

According to the former DAD name, a ID-group can be assigned. Thereafter, it can be selected and so the processing can be structured.

Access class

In the file manager, the access class can also be set when adding a new file (cf. Chapter 7.8).

For this file, plan data shall be additionally generated in a new way

To generate also plan data for e. g. files from third-party systems which are sent using the file manager, you must highlight this checkbox. If the corresponding accounts are available, then the data (if applicable with own grouping name) will be included in the plan data.

Highlighting this checkbox can be predefined for each session type using the parameter **Generate plan data in file manager** (see Core chapter 6.4.1: *Session types property page*).

Execution frequency:**Repetition**

Open the list box with the drop-down arrow to define the repeat cycle for the download session. For transmit sessions a change of the repeat cycle is not possible (also: Last date).

- Once
- Hourly
- Every 3 hours
- Every 6 hours
- Twice daily
- Once daily
- Every weekday
- Three times per week
- Once per week
- Twice per month
- Once per month
- Every time (daily until successful)

The repetition "Every time (daily until successful)" starts (depending on the waiting period entered below) an order again and again until it is terminated once a day successfully with return code 1. This frequency should be chosen for collection orders which typically should be successful once a day (e.g. retrieve a/c. statements).

The frequency "Once" is suitable for orders which should be triggered manually as and if required (e.g. retrieval of ES logs). For this case, the checkbox "Start 'Collect data' always manually" should be activated additionally (see Chapter 5.1.2.2: *Post-processing and transfer parameters property page*).

More about how to create collection orders comfortably using a wizard can be found in Chapter 5.2: *Wizard for collecting data from several banks / Autodial function*.

Pause in minutes before repetition

Enter here the time (in minutes), if it should be waited a certain time before the repetition. When choosing the execution frequency "Every time (daily until successful)", the field is predefined with the value 30 (minutes).

1st transmission

Enter the date and time for the first processing of a Comms. session in this box. You can leave the box blank if you do not want to specify a particular date/time for first transmission.

Last date

If you want to limit the transmission period for a Comms. session, enter the date and time of last transmission. You can leave the box blank if you want to transmit the order in a particular cycle with no expiry date, or in the case of a one-off transmission. You can only edit this box if the session was not added to the Comms. batch from a module.

If entries are made in the fields for "1. Transmission" and "Last date", then collection orders can only be executed within the time frame defined for them, e.g. hourly from 0 a.m. to 12 p.m. (exclusive! I.e., at 12 p.m. no more order is executed).

On workstation:

If the program has been installed on a local computer (standard application), this box always contains the value "Own" in the Processing database details dialog box, i.e. all Comms. session files are started on your local PC.

In the case of a network installation or a configuration as a single workstation installation on a network drive, however, you can use this selection list box to define the computer configured for data communication from which the Comms. session will be started.

For the selection of the Comms. PC, only those PCs are offered in the list, for which Comms. parameters are defined. A PC once chosen is prompted as default for each following Comms.

Period (when data should be downloaded)

The "From" and "Until" boxes relate only to data downloads. When you add a new Comms. session, use this box to specify the period for downloading data (e.g. account data) from the bank. If you leave the box "Collect data from/until" blank, all data for the specified file type made available on the Bank computer that has not yet been downloaded will be downloaded.



You can only be sure that all data made available to you by the bank will be downloaded if you leave the "Collect data from/until" box blank and do not enter any date limit.

The Electronic Signature is executed after clicking on **[Save]**.

With collect sessions the new entry of an order is completed directly by pressing the **[Save]** button.

5.1.2 File Manager: View Details

To obtain details relating to a single record, select the corresponding database entry by positioning the cursor and confirming with <**Return**> or a double-click. You can also open a record by clicking on it with the right mouse button and then selecting the menu item -**View details**-.

A dialog box which contains various property pages will open. As View details is primarily a **display function**, the data can only be viewed here - with one exception - but cannot be edited. The corresponding boxes are therefore inactive.

The header of each property page contains the **file name** of the selected file (including full path details). General information on the file such as the **file type**, **BPD name**, **attributes** status and, in the case of the session being rejected, the name of the user who rejected the session as well as the time and date of the rejection.

Access class

In the detailed view, the access class can also be set, unless transferred automatically from a Payments module.

The part below differs between the two property pages.

- 5.1.2.1 *Communications property page*
- 5.1.2.2 *Post-processing and transfer parameter property page*
- 5.1.2.3 *Comms. log / ES log property page*

5.1.2.1 Communications property page

The fields of the *Communications property page* give information on the course of the processing of the respective order and the status of the Comms.

The screenshot shows a 'File manager' window with the 'Communications' tab selected. The 'Post-Processing' sub-tab is active. The 'File name' field contains 'E:_323\MCCWIN\DISPO1.IZV'. The 'BPD file name' field contains 'OMIEBICS' and 'EBICS to omikron test bank'. The 'File Type' is 'IZV Domestic payments file'. The 'Access class' is '?'. The 'Receive' checkbox is unchecked, and the 'Send' checkbox is checked. The 'Attribute' is 'T' and the 'Order number' is 'A020'. Below these fields is a table for 'Executed actions' with columns for 'Internal name', 'Date / Time', and 'Time'. The table contains one row for 'Order created' with internal name '1', date '06/07/12', and time '11:50'. Below the table are fields for 'Electronic signatures', 'Order number bank / Comms', 'Bank server time', 'Electronic signatures', 'ES required / made', 'Status original', 'Status signature', 'Comms', 'AC / Result / PRF2', and 'Comms'. The 'ES required / made' field shows '1 / 0'. The 'Status original' and 'Status signature' fields are dropdown menus. The 'Comms' field shows '0 / 0'. The 'AC / Result / PRF2' field is empty. The 'Comms' field is empty. The 'Order number bank / Comms' field is empty. The 'Bank server time' field is empty. The 'Electronic signatures' field is empty. The 'Executed actions' table is empty except for the first row. The 'File name' field is 'E:_323\MCCWIN\DISPO1.IZV'. The 'BPD file name' field is 'OMIEBICS' and 'EBICS to omikron test bank'. The 'File Type' is 'IZV Domestic payments file'. The 'Access class' is '?'. The 'Receive' checkbox is unchecked, and the 'Send' checkbox is checked. The 'Attribute' is 'T' and the 'Order number' is 'A020'. The 'Executed actions' table has columns for 'Internal name', 'Date / Time', and 'Time'. The table contains one row for 'Order created' with internal name '1', date '06/07/12', and time '11:50'. Below the table are fields for 'Electronic signatures', 'Order number bank / Comms', 'Bank server time', 'Electronic signatures', 'ES required / made', 'Status original', 'Status signature', 'Comms', 'AC / Result / PRF2', and 'Comms'. The 'ES required / made' field shows '1 / 0'. The 'Status original' and 'Status signature' fields are dropdown menus. The 'Comms' field shows '0 / 0'. The 'AC / Result / PRF2' field is empty. The 'Comms' field is empty. The 'Order number bank / Comms' field is empty. The 'Bank server time' field is empty. The 'Electronic signatures' field is empty.

Executed actions:

When entering the user (internal name), date and time of the action, you see who has created the order, who has rejected the order, who has approved the order (up to two approvals), who has made signatures (up to six Electronic signatures) and when transmission has started.

After the switch to the new protocol version H004 according to the EBICS specification version 2.5 the order numbers are allocated by the bank server for transmit sessions, but no longer by the client system. However, this is only important for the adaptation of bank and customer system (e.g. for protocols or distributed signature). Therefore, the processing remains unchanged, but the order number allocated by the bank system is displayed here as **Order number bank** additionally for analysis purposes.

In addition, you find here date and time of the **Comms.** on Customer and Bank server side (Bank server time).

Electronic signatures:

All information concerning the Electronic signature is combined here. So you can find here the number of Electronic signatures required/made and the status of original file as well as signature file.

Comms.:

The first "Result" box contains the **Return code** (= **RC**) sent by the bank to acknowledge whether the Comms. session was processed without error and if transmission was interrupted. A "1" means that the Comms. session was processed without error. Other Return codes are listed in Chapter 5.4: *Return codes*.

This is followed by a second result (sub-return code) and a checksum (**PRF2**). Finally two lines show the plain text of the return codes and the original file name.

5.1.2.2 Post-processing and transfer parameters property page

Information on the post-processing:

The *Post-processing and transfer parameters property page* contains, inter alia, an option for the further treatment of the file after the Comms.

I. e. the field "**Deletion by days**" can be edited here. For the time of the number of days entered there, the file remains saved in the system, even if no application has "strong interest" in this file type. After the expiry of this storage period, the file (and the entry in the database) will be deleted without further question.



Please note:

Only if the checkbox **Delete file after processing through all modules** is set for the respective **session type**, a received file will be deleted at next logon in the automat after all modules have processed this file with interest .

The screenshot shows the 'File manager' dialog box with the 'Post-Processing' tab selected. The 'File name' field contains 'E:\multlang\SPAWIN\11091403.CCT'. The 'BPD file name' field contains 'EBIXBANK'. The 'File type' field contains 'CCT SEPA Credit Transfer ZKA'. The 'Access class' field contains '?'. The 'Information on post-processing' section has a 'Deletion by days' field set to '30' and a 'Processed by module' section with several checkboxes. The 'Information on transmission' section has an 'ID-Group' field set to 'SPA20116', a 'File type' field set to 'Original/Signature together', an 'Encryption' field set to 'Encryption (Hybrid DES/RSA)', a 'Compression' checkbox checked, an 'Execute on workstation' field set to 'Own', an 'Execution frequency' field set to 'Once', a 'Repetition' field set to 'Once', a 'How many minutes pause before a repetition?' field set to '0', a 'Start 'collect data' allways manually' checkbox unchecked, a '1. Transmission' field set to '22.09.2011', a 'Last date' field set to '22.09.2011', a 'Next communication' field, and an 'Abbreviation for stack of orders' field set to 'SPA20116'. The 'Original file name' field at the bottom contains 'E:\MULTLANG\SPAWIN\11091403.CCT'. The dialog has 'Print', 'Help', and 'Save' buttons at the bottom right.

Below that the applications are shown, which have recorded an "interest" in the file ("**Processed by module**"). If the processing through a module occurred, this is indicated by showing the processing time here.



Assigning "interests" ensures that all applications which must access particular session types are provided with them for processing only once.

For example, Cash Management has a "**strong interest**" in session type "STA" in account data downloaded from the bank. This means that, irrespective of the storage period specified, the data is not deleted until the application(s) recorded as having a "strong interest" has/have processed the data flagged in this way.

If an application records a "**normal interest**", the data necessary for processing is deleted when the custody period expires. The data is deleted regardless of whether the application has already processed the data or not.

Information on the transmission:

According to the former DAD name, a **ID-Group** will be kept. Thereafter, it can be selected and so the processing can be structured.

File type

drop-down arrow to the right in the window to view a list of file types.

The file type of the file to be sent or to be received is shown. It distinctive between:

- Original file without signature
- Original file with signature
- Signature file

Depending on the used Comms. process, further attributes can be chosen here, e. g. **encryption** using a list box for the procedures FTAM or FTP or a **compression** via FLAM using a corresponding checkbox.

On workstation:

If the program has been installed on a local computer (standard application), this box always contains the value "Own" in the Processing database details dialog box, i.e. all Comms. session files are started on your local PC.

In the case of a network installation or a configuration as a single workstation installation on a network drive, however, you can use this selection list box to define the computer configured for data communication from which the Comms. session will be started.

Execution frequency:

The **Execution frequency** for repetitive sessions will be set here. Chose as execution frequency from the field "**Repetition**":

- Once
- Hourly
- Every 3 hours
- Every 6 hours
- Twice daily
- Once daily
- Every weekday
- Three times per week
- Once per week
- Twice per month
- Once per month
- Every time (daily until successful)

By selecting an appropriate item from the list you choose the favoured execution frequency.

