SECARTIS

STARCOIN Specification Purchase Terminal offline Transactions

Edition 10.06.2002

Author SECARTIS

Status DRAFT/CONFIDENTIAL

Version 0.0.9/Revision 07-06-02

Giesecke & Devrient GmbH
Prinzregentenstr. 159
Postfach 80 07 29
81607 München

Secartis AG
Bretonischer Ring 3
85630 Grasbrunn
Germany

Content

1 Introduction

1.1 Scope of this document

This document describes the IEP, ECH and Debit-POS offline payment functionality for STARCOIN purchase terminals.

1.2 Versions of this document

Version	Date	Changes	Author
0.0.9	07-06-02	First preliminary version of document	Secartis

? Tabelle 1: Versions of this document

1.3 Referenced documents

Version	Date	Name	Author
	08/96	STARCOS S 1.2 manual	G&D

? Tabelle 2: Refrenced documents

1.4 Notations

The term „terminal“ stands for any kind of card accepting device, like Point of sale terminals, ATMs, vending terminals, etc.

1.5 Overview

The terminal and terminal software are designed to handle cashless payment transactions through the use of a chip card. The terminal card (also called SAM – Secure Application Module) supports this objective by allowing a check on the correctness of the customer card (ICC – Integrated Chip Card) and the payment transaction. This specification describes three types of payment:

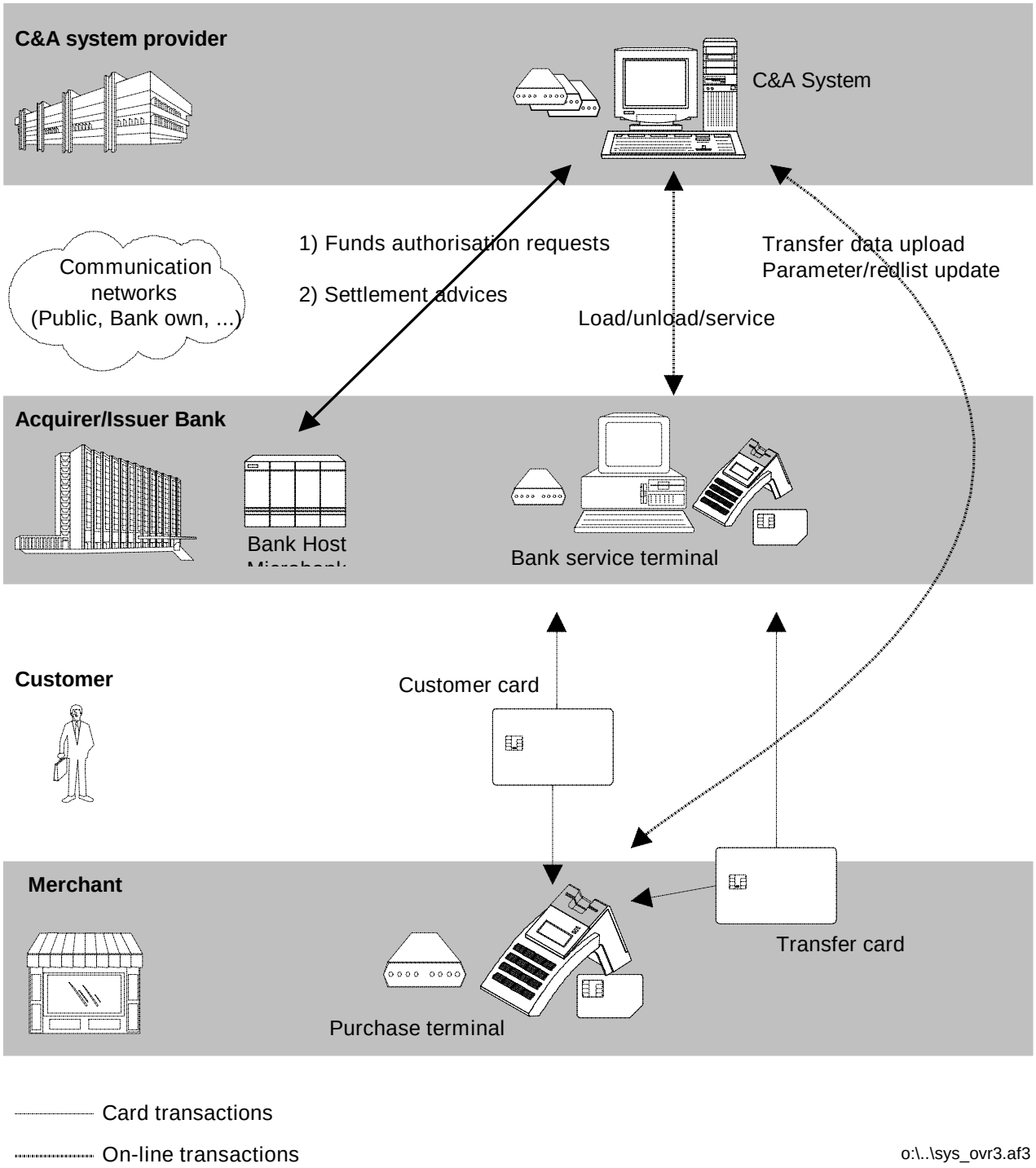
- IEP payment (payment by electronic purse)
- ECH payment (payment by electronic cheque)
- off-line Debit-POS payment.