The repetition "Every time (daily until successful)" starts (depending on the waiting period entered below) an order again and again until it is terminated once a day successfully with return code 1. This frequency should be chosen for collection orders which typically should be successful once a day (e.g. retrieve a/c. statements).

The frequency "Once" is suitable for orders which should be triggered manually as and if required (e.g. retrieval of ES logs). For this case, the checkbox "Start 'Collect data' always manually" should be activated additionally (see below).

Pause in minutes before repetition

Enter here the time (in minutes), if it should be waited a certain time before the repetition. When choosing the execution frequency "Every time (daily until successful)", the field is predefined with the value 30 (minutes).

Start 'Collect data' always manually

If a collection order is to be started always manually using the icon, then this check box is to be activated. If you have specified during the collection order definition via wizard the fact that you would like to start communication manually, the check box is already ticked (see Chapter 5.2: *Wizard for collecting data from several banks / Autodial function*).

1. Transmission**Last date**

Store the date for the first transmission of a file in the corresponding text box with date (to be included using the calendar) and time. For transmissions with Electronic signature, the date applies respectively for original file and signature file.

If the communication job is to be executed only to a defined date in an execution frequency entered before, thus define a last execution date with date (to be included using the calendar) and time. The communication job will no longer be executed if the last date has been exceeded.

Next communication

The "Next communication" field displays when a comms. order is pending execution for the next time. On the basis of the predefined frequency, the next execution time (date and time) is calculated and displayed.

For the Display of the next due date time in the overview of the file manager, see Chapter 5.1.1: *File Manager: Database overview*.

Abbreviation for order batch

In order to be able to combine communication orders in groups, they can be labelled with a collective abbreviation. The abbreviation (max. 8 digits alphanumerically) is assigned on setting up order batches (see Chapter 5.2: *Wizard for collecting data from several banks / Autodial function*).

If an order is assigned to such an order batch, then its abbreviation is displayed here.

Period (when data should be downloaded)

The "From" and "Until" boxes relate only to data downloads. When you add a new Comms. session, use this box to specify the period for downloading data (e.g. account data) from the bank. If you leave the box "Collect data from/until" blank, all data for the specified file type made available on the Bank computer that has not yet been downloaded will be downloaded.



Only if you leave the field "Collect data from/to" untagged and you do not enter a date limitation, you can be sure that you receive all data provided for you on bank side.



Please note:

With collection orders to be started manually the latter fields are generally deactivated and simple display boxes. The maintenance of these fields is only possible using the Wizard for collecting data from several banks (see Chapter 5.2).

5.1.2.3 Comms. log / ES log property page

On the *ES log property page* the results of collected bank logs (e.g. concerning signature check) are displayed. This property page, if available, is inserted between the two other property pages (the language of the contents depends on the language of the corresponding bank server).

With EBICS 2.5 as an alternative to the well-known session type PTK you can retrieve with the session type HAC a customer log in XML format. This is also allocated to the corresponding file manager entry and prepared for display analog to PTK.

Example:

File manager

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

File name: I:\MCC323R2\MCCWIN\SAV\12070602.IZV

BPD file name: EBC323KK | UFA-EBICSSERVER 3.22 auf LW K, | ES check OK

File type: IZV Domestic payments file ☐ Received **Attribute Order number**

Access class: ? ☒ Send **B** **AOB**

```

06.07.12 10:39:30    FILE_UPLOAD 120706105032529
                   Hostname   : EBICSUFA
                   Order      : IZV B03R
                   Customer   : EBC323KK Ebics BR 323
                   User       : EBC323IT
                   Result     : TS01 Die Übertragung der Datei war erfolgreich

06.07.12 10:39:30    ES_VERIFICATION 120706105032529
                   Hostname   : EBICSUFA
                   Order      : IZV B03R
                   Customer   : EBC323KK Ebics BR 323
                   User       : EBC323IT
                   User       : EBC323T2
                   Result     : DS01 Elektronische Unterschrift(en) korrekt

06.07.12 10:39:30    ORDER_HAC_FINAL_POS 120706105032529
                   Hostname   : EBICSUFA
                   Order      : IZV B03R
                   Customer   : EBC323KK Ebics BR 323
                   User       : EBC323IT

=====
G U T S C H R I F T E N
Bankleitzahl       : 20090700
Kontonummer       : 0030004712
Auftraggeber      : AUFTRAGGEBER 1
Erstellungsdatum  : 04.07.12
Anzahl der Zahlungssätze : 1
Summe der Beträge (EUR) : 67,00
Summe der Kontonummern : 30.004.712
Summe der Bankleitzahlen : 20.090.700
Ausführungstermin : 04.07.2012
=====

```

< Print Help Save

5.2 Wizard for collecting data from several banks / Autodial function

Comms. processes are normally background operations so that users can continue using other program functions even when transmission is taking place. A typical example for that kind of process is the collection of account information.

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**).

In addition you can start the collection orders manually by a mouse-click at any time using an icon from the toolbar.

To define or to change collection orders please choose the menu item -Assistant for 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.

By assigning different labellings using the "Order batch" function, different "batches" of collection orders can be administered (similarly to the DAD in former versions). By repeated calling of the wizard using the menu item different order batches for different purposes can thus be provided.

If collection orders are to be combined as "batches", then you can choose a description for such an **"Order batch"** using the list box "Abbreviation of batch order" (the order batch with the abbreviation "Automat" with an identical ID-Group [in the file manager] is always available as default entry and is immediately available for collection orders to be assigned individually).


New descriptions for order batches can be created using the adjacent [**New**] button. After pressing this button, you are prompted to enter an abbreviation (max. 8 digits alphanumeric) for the new order batch. Finally confirm your entry with [**OK**].

1 Select the banks and/or Session types/Define collection orders

Choose the bank from which you want to collect data by mouse-click from the list of banks ().

Check one of the **available** download **session types** for the selected **bank**. By pressing the

[**Add session type**] you will add the selected session type to the list of **pre-defined collection orders to your banks**.

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

Additionally, if you have marked a collection order in the list by mouse-click and if it is available from the transmission method, you can decide, whether you want to "**Compress** the downloaded **data**" and/or whether you want to "**Encrypt** the downloaded **data**".

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

To delete collection orders please mark the order in the list and then press the [**Remove marked collection order from processing**].

Execution frequency:

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

However, you can start all these orders at a time decided by you using the corresponding icon (see below) if you highlight the checkbox "**Start Comms. manually**".

Thus within a batch -similarly like in former times in a DAD- collection orders with different repetition cycles and periods can be defined, which are executed **only if due**, as soon as the batch is started manually via icon.



Please note:

Settings in this area restrict the possibility for the execution of collection orders to be started manually (if they do not match the criteria selected here they are regarded as "not due").

So e.g. after the first manual start (of the batch) a collection order with the repetition cycle "Every hour" can be started again at the earliest after one hour by manual starting. Only then it is due again. If the batch is started manually in the meantime, the mentioned collection order remains unconsidered for execution.

If entries are made in the fields for "1. Transmission "and" Last date ", then the collection orders can only be executed within the time frame defined for them in each case by manual starting of the appropriate order batch, e.g. daily from 9 a.m. to 5 p.m. (exclusive! I.e., at 5 p.m. no more order is executed).

Use this setting (only time, no date) to restrict also the execution of automatic jobs which should be repeated several times a day to a defined time frame.

The autodial 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.

Repetition

Open the list box with the drop-down arrow to define the repeat cycle for the download session. If the session was added from a module, you cannot change the repeat cycle here.

Choose between

- Once
- Hourly
- Every 3 hours
- Every 6 hours

- Twice daily
- Once daily
- Every weekday
- Three times per week
- Once per week
- Twice per month
- Once per month
- Every time (daily until successful)

The frequency "Once" is suitable for orders which should be triggered manually as and if required (e.g. retrieval of ES logs). For this case, the checkbox "Start 'Collect data' always manually" should be activated additionally.

The repetition "Every time (daily until successful)" starts (depending on the waiting period entered below) an order again and again until it is terminated once a day successfully with return code 1. This frequency should be chosen for collection orders which typically should be successful once a day (e.g. retrieve a/c. statements).

Also with an execution started from the file manager the following waiting cycle is considered.

Pause in minutes before repetition

Enter here the time (in minutes), if it should be waited a certain time before the repetition. When choosing the execution frequency "Every time (daily until successful)", the field is predefined with the value 30 (minutes).

The entry "0" also corresponds to this value (default). To prevent too frequent collection processes, in case of a frequency "Every time (daily until successful)" and a pause < 10 minutes, the time period for the next transmission will be automatically increased up to "10" minutes.

1st transmission

Enter the date and time for the first processing of a Comms. session in this box. You can leave the box blank if you do not want to specify a particular date/time for first transmission.

Last date

If you want to limit the transmission period for a Comms. session, enter the date and time of last transmission. You can leave the box blank if you want to transmit the order in a particular cycle with no expiry date, or in the case of a one-off transmission. You can only edit this box if the session was not added to the Comms. batch from a module.

Then press [**Next >**].

2 Enter Comms. password

Enter your current Comms. password. 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.

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 >**].

Enter password

Bank(s) EBICS

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.

☐ Use the same Comms. password for all banks

Comms. password

EBICS

Please enter your valid password. This is used for validation of the communication access with the bank.

Password

< Zurück Weiter > Help

3 Start communication

If you have decided on the first page that you want to start the communication manually, you can finally define that the defined orders may **always be started** only on the **own PC** for **collection**. To do so, leave the corresponding checkbox highlighted. Otherwise, you can define behind "**On workstation:**" a PC within a network on which the Comms. batches should be processed (for autodial function as well).

Close this last step using the [**Complete**] button.

Then the Comms. session with the ID-Group "AUTOMAT" will be generated from your entries.

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

Start Comms.

If you want to start the communication manually, you can now define whether this is started in principle on the workstation, on which the menu item has been triggered.

☒ Always start retrieval on own workstation

Please define a workstation, on which the Comms. batches shall be processed.

On workstation: Own

< Zurück Fertig stellen Help

"Collect information from bank(s)" function / Autodial function (manually)

The **manual** starting of the autodial function for the processing of your defined collection orders is made from the main application window using the following icon from the toolbar:



If several order batches are available for communication which can be started manually, then after clicking the icon these are offered for selection, if they contain at least one due collection order just now:

**Please note:**

If a batch contains only orders, which are not due regarding to execution time and/or frequency (e.g. because the manual start time does not match a given time frame), this batch will not be offered for selection.

If no order batch to be started manually with at least one due collection order is available, "No record found." is displayed in the selection list:

Select the desired order batch by a mouse click and confirm with [**OK**]. Only the due orders of the chosen batch are then executed.

Subsequently, all orders with e.g. frequency "Once", for which the communication shall be executed manually (appropriate checkbox ticked, see above), are executed immediately and then set to the status "Pending Comms." afterwards irrespective of the result. Thus they can be started again manually at any time.

(If a date for the first transmission has been entered, the orders are not executed immediately, but to the given date.)

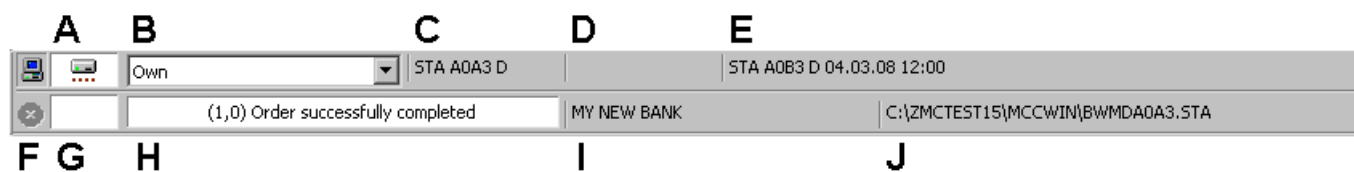
Orders with frequency "Every time (daily until successful)" can be started via icon until they have been successful once on the current day.

5.3 Execute Comms.




Comms. processes are normally background operations so that users can continue using other program functions even when transmission is taking place.

To execute the communication jobs included in the file manager, use the buttons [**Execute order**] or [**Execute all due orders**].

The execution of communication jobs is made automatically if a corresponding entry is available in the file manager and the **Comms. bar** can be seen on the screen (switchable using menu -View-).



Parts of the Comms. bar and what they show or effect:

A: Current status of the communication processing in symbols (disconnected mode:  , connected mode:  , post-processing mode: )

B: PC whose communication status should be displayed

C: Name of the Comms. batch just executed

D: Name of the Comms. module which is just active (Comms. process, e.g. MCFT, EBICS))

E: Next Comms. batch pending for execution

F: Stop button to cancel the Comms. batch currently executed

G: Status symbol of the communication job currently executed (e.g. connection, transfer direction, disconnection):  ,  ,  , 

H: Progress display of the Comms. batch currently executed / result

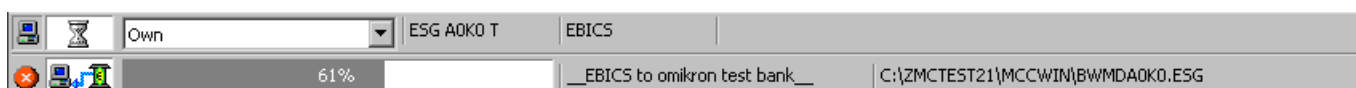
I: Name of the bank (parameter file) for which (currently) a Comms. is / was executed

J: Name of the file for the Comms. batch (currently) executed

Using a list box (field B) you can, if you work in a network, define the PC whose Comms. status shall be displayed in the Comms. bar.

If **no** Comms. batches are definitely pending for execution, thus the **Comms. bar** displays (if activated using -View- / -Comms. bar-) that no Comms. batch is currently in processing (**disconnected mode**, cf. to the bar above). In addition, you see in the Comms. bar which Comms. batch will be when processed next.

If Comms. batches are definitely pending for execution (execution time reached) or have been started, thus the Comms. bar changes immediately to the **connected mode**:

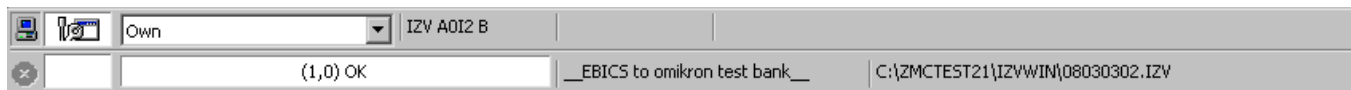


You can take the following information from the first line of the Comms. bar: Name of the Comms. batch just executed and name of the used Comms. process. Via the fields G and H in the second line you get further information about the status of the processing of the order.

Use the stop button (⊗) in the second line to cancel the Comms. just during execution. Clicking the stop button means that only the order just in execution is transferred per Comms. All following orders will not be processed.

The system shows either the message "Cancelled by user " or in case of creating the start block in an EPFT transmission "Error when creating the start message".

Data transmission remains active as long as due Comms. sessions are present. After closing the Comms., the Comms. bar changes to the **post-processing mode**:



Once all due sessions have been processed, the Comms. dialog box closes and data transmission ends with the corresponding return codes and message texts (e.g. "(1,0) Order successfully completed!").

After the transmission, the result of the last connection remains in the second line for control purposes.

As soon as the time for the execution of an automatic Comms. batch is reached, the Comms. starts again.

Using the item from the -View- menu you can activate the so-called **Comms. log**, which is displayed in a separate window (showing all data transmissions since program start). The window always remains as the highest window open and displays some information of the communications log. Successfully completed transmissions are identified by a green check mark (✓). If an error message occurs you will be warned by an appropriate symbol (⚠).

Comms. Log		
Time	Bank	Session type / Result / File
✓ 15:33-15:33	OMIEBICS	IZV Domestic payments file 1 (0) OK C:\...\MCCWIN\SAV\RESEND\09072201.IZV
✓ 15:37-15:37	OMIEBICS	PTK Receive log file 1 (0) positive Quittung erhalten
✓ 15:39-15:39	OMIEBICS	ESG Get file for distributed Signature 1 (0) OK
✓ 15:41-15:41	OMIEBICS	ESP Send distributed Signature 1 (0) OK
✓ 15:44-15:44	OMIEBICS	C:\...\MCCWIN\DAT\ESPA0B3.INF PTK Receive log file 1 (0) positive Quittung erhalten

In the event of transmission not being successfully completed, refer to the Comms. log for further details (see Chapter 6.10: Logs)

Special procedures when using the EPFT communication method:

If you want to transmit data using **EPFT**, the **start block** is generated first. The start block contains, amongst other information, the Customer Payment Key (**KZV**).

This key is calculated for each EPFT transmission. The message "**KZVUP Calculation**" is displayed whilst the key is being calculated. The Customer Payment Key (KZV) is a dynamic key calculated individually for each user using the **Diffie/Hellman Public Key Exchange** method. The key itself is not transmitted, but forms the start value for the subsequent **Customer Payment Key Recalculation**. Only the change calculated in the Customer Payment Key is transmitted to the bank. The start block is decoded by the bank computer.

The key is changed on both the bank and customer computers once transmission has been completed without errors. The Customer Payment Key must be then recalculated.

After recalculation, the Customer Payment Key is saved on the customer computer in encrypted form in the corresponding Bank Parameter Data file. If the Bank Parameter Data file is saved on a diskette, this **diskette** must remain in the floppy drive **until calculation of the new Customer Payment Key has been completed**.

Calculation of the new Customer Payment Key is finished when the message "KZV Recalculation" in the lower half of the screen disappears and the key has been written to the bank disk.

5.4 Return codes

The meaning of the Return codes depends on the Comms. method employed.

There are different types of Return codes:

- EPFT (MCFT) return codes
- FTAM return codes
- FTP Return codes
- EBICS return codes

The following list explains the meaning of the return codes issued by the bank computer. It is followed by a brief description of the possible error causes.



Lines marked by this symbol describe a suggested error rectification.



If you see this symbol, you should call your bank's systems consultant and notify the error.

The following **EPFT return codes** may be issued:

RC Meaning, cause and rectification of error

0 Transmission not yet started

No transmission has been started, or transmission was interrupted, e.g. due to poor line quality.



Start or repeat transmission.

1 Transmission successfully completed

Transmission was completed without any errors and no further action on your part is required.

In the case of a session with distributed signatures, return subcodes may still be transmitted using the MCDFUE process which specify the result in further detail, i.e.:

-1 Forwarded for second signature:

The signature was correct, but insufficient. The file will be provided to another customer authorised to enter the second signature.

-2 Insufficient signatures:

Will only be issued when a second signature is sent (session type ESP). The signature was received correctly, but must be completed by the second signature from another customer.

-3 File already processed:

Will only be issued when a second signature is sent (session type ESP). The signature was received correctly, but the file has already been fully signed by another customer. The signature sent is rejected by the bank.

-4 Last second signature insufficient

2*

Subscriber number not registered



Your subscribed number has been (accidentally) deleted on the bank computer.

3*

Incorrect transaction number



The bank computer expects different information from the information transmitted.

4

Transmission rejected by bank computer

The function -Download files- has not been performed on the bank computer for some time. The memory reserved for you has been allocated.



Repeat transmission later.

5*

User number blocked



Your user number has been blocked by the bank. You can no longer send data to or download data from the bank. You need a new bank diskette with a new Bank Parameter Data (BPD) file.

6

User entry busy

The bank computer is currently performing e.g. the function -Download files- which will free up memory for the files you have sent.



Repeat transmission later.

7* Invalid session type

The bank computer is unable to process the data type you have sent.

8* Installation routine not performed

Before you transfer data for the first time, you must perform an installation routine. This tells the bank computer that it must now expect data transfers from you. Without this installation, the bank computer will reject any attempt at transmission.



Initialise your password with (INI) or use the New User Wizard , to generate the initialisation sessions for EPFT and FTAM banks.

9 Internal error: see error log

The hard disk capacity of the bank is insufficient to save the data you have transferred. The bank must reorganise its hard disk.

10* File has already been transmitted

You tried to send a file which you have previously sent to the bank.

Please check whether you accidentally sent the file again or if you really want to retransmit this file.

If you really want to retransmit the file, call your bank's systems consultant. He will take the necessary action.



If you only initialised transmission of the file by accident, no further action on your part is required.

11 Transmission interrupted by bank computer

Transmission has been interrupted, possibly because of poor line quality.



Repeat transmission later

12 Incorrect checksum

The data have been corrupted, possibly due to poor line quality.



Repeat transmission later

13 No data available

The bank computer (currently) has no data which you can download.



Repeat your download attempt later

14* You have no transmission permission for this account

The transmission permission for a particular account has been deleted by the bank.

15* No authorisation for this session type

The bank has deleted, or has not issued, transmission permission for a particular data type (DTAUS file, DTAZV file, signature file, etc.).

16 Error during message logic check

The data have been corrupted, possibly due to poor line quality.



Repeat transmission later

17* User blocked after 3 unsuccessful attempts

Access to the bank computer has been blocked after you have entered a wrong user PIN to initialise a transmit/download session three times in a row. You can no longer send data to or download data from the bank. You need a new bank diskette with a new Bank Parameter Data (BPD) file.

18* Customer computer date invalid

The system data of your computer is more than 2 days ahead or 14 days before the bank computer's system date.



Check your system date with the DOS "date" command. Change the system date and repeat transmission.

19 Cancelled by user

Your computer's hard disk capacity is insufficient to save the data downloaded from the bank.



Reorganise your databases, e.g. by opening menu item -Admin.- / -Reorganisation- (see Core Module Chapter 7.3: *Database reorganisation*) or by backing up the data to external storage devices after closing the application to free space on your hard disk.

20 Cancelled with ESC

Transmission was cancelled by pressing <ESC> .

21* File has been manipulated (checksum)

Validation by the bank computer showed that the transmitted file had been manipulated in the customer computer after it had been added to a Comms. batch.



Replace the manipulated file and repeat transmission.

22 Can't write local file

An error occurred while the downloaded file was being written to your hard disk.



Check your hard disk and repeat transmission.

23* **Start message decryption error**

The user PIN you entered is no longer valid because it has already been changed.



Enter the currently valid PIN and repeat transmission/download.

25 **User not yet released**

Transmission was rejected because you have not yet been released in the bank computer.



Ask your bank's systems consultant why your user record has still not been released.

27 **Other order with bank not complete**

The transmission has been rejected, since your customer system has not completely closed a preceded communication with the relevant Bank server.



Before other files can be transmitted, you must first execute again the incomplete order which is marked with answer code 29 in order that it can be completely closed. Then the blocking of this bank will be automatically cancelled.

29 **Agreement bank is missing, please repeat**

The transmission of this order has not been completely closed because the connection is cancelled before the confirmation of the bank system has been received. The bank system can have correctly completed the processing or also can have registered a cancel. The status of this order is pending.



Please execute this order again in order that it can be completely closed. Hereby, the data will first not be transferred again, but the status of this order will be prompted at the bank. If the bank system has accepted the data, the status will be set to AC 1 and the order is positively closed. If the bank system has not received the data, the AC 11 will be set and the transmission will be repeated.

If the affected payment file is transferred with a new Comms. batch once again, this could lead to a double processing at the bank. Therefore the affected bank parameter file is blocked as long as the incomplete order is completely processed. For this reason, other orders to this bank will be cancelled during this period with AC 27.