Payments made and all other special events are logged and assembled for collection (sometimes also called reconciliation). "Collection" means the transfer of a number of transactions to the Clearing & Administration (C&A) system. The transfer may be made via special chip cards, the so-called transfer cards or a modem link.

The C&A system, on the other side, acknowledges Redlists (to block specified customer cards for payments), terminal parameter updates and terminal card parameter updates (for terminal card parameter maintenance) to the terminal.

1.6 Scheme structure

STARCOIN - System overview



This specification describes only the offline payment related purchase terminal functionality!

2 Hardware requirements

2.1 General requirements

- An off-line terminal must act without an on-line-connection to the host and has therefore to provide dedicated functions beneath the usual functionality of such a terminal. These functions are, primarily, controlling communication between the two chip cards, checking authorisation and recording the transactions.

- The terminal must be able to communicate by modem at a transmission rate of at least 9600 bits/sec. It must also have provision for automatic transfer of data via the modem interface starting at a preset time (± 15 min tolerance range).

- A (modular) integrated modem is desirable and would be vital for many installations.

- It must be possible to handle data exchange for transaction settlement alternatively by the chip card contacting unit or modem interface.

- The display should be able to show at least two lines of 16 characters each. The characters must be at least 5 mm in height and must be easy to read. Where a display has more than two lines, the number of characters per line may be reduced to 12.

- The customer keypad in offline Debit-POS terminals must have as minimum features: a numbers block, OK key (green), cancel key (red),clear/correction key (yellow) and menu key (blue).
  IEP only (!) terminals do not require a keypad at all.

- All keys must be marked to show their functions (i.e. "OK", "CANCEL", "CLEAR", "MENU").

- The PIN keypad should be on or above the electronics which in turn must be next to the chip card contacting unit. The PIN must not leave the terminal. No PIN encoding is permitted in the terminal. The PIN is encoded solely in the card.

- The layout of the PIN keypad must be designed according to ISO 9564.

- The keys must be easy to use and the customer must be able to feel or hear the keys being pressed.

- A visor should be provided to allow secure entry of the PIN code.

- The customer display must be controlled directly from the terminal electronics.

- Merchant terminals may use one keypad both for input by the dealer and by the customer (“turn-around terminal”). The keypad must support the requirements of the dealer keypad.

2.2 Requirements to be met by chip card readers

Each terminal must be provided with at least three chip card contacting units. One unit is used for customer cards (but may in addition be used for collection cards) while the remaining units are required solely for terminal cards (the security module for payment transactions). While the customer cards and collection cards must comply with the ISO standard (ISO 7816-1ff, ID-1), it is possible to design terminal cards (SAMs) as plug-in cards. The terminal operator can either exchange cards in a relative simple operation or get a fixed unit (that can be replaced only by service technicians). Either option must provide for security in ensuring that the customer cannot remove the terminal card.