Warning:

If the bank system cannot be reached for the renewed execution of the incomplete order, the AC 29 remains. You cannot be sure that the order is NOT received at the bank. Before you execute the order in another way, contact your bank. Only in this way double executions can be surely excluded!

The following EPFT Return codes occur only if you are using the EPFT communication method with Electronic Signature (= **MCFT**).

RC	Meaning
28	One or more signatures still missing The number of required signatures has not yet been reached.
30*	Public Key not yet released You sent a session type PUB, but this has not yet been released on the bank computer by <Shift>+<F8>.
31*	Electronic Signature incorrect 1. After the start block: ES verification failure. Reason: Customer is using an obsolete keypair. 2. After the trailer block: Hash value of the file is incorrect. Reason: The transmitted file does not match the signed file.
32*	No Public Key Your public key is not saved on the bank computer. This may be because you have generated a keypair but have not yet sent it to the bank.
33*	Inconsistent Signature file The signature is inconsistent because - the same user has signed more than once, - the timestamp of the original file is different.
34	Insufficient signatures The number of signatures entered is insufficient. One of the following return subcodes is issued: -2 Signature category is invalid The ES file contains an insufficient combination of signature categories. (E), (AA) and (AB) are valid. -5 The file must be signed. The file was sent without a signature, but this is required by the bank computer. -6 User not authorised to sign This user has signature category N.
35*	No signature permission for this account When the original file or the ESP file is sent, the account for which there is no permission is displayed in the Comms. batch. It may also be the case that the user does have signing permission, but that the user's signature category is insufficient.
36	Reserved (for internal control purposes)
37*	Limit exceeded

If Return codes marked * occur, the corresponding Comms. sessions are **not** automatically repeated as these involve serious errors or violations of the EPFT/MCDFUE security measures.

The following **FTAM Return codes** may be issued:

The explanations of the error causes, plus descriptions of how to rectify these errors, are contained in the corresponding RC numbers of the EPFT Return Codes.

RC	Meaning
0	Transmission not yet started
1	Order completed
2*	User ID not registered
3*	Incorrect password
5*	User ID locked
7*	Invalid order type
8*	User ID not initialised
9	Internal error
13	No data available (yet), try again later
15*	No authorisation for this session type
16	Formal error
17*	User ID locked after three unsuccessful attempts
24	No data available No data is available for downloading from the bank computer.
25	User ID not yet authorised
26*	Non-standard error; do not repeat transmission There is a malfunction on the bank computer.
27	Non-standard error; please repeat transmission Your record in the bank computer is being accessed, for example by a host process.
28	Negative acknowledgement; please repeat transmission (output text is variable)
29	Dial-up connection cancelled (output text is variable)

If Return codes marked * occur, the corresponding Comms. sessions are **not** automatically repeated as these involve serious errors or violations of the FTAM security measures.

The bank computer also issues the following return codes relating to **encryption**. These trigger off the corresponding customer system actions described below, as long as the customer system uses the "A3" application protocol version code in FTAM remote file names. (Older customer systems using version code "A2" generally do not receive these return codes.)

RC	Meaning
50	Action successful - Fetch new Bank Parameter data
51	Encryption code with the bank must be updated (session type VPB)
52	Data must be downloaded in encrypted form
53	Data must be downloaded in unencrypted form
54	Encryption code must be resent (VPK)
55	User does not have ES permission
56	Encryption code not yet released

The return codes are explained in Chapter 4.5.2: *Encryption return codes*.

In addition to the FTAM protocol return codes **which also apply to FTP**, the following return codes apply to online ES validation:

RC	Meaning
60	ES specified hash value OK
61	ES specified hash value not OK
62	ES OK
63	ES not OK, see log file
64	ES not validated, see log file
65	Data not yet ready, Pollingrate
66	Encryption version error You are trying to transmit data using an invalid version of the bank code. Your bank's systems consultant will ask you to download the current VPB.
67	Timestamp error The session you have generated is not within the bank computer's time window, i.e. it is too old or has been generated with a date in the future.

For **EBICS** a new systematic of six digit **return codes** was defined. The first two digits characterize the error class:

Error class	Meaning	Effect on current transaction
00	Information	none
01	Note	none
03	Warning	none
06	Error (unrecoverable)	none or increment of the recovery counter
09	Error (unrecoverable)	abort

Behind it, one digit for the EBICS identifier follows:

EBICS identifier	Meaning
0	no EBICS-specific return code (except "EBICS_OK")
1	EBICS-specific return code

Subsequently, one digit as identifier of a subcategory follows:

Subcategory	Meaning
0	no specific subcategory
1	Transaction management (technical)
2	Key management (functional)
3	Pre-validation (functional)

The last two digits characterize the specific error codes.

These EBICS return codes are mapped to the well-known return codes, in order to minimize the influence on the post-processing. The EBICS short text (if defined) and the associated symbolic name of the EBICS code are displayed in the text lines in the file manager and in the log.

With error class 06 the transaction can be continued after rectifying the error. The general action in this case is continuing the transaction after rectification of the error cause.

With error class 09 the transactions are aborted on bank side. The general action in this case is repeating the complete transaction after rectification of the error cause.

The following tables, which contain specific actions for some error codes, are structured for each EBICS return code (RC) according to the following scheme:

EBICS RC	Symbolic name	Return code
	Meaning, cause	Possible actions

Technical return codes:

00 0 0 00	EBICS_OK	01 OK
	On processing the EBICS request, no technical errors occurred.	
01 1 0 00	EBICS_DOWNLOAD_POSTPROCESS_DONE	01 Positive acknowledgement received
	After receipt of a positive acknowledgement the closing download processes were accomplished and the EBICS transaction was terminated.	
01 1 0 01	EBICS_DOWNLOAD_POSTPROCESS_SKIPPED	27 Negative acknowledgement received
	After receipt of a negative acknowledgement the transaction was terminated on server side without accomplishing the closing download processes.	
01 1 1 01	EBICS_TX_SEGMENT_NUMBER_UNDERRUN	27 Segment number has been under-run
	The total number of the segments transmitted in the transaction initialization has been under-run.	
03 1 0 01	EBICS_ORDER_PARAMS_IGNORED	27 Unknown order parameters are ignored
	Unknown order parameters were ignored (e.g. if OrderParams for Upload were given).	
06 1 0 01	EBICS_AUTHENTICATION_FAILED	27 Authentication signature defective
	The verification of the authentication signature was not successful.	
06 1 0 02	EBICS_INVALID_REQUEST	27 Message not EBICS-compliant
	The received message does not comply with the EBICS requirements syntactically.	
06 1 0 99	EBICS_INTERNAL_ERROR	27 Internal EBICS error
	While processing the EBICS requests, an internal error occurred.	
06 1 1 01	EBICS_TX_RECOVERY_SYNC	27 Synchronization required
	Starting the transaction again requires the synchronization between customer and bank system.	Continue the transaction by using the recovery point from the EBICS response of the bank systems.
09 1 0 02	EBICS_INVALID_USER_OR_USER_STATE	02 User unknown or user state incorrect
	Either the remitter of the order is unknown to the bank system, or the user state of the remitter stored in the bank system is invalid concerning the order type.	
09 1 0 03	EBICS_USER_UNKNOWN	02 User unknown

The remitter of the order is unknown to the bank system.

09 1 0 04 EBICS_INVALID_USER_STATE

02 User state incorrect

The user state of the remitter stored in the bank system is invalid concerning the session type.

09 1 0 05 EBICS_INVALID_ORDER_TYPE

07 Session type not allowed

The session type is unknown or not allowed to be used with EBICS.

09 1 0 06 EBICS_UNSUPPORTED_ORDER_TYPE

07 Session type not supported

The selected order type is optional with EBICS and is not supported by the bank.

09 1 0 07 EBICS_DISTRIBUTED_SIGNATURE_AUTHORISATION_FAILED

09 User has no signature authorization
i.e. verification defective

The user does not have an authorization to sign for the referenced order in the DES administration.

09 1 0 08 EBICS_BANK_PUBKEY_UPDATE_REQUIRED

66 Bank keys not valid

The public bank keys, which has the user available, are invalid.

Collection of the current bank keys via HPB

09 1 0 09 EBICS_SEGMENT_SIZE_EXCEEDED

26 Segment size exceeded

The defined size of an upload order data segment (with H002: 1 MB) was exceeded.

09 1 0 10 EBICS_INVALID_XML

26 XML not valid according to EBICS XML schema

XML validation against EBICS schema failed or XML not well-formed.

09 1 1 01 EBICS_TX_UNKNOWN_TXID

27 Transaction ID invalid

The transaction ID sent is invalid.

If the problem occurs on recovery with a recovery point before the last block:

Repeat with new transaction ID

If the problem occurs on recovery with a recovery point at the last block:

64 ES not validated, see log file

09 1 1 02 EBICS_TX_ABORT

27 Transaction aborted

The transaction was aborted on server side, since a recovery of the transaction is not supported or no longer possible due to a too high recovery counter.

09 1 1 03 EBICS_TX_MESSAGE_REPLAY

26 Message replay

	A message replay was recognized (duplicate nonce-timestamp pair).	
09 1 1 04	EBICS_TX_SEGMENT_NUMBER_EXCEEDED	26 Segment number exceeded
	The total segment number from the transaction initialization was exceeded.	
09 1 1 12	EBICS_INVALID_ORDER_PARAMS	26 Invalid order parameters
	The contents of OrderParams is invalid from content side, e.g. start after end at StandardOrderParams, fetchOffset with HVT greater than NumOrderInfos (total number of single order information in the order).	
09 1 1 13	EBICS_INVALID_REQUEST_CONTENT	26 Message content semantically not EBICS-compliant
	The received message corresponds syntactically to the EBICS XML schema, corresponds however semantically not to the EBICS requirements (e.g. IZV upload with UZHNN requires NumSegments = 0).	
09 1 1 17	EBICS_MAX_ORDER_DATA_SIZE_EXCEEDED	26 The Bank system does not support the required order size
	Upload or download of an incorrect large order file (e.g. for HVT, IZV, STA).	
09 1 1 18	EBICS_MAX_SEGMENTS_EXCEEDED	26 Maximum number of upload segments exceeded
	The bank system does not support the specified total number of segments for the upload.	
09 1 1 19	EBICS_MAX_TRANSACTIONS_EXCEEDED	26 Maximum number of parallel transaction per customer exceeded
	The maximum number of parallel EBICS transactions specified in the bank system for the customer was exceeded.	
09 1 1 20	EBICS_PARTNER_ID_MISMATCH	26 The PartnerID (=CustomerID) of the ES file does not match the PartnerID (=CustomerID) of the remitter
	On checking the remitted signatures in the user signature data document a partner ID was found, which is not identical to the partner ID of the user in the request header.	
09 1 1 21	EBICS_INCOMPATIBLE_ORDER_ATTRIBUTE	26 The indicated order attribute is not compatible to the order on the bank system
	E.g. order attribute "UZHNN" for order with order attribute "DZHNN", order attribute "DZHNN" for order with order attribute "UZHNN" or "OZHNN".	
	also: A file of this customer with the same order number (e.g. IZV A030) is already stored in the bank system.	Adapt next order number in the session types reference table and send order again.

Functional return codes:

00 0 0 00	EBICS_OK	01 OK
	On processing the EBICS request, no functional errors occurred.	
01 1 3 01	EBICS_NO_ONLINE_CHECKS	64 Pre-validation not supported i.e. ES not validated, see log file
	The optional pre-validation is not supported by the bank system.	
09 1 0 01	EBICS_DOWNLOAD_SIGNED_ONLY	26 Bank system requires signature
	The bank system supports only bank-functionally signed download order data for the sent order.	
09 1 0 02	EBICS_DOWNLOAD_UNSIGNED_ONLY	26 Bank system does not support signature
	The bank system supports only unsigned download order data for the sent order.	
09 0 0 03	EBICS_AUTHORISATION_FAILED	15 No authorization for this session type
	The user is not authorized to remit the order with the chosen session type.	
09 0 0 04	EBICS_INVALID_ORDER_DATA_FORMAT	26 Format errors in order data
	The transferred order data do not correspond to the defined format.	
09 0 0 05	EBICS_NO_DOWNLOAD_DATA_AVAILABLE	24 No data available at the moment i.e. no data available
	For the selected download session type no data are available at the moment.	Repeat download at a later time
09 0 0 06	EBICS_UNSUPPORTED_REQUEST_FOR_ORDER_INSTANCE	26 Request for this business transaction not possible
	The bank system does not support the selected order request for the concrete business transaction of the order.	
09 1 1 05	EBICS_RECOVERY_NOT_SUPPORTED	27 Bank system does not support recovery
	The bank system does not support recovery.	
09 1 1 11	EBICS_INVALID_SIGNATURE_FILE_FORMAT	33 Format errors in ES files i.e. inconsistent signature file
	The ES files sent do not correspond to the specified format. The ES file cannot be parsed syntactically (no bank-functional validation!).	
09 1 1 14	EBICS_ORDERID_UNKNOWN	26 Order ID unknown

The transmitted order ID is unknown. HVE, HVS, HVD, HVT with unknown combination partner ID (= customer ID) / order type / order ID.

09 1 1 15 EBICS_ORDERID_ALREADY_EXISTS

26 Order ID already existing

The transmitted order ID is already existing. For the customer an order with the same order ID was already remitted (duplicate order remittance).

09 1 1 16 EBICS_PROCESSING_ERROR

26 Other functional errors occurred

On processing the EBICS requests other functional errors occurred.
The message was correct, but could not be processed due to an other functional error.

09 1 2 01 EBICS_KEYMGMT_UNSUPPORTED_VERSION_SIGNATURE

26 Unsupported version of signature key

The algorithm version of the bank-functional signature key is not supported by the bank (order types INI and PUB).

INI: supported algorithm versions are given on the EBICS registration forms

PUB: supported algorithm versions are given in the bank parameters (HPD)

09 1 2 02 EBICS_KEYMGMT_UNSUPPORTED_VERSION_AUTHENTICATION

26 Unsupported version of authentication key

The algorithm version of the authentication key is not supported by the bank (order types HIA, HSA and HCA).

HIA, HSA: supported algorithm versions are given on the EBICS registration forms

HCA: supported algorithm versions are given in the bank parameters (HPD)

09 1 2 03 EBICS_KEYMGMT_UNSUPPORTED_VERSION_ENCRYPTION

26 Unsupported version of encryption key

The algorithm version of the encryption key is not supported by the bank (order types HIA, HSA and HCA).

HIA, HSA: supported algorithm versions are given on the EBICS registration forms

HCA: supported algorithm versions are given in the bank parameters (HPD)

09 1 2 04 EBICS_KEYMGMT_KEYLENGTH_ERROR_SIGNATURE

66 Invalid length of signature key

The key length of the bank-technical signature key is not supported by the bank (order types INI and PUB).

ask your bank for valid key lengths, generate new key

09 1 2 05 EBICS_KEYMGMT_KEYLENGTH_ERROR_AUTHENTICATION

66 Invalid length of authentication key

The key length of the authentication key is not supported by the bank (order types HIA, HSA and HCA).

ask your bank for valid key lengths, generate new key

09 1 2 06 EBICS_KEYMGMT_KEYLENGTH_ERROR_ENCRYPTION

66 Invalid length of encryption key

The key length of the encryption key is not supported by the bank (order types HIA, HSA and HCA).

ask your bank for valid key lengths, generate new key

09 1 2 07 EBICS_KEYMGMT_NO_X509_SUPPORT

66 Bank system does not support X.509 data

The bank system does not support the interpretation of X.509 data (order types INI, HIA, HSA, PUB, HCA).		
09 1 3 01	EBICS_SIGNATURE_VERIFICATION_FAILED	63 Verification of ES failed i.e. ES not OK
The verification of an ES failed. In the case of asynchronously accomplished orders the error can occur during the pre-validation.		
09 1 3 02	EBICS_ACCOUNT_AUTHORISATION_FAILED	14 Pre-validation account authorization failed i.e. no transmission permission for this account
The pre-validation of the account authorization failed.		
09 1 3 03	EBICS_AMOUNT_CHECK_FAILED	37 Pre-validation account limit failed i.e. limit exceeded
The pre-validation of the account limit failed.		
09 1 3 04	EBICS_SIGNER_UNKNOWN	02 Signature of an invalid user i.e. user number not registered
A signatory of the transmitted order is not a valid user.		
09 1 3 05	EBICS_INVALID_SIGNER_STATE	25 Signature with invalid user state i.e. user not yet released
The state of a signatory of the transmitted order is not valid.		
09 1 3 06	EBICS_DUPLICATE_SIGNATURE	33 The signatory has already signed this order i.e. inconsistent signature file
The transmitted order was already signed by the signatory.		

5.5 Post-processing / User Exits

A user-definable **UserCommsExit** is supported **after each transmission**. For each entry in the Comms. batch this exit will be called once.

The program will search for the "UserCommsExit.BAT" / "UserCommsExit.CMD" batch file or the "UserCommsExit.EXE" executable in the ..\MCCWIN or..\MCCWIN\PRG directory.

Within these files any script can be executed, e.g. for moving files.

If present, the exit is called with the following parameters (with the field length in brackets):

```
%1="aaa" file type/session type (3)
%2="A" transmission direction N, P or G (1)
%3="aaaa" job number (4)
%4="aaaaa" job attribute (5)
%5="aaaaaaaa" BPD name (8)
%6="aaaaaaaa" external user name/ user ID (8)
%7="n..n" Comms. return code (1-3)
%8="n..n" Comms. sub-return code (1-3)
%9="a..a" return text (0-40)
%10="a..a" return text part 2 (0-40)
%11="a..a" file name (0-128)
%12="a..a" access class (0-2)
%13="a..a" installation path inclusive working directory (max. 128)
%14="nnnnnnnn" organizational unit (8) [additional module]
%15="nnnnnnnn" client (8) [additional module]
```

All parameters are included in inverted commas. After call of the exit MultiCash waits on the completion of the process and then continues in the normal processing.

The exit is called **again globally** (i.e. not for each processed file) **at the end of a post processing cycle**, in order to make further actions possible at this time (e.g. moving all collected STA files).

In this case only in parameter %1 the content "/A" is entered.

UserCommsExit2 can be called

- after Comms. for each file and
- at the end of the post-processing one time for all files (e.g. to pass on AUSZUG.TXT/UMSATZ.TXT)

with the following parameters:

```
%1 Processing flag (0 = after Comms. for each file, 1 = one time after post-processing)
%2="a..a" file name (0-128)
%3="aaa" file type/session type (3)
%4="aaa" external session type FUL or FDL (3)
%5="a..a" file format (0-50)
%6="a" transmission direction N, P oder G(1)
%7="aaaa" job number (4)
%8="aaaaa" job attribute (5)
%9="aaaaaaaa" BPD name (8)
%10="a" test flag Y oder N (1)
%11="a...a" external user name/user ID (35)
%12="n..n" Comms. return code (1-3)
%13="n..n" Comms. sub-return code (1-3)
%14="a..a" return text (0-40)
```

%15="a..a" return text part 2 (0-40)
%16="a..a" installation path inclusive working directory (0-128)
%17="a..a" access class (0-2)
%18="nnnnnnnn" organizational unit (8) [additional module]
%19="nnnnnnnn" client (8) [additional module]
%20="aaaa" external job number (4)

5.6 Monthly statistics (supplementary module)

Use the menu item of the same name to get a **monthly statistics**.

By means of format subsystems, the transaction data of sent payment files are extracted for the monthly statistics. When exchanging other data such as, for example, a/c. statements, logs or exchange rates, the number of files is stored.

The collected information is stored month by month in aggregated form in a database table. In addition, the data are stored separated by

Organizational criteria of the operator:

- Unit (as far as the system is operated as ASP version)
- Organizational unit (as far as the Organizational Units module is installed)
- Access class (e.g. wage/salary)

Bank-technical criteria:

- Bank parameter file
- Session type (e.g. DP, FP)
- Transaction type (e.g. domestic payment with/without signature, direct debit with/without signature)
- Currency
- Bank-ID
- A/c. number

Separated by the above mentioned criteria, the following data are saved in each case:

- Date and time of the last data exchange
- Total amount per month
- Number of transactions per month
- Number of collective orders per month
- Number of files per month

In this process, the four last criteria are also registered for each day in the month in order that peak times can be located, as and when required.

For each of the above described criteria combinations, a totals record is displayed per month (in the record list of the database overview) as well as within the month the daily statistics (in the display area of the database overview).

By each criterion or by combinations thereof you can make selections and filter out with this the desired information. This is made either with the quick selection bar or using the standardized selection dialog.

In addition, the data can be output in classified print reports.

For the individual further processing of the statistical data you can define an export interface and then output the data in, for example, a CSV file.



Please note ...

By default, all statistics entries are kept for a period of 12 months. Older entries are deleted when starting the monthly statistics.

This storage period can be defined using a CSUB.PRO entry: STATISTIK_VERWAHRDAUER
nnn

This entry indicates the storage period in months. An entry of '1' would remove, for example, on 1.3.2012 all entries from January 2012 and earlier from the database.

Table of Contents: Chapter 6

	Page
6 Electronic Signature.....	6-2
6.1 Generate / Send ES keypair	6-3
6.2 Change ES Password.....	6-8
6.3 Convert signature version	6-9
6.3.1 Convert ES version from A003 to A004 (only for FTAM/FTP accesses)	6-10
6.3.2 Convert ES version to A005 / A006 or M005 / M006	6-12

6 Electronic Signature

The bank uses the Electronic Signature to identify the sender (customer). If all Electronic Signatures are correct, the bank executes your orders, transfers, direct debits, foreign payment orders, etc.



An Electronic Signature for an order can only be issued if you are using the Comms. methods MCFT, FTAM, FTP or EBICS.

The Electronic Signature is an encrypted confirmation of your payment orders and other instructions.

Encryption consists of two components, the ("secret") **Private Key** known only to you and the **Public Key** known also to your bank.

The Signature is generated with the Private Key and can therefore only originate from you. The Bank uses the Public Key to verify the Electronic Signature and its validity.

The procedure is based on internationally recognised cryptographic algorithms (RSA algorithm). The manipulation or forging of an Electronic Signature is de facto impossible.

You must generate the two keys (private and public key) needed to issue an Electronic Signature (cf. Chapter 6.1: *Generate / Send ES keypair*)

Following encryption, the private (secret) key is saved on an ES medium (see Chapter 6.1.5: *Electronic signature property page*) with an ES password of your choice. You must send the public key to your bank using session type PUB.

You can change the ES password using menu item -Communication- / -Change ES password-.

You sign your orders with the Electronic Signature either directly after the orders have been generated or later in the File Manager.

6.1 Generate / Send ES keypair

A key medium containing the private key encrypted with the ES password is needed to issue the Electronic Signature.

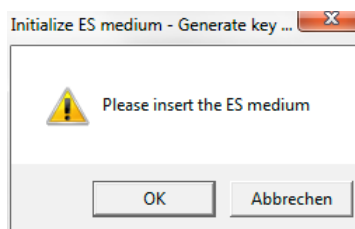
The public key of the keypair is saved on the hard disk in the file "<User>.<ES version>.PUB". You must send this key to your bank using session type PUB.

Keys already kept on a key medium can be transferred to the system.

A wizard will guide you through the steps that need to be taken to generate / to send a (new) keypair or to import an already existing one into the system.

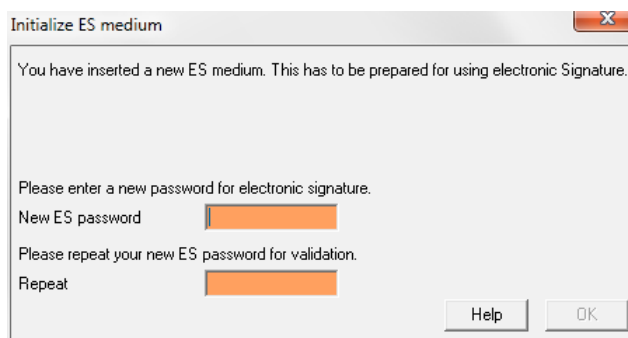
1 Initialize ES medium

In the first step you are prompted to insert the selected ES medium (see Chapter 6.1.5 in the Core module: *Electronic Signature property page*). 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.



Please note:

You must always enter the ES password when you sign a file. You cannot issue an Electronic Signature without a valid ES password.

You can change the ES password using menu item -Communication- / -Change ES password-.

2 Generate a new ES keypair / Import of keys



A separate keypair must be created for **each user** authorised to issue Electronic Signatures.

The **-Generate keypair-** checkbox in the dialog window is still ticked.

In order to generate a new keypair, you must 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.

If existing keys (e.g. generated before) should be sent to the bank(s) or keys provided on a key medium should be imported into the system, uncheck the check box mentioned above. On importing already existing keys you additionally have to enter the current valid **ES password** once in a field below.

Entry of the characters is concealed, i.e. each character you enter is represented by an * (asterisk).

Finally confirm your entry by clicking on [**Next**].

Incidentally:

Key calculation is based on prime numbers formed on the basis of the character string you have entered. The search for valid prime numbers may take some time.

At the same time as you save the private key on the diskette, the public key is copied to a file so that it can be transmitted to your bank. Your bank needs the public key to verify your Electronic Signature.

The public key is copied to a file in directory `..\DAT` with the extension **".PUB"**. The actual file name is formed from the name of the current user and the ES version.

Example:

If the name of the authorised user is "smith" and Mr. Smith generates a keypair, a file named `SMITH.<ES version>.PUB` is created in directory `..\DAT`. This file then contains the public key for transmission to the bank.

The Public Key needed by the bank to verify your Electronic Signature must be transmitted to the bank using session type **PUB**.

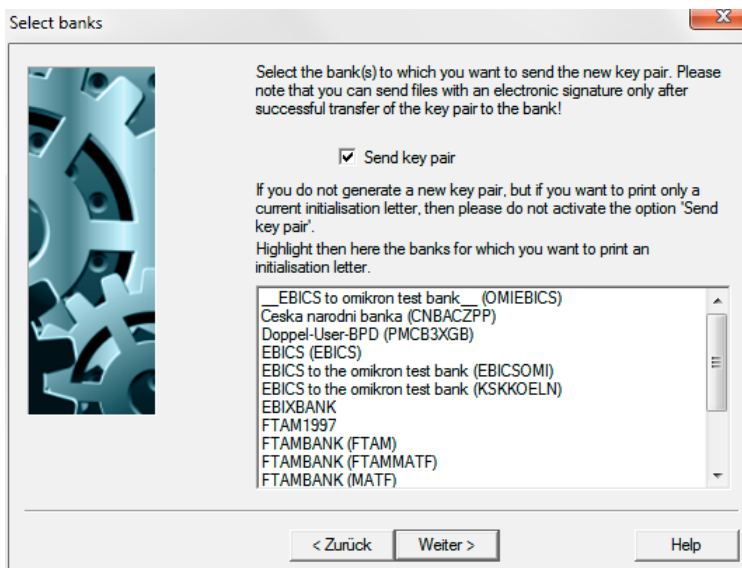
If you generate the keypair before starting the initialization session (session type **INI**), the public key is automatically sent to the bank during initialization.

**Please note:**

Each time you generate a new keypair, you **must** send the new public key to the bank before you can issue an Electronic Signature.

3 Select the bank(s)

Click on the bank(s) to which you want to send the new keypair. They can be selected from the list below the "**Send keypair**" box which is already checked.



If you only wish to print a current initialization letter and not to send a new keypair, please remove the tick in the check box.

You can select one or more banks from a list of available banks, for which an initialization letter should be printed.

Then press [**Next >**].

**Please note:**

It is only possible to send files with an Electronic Signature **after** keypair has been successfully sent to the bank.

4 Enter Comms. password

You have to enter the current Comms. password below the selected bank(s). This is needed by the bank to verify the change of key.

If you have selected several banks, you determine by ticking the "**Use the same Comms. password for all banks**" check box, that for all banks the same Comms. password is used. Otherwise you leave this option unchecked. Then for each selected bank the current valid Comms. password is prompted afterwards.

The password definition is concealed, i.e. when you press a key you only see an * (asterisk) on the screen. Close password definition by clicking on [**Next >**].

5 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.

The "**Print INI-Letter(s)**" option is still checked.

If you do not wish to print any initialization letter(s), uncheck the appropriate option.

Some banks support key activation using your current key, which is still valid. In this case the sending of an initialization letter to the bank is not necessary (see *Sending PUB orders with ES* in Chapter 6.3 for this).

If provided by your bank, you can enter your valid **ES password** to activate the new key directly using your current valid key.

As EBICS user with the status "Ready" you can update your bank specific keys using a PUB session. After choosing an EBICS BPD, the checkbox for the key activation is highlighted and disabled. You have to insert your signature medium and to enter the signature password (**ES password**). The new key is then signed with the old one. An INI letter is then not created for the EBICS access, since the authenticity of the transmitted keys is secured by the ES.

An exception exists, if you use a chip card, containing only the current key in each case. In this case, you first have to block your bank access (SPR session). Subsequent to this, execute an initialization with your new chip card then.

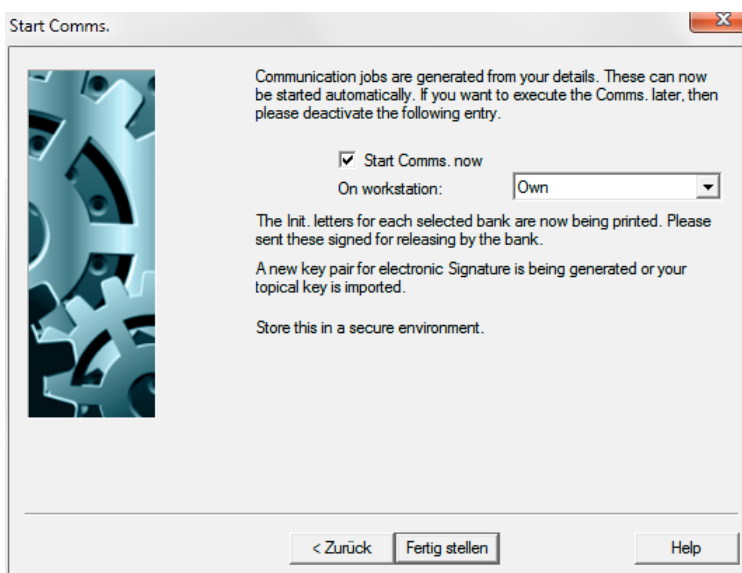
You have to click on [**Next >**] then.

You can go back to a previous step and make any necessary alterations using the [**< Back**] button.

6 Start communication

A Comms. session file is generated from your entries. Comms. can be started automatically during this last step if you confirm the default entry using the [**Complete**] button. If you do not wish to start the Comms. immediately, you will have to deactivate the entry "**Start Comms Now**".

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.



The new keypair for the Electronic Signature is then generated or the current key is imported into the system.



Always keep the ES medium in a secure place!

If you are using the immediate key activation option (by *Sending PUB orders with ES*), the issuing of the Electronic Signature follows directly.

Closing messages which appear after the successful generation of the key (such as the creation of a Comms. batch to send the key at a later time) quit by clicking on [**OK**].

Initialization letters will then be printed for each selected bank. Please sign this letter and send it to your bank to activate the keypair.

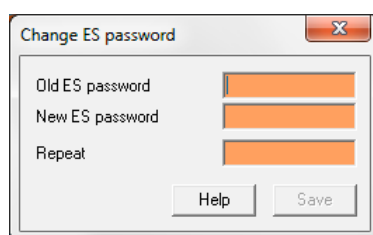
6.2 Change ES Password

The ES password is used to encrypt the private key saved on the ES medium. You can only issue an Electronic Signature after you have entered your ES password.

If you need to change the password for your key disk, choose menu item -Change ES password- in the -Communication- menu.

First you are prompted to insert your **ES medium** so that the private key on the medium can be encrypted using the new ES password. After inserting the ES medium press the [**OK**] button.

A message prompts you to enter the current (**old**) **ES password**. Then enter the **new ES password**. Entry is concealed, i.e. each character you enter is represented by an * (asterisk). You must then **repeat** entry of the new ES password for your own protection. Confirm your entry with [**OK**].

A screenshot of a Windows-style dialog box titled "Change ES password". The dialog has a standard title bar with a close button (X). Inside, there are three text input fields, each preceded by a label: "Old ES password", "New ES password", and "Repeat". The input fields are currently empty. At the bottom of the dialog, there are two buttons: "Help" and "Save".

Also confirm the closing message with [**OK**].



Because this procedure only involves the encryption of, and not any change to, the private key, there is no need to transmit the public key to your bank.

6.3 Convert signature version

The following describes two conversion wizards, which facilitate the upgrade to new Electronic Signature versions:

Chapter 6.3.1: *Convert ES version from A003 to A004*

Please note: This conversion is only possible for FTAM/FTP accesses.

Chapter 6.3.2: *Convert ES version from A004 to A005 / A006*

Please note: This conversion is only possible for EBICS accesses.

Since EBICS does not support the ES version A003, it is **not** possible to convert A003 to A005/A006 directly!

For the basic conversion of the FTAM/FTP Comms. procedure to EBICS see:

Chapter 4.6: *Convert FTAM/FTP bank access to EBICS*

Please note: This conversion is only possible for FTAM/FTP accesses with ES version A004.

6.3.1 Convert ES version from A003 to A004 (only for FTAM/FTP accesses)

Starting from program version 3.01.001, the Electronic signature will be supported in the new versions A004/M002 that work with 1024-bit signature keys:

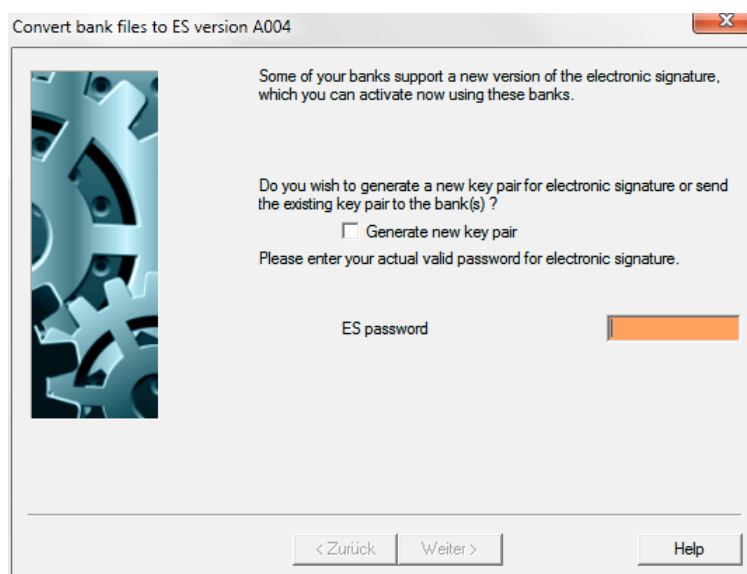
FTAM/FTP: Signature version A004

MCFT: Signature version M002

In addition to the extension of the signature keys it has been agreed with the banks to support the sending of the new Public Key with Electronic signature in order to facilitate the transition to the new signature.

While the keys are updated completely automatic with MCFT in the context of communication with the bank, with FTAM/FTP a comfortable conversion function enables the smooth transition to the new versions.

As soon as you have collected/received a bank parameter file from a bank where the support of the new signature version will be signaled to your system using the bank parameter string, you will be pointed out to the facts of the now possible conversion by a window when starting the program ("**Convert bank files to ES version A004**").

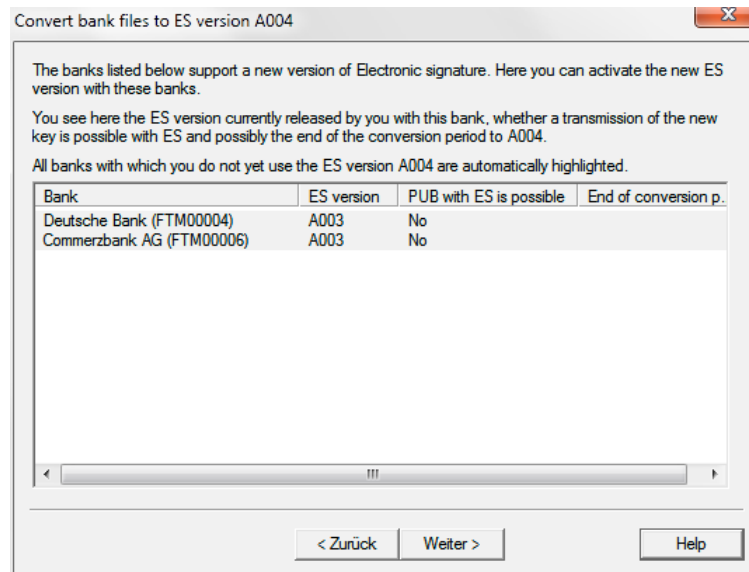


In order to generate a new keypair for the Electronic signature or send the generated keypair to the bank(s), follow the instructions already described in Chapter 6.1 ("Generate new keypair"). If you generate a new keypair, this will be made both in A003 format and A004 format. When executing the PUB order later, the Public Key will be sent in the new format to the banks that have signaled the support of the new ES version.

Using the [**Next**>] button you come to the next step of the wizard.

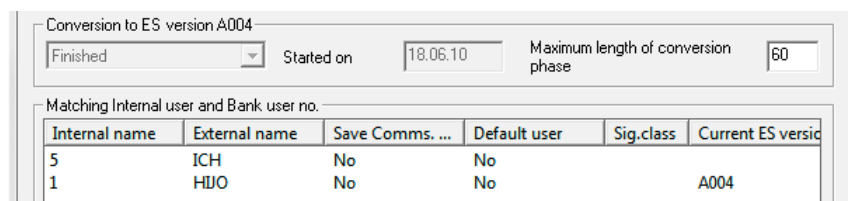
Apart from the name(s) of the bank(s) that offer(s) the conversion option, you find information on the ES version currently released with this bank (A003), whether a transmission of the new key is possible with Electronic signature and, if necessary, the end of the conversion period to the new ES version A004. All banks with which you do not use the new ES version A004 yet are automatically highlighted.

6.3.1 Convert ES version from A003 to A004 (only for FTAM/FTP accesses)



If the bank supports the sending of PUB orders with Electronic Signature, you can release the new key directly using your old key which is still valid. Then the sending of the initialization letter to the bank can be omitted. For this, enter your valid ES password in the corresponding field when following the wizard at that step where the print of the initialization letters is initiated and complete the wizard. In case of a positive ES check with your old key, the new key will be automatically activated and released. In case the signature check has failed, the key status at the bank will be set to "Initialized " and can be released as so far manually by an initialization letter. The same applies to the sending of PUB orders without ES.

After the conversion you make signatures in A004 format that can be combined with signatures in A003 format by other users until all users have converted their signature versions. Each ES version currently used will be displayed in the FTAM or FTP bank parameter files for each user along with information on the status of the ES conversion process (not started, can be started, started, ready), on the start of the conversion and on the max. length of the conversion phase (60 days by default).



6.3.2 Convert ES version to A005 / A006 or M005 / M006

Starting from program version 3.22.001, the Electronic signature will be supported in the new versions A005 / A006 and/or M005 / M006 that work with signature keys of 1536-4096 bit length (Default: 2048).

EBICS: Signature version A005 / A006 (EBICS version 2.4, EBICS protocol version H003)

A005 for smartcards, which support only this
A006 always for software ES/ES server / all other smartcards

MCFT: Signature version M005 / M006 analogously

For EBICS and MCFT, a similar procedure for the conversion of the signature keys is used. Each day, the first time the user logs on, a wizard will prompt the user to make the changes, if the bank systems have signalized the support of the new procedures (e.g. cf. to Chapter 3.5: *EBICS*: EBICS parameters). You can simply cancel this wizard if you don't want to make the conversion at that moment.



The key container files will now be converted and cannot be used further in older program versions!

If you decide on the conversion of the signatures, the program leads you as follows through the migration process:

1.

If you use a smartcard please note this special case: Some smartcards come with a fixed key and don't support the generation of a new key pair (e.g. the SECCOS smartcard of the German banking community). If you work with this card you can switch to the new signature version only, if you have received a new appropriate smartcard. Due to the fact that the new key has to be signed with the old one, you have to change the cards in your reader during the conversion procedure. In this case the system behaves like this:

If no smartcard is placed in the reader during first program start of the day (per user) and all defined banks have signalized to support the new signature versions A005/A006 or M005/M006 the following advice will be displayed:

If you have received a new chip card and you want to change your signature to the recommended new version, insert your new chip card and follow this wizard to the end!

Please insert now the new smartcard and proceed.

2.

If you use the SECCOS smartcard the new public key is just imported.

In all other cases you generate a new key pair for the new signature procedure. The keys used so far remain unchanged so that the new keys can be signed with the old ones:

Convert bank files to ES version A005/A006/M005/M006

Some of your banks support a new version of the electronic signature, which you can activate now using these banks.

Do you wish to generate a new key pair for electronic signature or send the existing key pair to the bank(s) ?

☐ Generate new key pair

Please enter your actual valid password for electronic signature.

ES password

< Zurück Weiter > Help

3.

In the next step all banks for which the signature can be converted are displayed. You should convert all banks together:

Convert bank files to ES version A005/A006/M005/M006

The banks listed below support a new version of Electronic signature. Here you can activate the new ES version with these banks.

You see here the ES version currently released by you with this bank.

All banks with which you do not yet use the new ES version are automatically highlighted.

Bank	ES version
Ceska narodni banka (CNBACZPP)	M002
Omikron Test INTERN (MCFTBANK)	M002
MCFTBANK Omikron Test INTERN (MKA)	M003
Meine neue Hausbank (MKA77)	M003
Doppel-User-BPD (PMCB3XGB)	M002
Banco estandar (MCFT-BPD) (TESTBANK)	M003

< Zurück Weiter > Help

4.

Next, the communication password is prompted.

5.

By entering your ES password you now sign the new public keys (with your old one) so that no confirmation letter and no approval by the bank are required:

Please note that for EBICS a key change without signature is not planned.

If you use the SECCOS smartcard you are now asked to insert the old smartcard in order to sign the order with the old still valid key:

Please remove your new chip card and insert your current valid chip card!

6.

If you see this display, the key change has been completed and you can continue to work directly with the new keys:

All transmissions successfully completed.

Sample ES initialization letter

User name	Smith
Date	23.12.08
Time	13:21
User ID	00000002
Bank name	MCB30
ES version	M002

Public key for the
Electronic Signature

Exponent 1024

[illegible]

Modulus 1024

9b	5a	7c	f7	9d	49	68	23	38	c7	74	c4	32	df	0d	13
a1	5e	0c	64	9b	24	2c	df	b8	da	95	5e	53	76	c5	5e
80	00	53	10	b1	cc	3a	72	98	0d	0d	19	23	dd	63	85
ce	35	81	a3	96	44	da	c7	5d	62	03	74	57	b3	b4	23
2f	50	24	4c	a7	e4	60	4f	0f	dc	2e	34	39	11	57	15
6f	c0	92	de	d1	5d	66	83	93	3c	f0	a7	b6	56	35	f0
76	9f	a7	b9	9d	e0	12	5f	85	91	5e	3c	f2	ec	e2	60
50	87	b8	f7	36	c6	cf	54	da	7d	8a	8a	82	9d	cb	33

```
Hash      21 33 E7 30
          72 C4 EC EA
          64 DE CC 2B
          2E A7 CD B5
          E1 68 50 AC
```

I herewith confirm the above public
key for my Electronic Signature

Place/Date

[illegible]

Signature _____

Index**-A-**

- Access class
 - Detailed View of File Manager 5-20
 - New entry of Comms. session 5-18
- Access class in favourite 5-12
- Access data for EBICS 3-20
- Access data for EBICS (conversion wizard) 4-23
- Accomplish internal approval 5-8
- Account 3-37
- Activate encryption with banks 4-16
- Add data of known EBICS accesses 3-19
- Add data of known EBICS accesses (conversion wizard) 4-23
- Additional plan data generation 5-18
- Administration of key media 4-32
- Alternative number 2-5
- Assign certificate 4-42
- AT Commands 2-17
- Attributes property page 5-14
- Auftragsart HCA 4-26
- Authentication password
 - Change 4-31
- Authentication status of the bank 3-21
- Authentication versions 3-25
- Authorization by second TAN 3-33
- Autodial function 5-28
 - Enter Comms. password 5-30
- Autodial function (manually) 5-32
- Automatic deletion of files after processing 5-23
- Automatic retrieval of log files 3-21

-B-

- Backup private key 4-33
- Bank data 3-23
- Bank dialog 3-38
- Bank Parameter Data file 3-2
- Bank parameters 3-7
- Bank specific certificate for customer key 3-25
- Batch processing 5-4
- Baud 2-8
- Baud rate 2-5, 2-11
- Bits 2-5, 2-8, 2-11
- Block a Comms. access (Session type SPR) 4-13
- BPD file for HBCI 3-27
- BPD for EBICS 3-19
- BPD for EPFT 3-5
- BPD for FTAM 3-13
- BPD for FTP 3-17
- BPD for HBCI+ 3-32
- BPD for WOP 3-41
- BPD fur MCFT 3-5
- Break before repetition
 - Autodial function 5-30
 - Detailed View of File Manager 5-25

-C-

- Call PAD 2-8
- Cancel original order at the bank 5-9
- Cancellation of ESP orders 5-9
- Cancellation order HVS 5-9
- CAPI 2-12
- Certificate issued on 4-38
- Certification Authority 4-38
- Change Comms Password 4-3

- Change Comms. password (MCFT) 3-9
- Change EBICS Comms. password 4-31
- Change ES Password 6-8
- Character set for ETEBAC3 3-38
- Check access 3-20
- Check URL 3-20
- Clear the line 2-9
- Collect data from several banks 5-28
- Collect information from bank(s) function 5-32
- Collect retrievable session types 3-25
- Collection of account information 5-28
- Collection orders always be started on own PC 5-31
- Comms. bar 5-33
- Comms. log 5-34
- Comms. log property page 5-27
- Comms. methods 1-4
- Comms. mode 3-38
- Comms. parameters 2-3
- Comms. password 5-17
- Comms. password change (EBICS) 4-31
- Communication 1-3
- Communication menu 2-2
- Communications property page 5-21
- Compatibility settings 3-24
- Configure parameter cards 3-39
- Connect 2-9
- Context sensitive menu 5-7
- Conversion wizard A004 6-10
- Conversion wizard A005/A006 6-12
- Convert ES version from A003 to A004 6-10
- Convert ES version from A004 to A005 / A006 or M005 / M006 6-12
- Convert FTAM/FTP bank access to EBICS 4-22
- Convert signature version 6-9
- Cover letter for initialization letter 4-7
- Cover sheet for INI letter 4-7
- Create BPD 3-3
- Create ETEBAC3 BPD file 3-37
- Create keypair 6-3
- Customer ID for FTAM 3-14
- Customer logfile in XML format 3-21
- Customer no. 3-6

-D-

- Data communications 1-2
- Database overview
 - File Manager 5-3
- Deactivate account authorization (pre-validation) 3-25
- Deactivate recovery of aborted transmissions 3-25
- Default user 4-23
- Define Bank Parameter Data files 3-2
- Define collection orders from several banks 5-28
- Define default user 3-9
- Define EBICS communication address 4-23
- Delete all highlights from records (File Manager 5-8
- Delete file after processing through all modules 5-23
- Delete private key 4-33
- DES cancellation 5-9
- DES transaction details 5-9
- Description of bank parameter file 3-6
- Description of BPD file 3-37

- Dial command 2-5, 2-11
- Dialling 2-6, 2-11
- Diffie/Hellman Public Key Exchange 1-8
- Disconnect modem 2-6
- Display file (Favourite) 5-12
- Display file (File Manager) 5-10
- Distributed Electronic Signature (ES) with MCFT 1-11
- Distributed Signature with FTP 1-20
- Dot notation for IP address 3-6, 3-17
- Download bank parameters 3-26
- Download customer data 3-25
- Download subscriber data 3-25
- Download supported EBICS versions 3-21
- DS 1-19
- E-**
- EBICS 1-21
 - Change authentication keys 4-26
- EBICS bank server selection 3-19
- EBICS bank server selection (conversion wizard) 4-23
- EBICS BPD 3-19
- EBICS communication address 4-23
- EBICS customer ID 3-21
- EBICS customer logfile in XML format 3-21
- EBICS host name (bank parameter file) 3-21
- EBICS host name (conversion wizard) 4-23
- EBICS parameters 3-24
- EBICS protocol version 3-21
- EBICS protocol versions 3-25
- EBICS request HVT 5-9
- EBICS return codes 5-43
- EBICS URL (conversion wizard) 4-23
- EBICS URL check 3-20
- EBICS version 2.4 1-21
- Efficient maintenance of several orders 5-4
- Electronic Banking Internet Communication Standard 1-21
- Electronic Payment File Transfer 1-6
- Electronic Signature 4-17, 6-2
- Electronic Signature (ES) with MCFT 1-10
- Electronic signature in the new versions A004/M002 6-10
- Electronic Signature in the new versions A005 / A006 and/or M005 / M006 6-12
- Encryption for FTAM/FTP 4-15
- Encryption of files sent using FTAM 1-16
- Encryption return codes 4-21
- Encryption versions 3-26
- Enter Comms. password 6-5
- EPF return code 5-36
- EPFT 1-6
- EPFT BPD 3-5
- ES 4-17
- ES independently from the drive letter of the USB stick 4-33
- ES log property page 5-27
- ES password
 - New entry of Comms. session 5-18
- ESP order cancellation 5-9
- ETEBAC 1-26
- ETEBAC3 3-37
- Exchange EBICS authentication keys 4-26
- Execute Comms 5-33
- Execute favourites 5-11
- Execution frequency for repetitive sessions 5-24
- Exits 5-50
- Export bank parameter file 3-8
- Export MCFT BPD 3-12
- External name 3-22
- F-**
- Favourites execution 5-11
- FDL 1-21
- File deletion after processing 5-23
- File Manager 5-2
 - View details 5-20
- File table 5-2
- File Transfer Access Method 1-13
- File Transfer Protocol 1-18
- File type
 - Detailed View of File Manager 5-24
- File type (New entry file manager) 5-14
- First initialization of bank access 4-5
- First transmission
 - Autodial function 5-30
 - Detailed View of File Manager 5-25
 - New entry of Comms. session 5-19
- FLAM 1-13
- FTAM 1-13
- FTAM 4-17
- FTAM bank parameters 3-14
- FTAM BPD 3-13
- FTAM Host name 3-14
- FTAM Return code 5-41
- FTP 1-18, 4-17
- FTP BPD 3-17
- FTP return code 5-42
- FUL 1-21
- G-**
- Generate / Send ES keypair 6-3
- Generate a new ES keypair 6-3
- Generate certificate request 4-36, 4-39
- Generate new plan data 5-18
- Generate self-signed certificate 4-36
- Generate system key and certificate 4-35
- Generate TLS key and certificate 4-36
- Generation and verification of the 1-15
- Globally Unique Identifier 4-33
- H-**
- HAA 3-25
- HAC request 3-21
- Hang up 2-9
- Hang up command 2-6, 2-11
- HBCI 1-25
- HBCI Plus 1-25
- HBCI+ 1-25
- HBCI+ BPD 3-32
- HBCI-BPD 3-27
- HCA 4-26
- HEV request 3-21
- HIA 4-8
- HIA session type 4-8
- Historical inventory (File Manager) 5-3
- HKD 3-25
- HKD request 3-23
- Home Banking Computer Interface 1-25
- Host name for EBICS 4-23
- HPB 4-8, 4-27
- HPB session type 4-8
- HPD request 3-26
- HTD 3-25
- HTD requests 3-23

HVS cancellation order 5-9
HVT request 5-9

-I-

ID-Group
 Detailed View of File Manager 5-24
 New entry of Comms. session 5-18
Import certificate 4-41
Import certificate response 4-37
Import MCFT BPD 3-10
Import of keys 6-3
Import PKCS#7 certificate file 4-38
Init. String 1 2-8
Init. String 2 2-8
Initialisation string 2-5, 2-11
Initialize ES medium 6-3
Internal name 3-15, 3-22
Inventory, historical (File Manager) 5-3
ISA Server 2-14
ISDN 2-12
ISDN direct connection 3-37
ISDN no. of the bank 3-38
ISDN no. of TRANSPAC 3-38

-K-

Key media administration wizard 4-32

-L-

Last date
 Autodial function 5-30
 Detailed View of File Manager 5-25
 New entry of Comms. session 5-19
Last transmission on 3-38

-M-

Maintain period (HBCI und HBCI+) 3-35
Maintain TAN list (HBCI+) 3-36
Manage certificates 4-34
Manual update of bank accesses 3-21
Mark all records in File Manager 5-8
MCFT 1-9
MCFT BPD 3-5
MCFT BPD export 3-12
MCFT BPD import 3-10
MCFT not via proxy 2-14
Memory stick registered as ES medium 4-32
Modem PAD access 2-4
Modem type 2-4, 2-10
Modem-Modem direct connection 2-10
Monthly statistics (supplementary module) 5-52
Move private key 4-33
MSN (Multiple Subscriber Number with EURO-
 ISDN) 2-12
MultiCash FileTransfer 1-9
Multiple selection 5-4
Multi-user BPD 3-2, 3-10

-N-

Next communication
 Detailed view of File Manager 5-25
Normal interest 5-24
NUA 3-6
NUA prefix 2-8
Number 2-5

-O-

On workstation

Detailed View of File Manager 5-24
New entry of Comms. session 5-19
Online file transfer using EPFT 1-6
Operation mode for EBICS 3-21
Order batch
 Detailed View of File Manager 5-25
Order number bank 5-21
Order type FDL 1-21
Order type FUL 1-21
Original file 5-15
Original file retrieval 5-9

-P-

PAD Access 2-4
PAD answer 2-8
Parameter cards 3-39
Parameters for EBICS accesses (conversion
 wizard) 4-23
Parameters für EBICS accesses 3-20
Parity 2-5, 2-8
Parts of the Comms. bar 5-33
Password 2-5
 New entry of Comms. session 5-18
Password and execution data property page 5-17
Pause after Comms. for ETEBAC3 3-39
Payment Status Report instead of customer log
 file? 3-25
PCV 3-39
Period (when data should be downloaded) 5-19
Plan data for files from third-party systems 5-18
Port 2-5, 2-10
Post-processing 5-50
Post-processing and transfer parameters property
 page 5-23
Pre-validation deactivation 3-25
Print INI letter(s) 4-6
Print INI letter(s) without cover sheet 4-7
Print initialization letter(s) 4-18, 6-6
Priorities property page 2-15
Priorities property page (Comms. procedures) 2-15
Private key backup 4-33
Private key deletion 4-33
Private key moving 4-33
Proxy authentication protocols 2-14
Proxy settings 2-14
PSN ID 2-5
PUB orders with Electronic Signature 6-11

-R-

RC 5-22
Recovery deactivation 3-25
Register USB stick for electronic signature on a
 workstation 4-32
Repetition
 Autodial function 5-29
 Detailed View of File Manager 5-24
 New entry of Comms. session 5-18, 5-19
Request certificate of a Certification Authority (CA)
 4-36
Request of session types 3-25
Resend successfully sent files 5-8
Reset EPFT/MCFT communication access 4-10
Reset sorting of file manager entries 5-8
Reset via signature 4-11
Retrieval of log files 3-21
Retrieve DES transaction details 5-9
Retrieve original files exceeding limit 5-9
Return codes 5-35

Return codes for EBICS 5-43
Return codes for online ES validation 5-42
Revoke internal approval 5-8

-S-

Select bank property page 5-12
Select EBICS bank server 3-19
Select EBICS bank server (conversion wizard) 4-23
Select file property page 5-16
Select the bank(s) 6-5
Selection list Stock (File Manager) 5-3
Self-signed certificate for authentication and encryption key? 3-25
Self-signed certificate for signature key 3-25
Send keypair 6-3
Send with transport signature from favourite 5-12
Sending of PUB orders with ES 6-11
Session type HAA 3-25
Session type HAC 3-21
Session type HEV 3-21
Session type HIA 4-8
Session type HKD 3-23, 3-25
Session type HPB 4-8, 4-27
Session type HPD 3-26
Session type HTD 3-23, 3-25
Session type property page 5-14
Session types ACK or HAC 3-25
Session type HCA 4-26
Session type HPB 4-27
Signature file 5-15
Signature versions 3-26
Special communication functions 4-2
Start autodial function manually 5-28
Start Collectdata allways manually via icon
 Detailed View of File Manager 5-25
Start collection orders via icon 5-29
Start Comms. manually (collection orders) 5-29
Start communication 6-7
Statement number 3-35
Store GUID 4-33
Strong interest 5-24
Supported EBICS protocol versions 3-21
Supported EBICS versions 3-21
Suppress pre-validation 3-25
Suppress recovery 3-25

-T-

TCP/IP 3-6
TCP/IP connection property page 2-13

TCP/IP settings globally for all workstations 2-15
Technical user 4-23
Telephone link 2-6, 2-11
Test connection to the bank host 3-20
Test mode activated 3-25
Test mode available 3-25
Transaction details retrieval 5-9
Transaction number 3-36
Transfer of public bank keys 4-8
Transfer of the public bank keys 4-27
Transmission no. for ETEBAC3 3-38
Transmission of encrypted data using FTAM 1-17
TRANSPAC NUA 3-37
Transport signature from favourite 5-12
Type of customer log 3-21

-U-

Update existing bank accesses 3-21
URL check 3-20
URL of EBICS access (conversion wizard) 4-23
USB stick for the Electronic Signature to be registered on a specific computer 4-32
Use electronic signature for payment authorization 3-25
Use second TAN for transmission of payment orders? 3-33
Use TAN list of another bank parameter file? 3-33
User data field 3-39
User Exits 5-50
User ID 3-37
User number 3-6
UserCommsExit 5-50
UserCommsExit2 5-50
User-definable exit 5-50

-V-

View file button (Favourite) 5-12
View file button (File Manager) 5-10

-W-

Wizard for collecting data 5-28
Wizard for key media administration 4-32
WOP BPD 3-41

-X-

X.25-leased line 2-7
X25 NUA of the bank (X25 B-canal) 3-38