- The chip card contacting unit must comply with ISO standard 7816-2 and should not be a "sliding reader" (except for the chip card contacting units for the terminal cards). External communication must meet ISO standard 7816-3 with protocol ‘T=1’ as well as protocol ‘T=0’, taking into account ‘direct convention’ as well as ‘indirect convention’. Adjustment to the chip card protocol must be automatic.

- The terminal software must be able to reset to the customer card.

- Provision must be made to prevent customers from removing terminal cards.

- Provision must be made to return the card to the customer under all circumstances (even in the case of a power failure). Where no dealer personnel is available in the vicinity of the terminal during operating hours to help customers in the case of a

failure, it must be possible for the customer to get back the card without the need for special tools or expertise.

- An interlocking device for the customer card would be desirable that blocks the card mechanically and releases it at the end of a transaction, upon abortion or in the event of a power failure.

- MTBF: 150,000 card cycles minimum (except chip card contacting unit for the terminal card).

- For electric properties see the chapter on the interface to the chip card.

- The terminal must have the ability to detect the removal of the cardholder card and has to call the customers attention to remove his card after the transaction has been finished (or aborted) by acoustic signal.

2.3 Memory requirements

The minimum memory requirement is calculated on the basis of the following criteria for merchant terminals:

- 800 (min.) transaction entries of approx. 70 bytes each

Data compression methods may be integrated to reduce the memory requirements, provided that the time limits are not exceeded.

Any further reserve capacities should be designed to be utilised by the transaction memory.

Please note: Memory must be maintained even after a power failure for at least 30 days.

2.4 Fields of application

The diversity of environments and resulting hardware requirements are not discussed at this point. Environments such as department stores, taxi cabs or parking lots have different needs with regard to temperature, dust, moisture, vibrations, etc., and different facilities (e.g. power supply).

The terminal may be used only in such locations and fields where it can truly meet all requirements and where it can be guaranteed that neither the customer card nor the terminal card will suffer any damage (not even minor damage) .

3 General requirements and functions

3.1 General operational sequence

After starting (Chapter 3.2), the terminal goes into its waiting mode. During this mode (basic state), the terminal must monitor the card reader for customer cards and monitor entries at the terminal.

A payment transaction is initiated by the entry of an amount for payment at the terminal (Chapter 3.4 Payments).

With specified cards, insertion of a card starts a processing sequence or the display of a message. Insertion of a transfer card (or an other collection device) initiates a collection and, depending on the menu settings, an exchange of data (Chapter3.6.2 Processing of a transfer card).

When corresponding flags are set on the terminal card, insertion of the customer card initiates a show of the credit balance still available for the electronic purse and/or electronic cheque on the customer display (Chapter 3.3 Display of customer card balance).

The customer display must indicate when the terminal is not ready to make payments. All error messages must be clear and easy to understand. For the terminal software to be accepted, its documentation must list all error messages and troubleshooting procedures available for the software.

Where a merchant display has been provided, the cause of the error must be output on this display.

3.2 System start

The system can only be started by inserting a terminal card in the card reader provided for this purpose. The terminal card must always be a prerequisite for starting the system. Where the terminal card is missing or when a not correctable error occurs during initialisation, an error message must be displayed (cf. above) and the program must be aborted.

When the terminal recognises a change of terminal cards (physical or logical change), it must generate a collection with defective terminal card independent of fact, whether not collected transactions are stored or not.

At the first start the terminal must read the terminal ID from the terminal card and store it. On every system start the terminal must read in from the terminal card the terminal ID

and the PSAM number. If the read terminal ID differs from the stored ID the terminal card has to be rejected. If the PSAM number differs from the last recently used value (this is only possible, if the terminal card has been changed) the terminal has to perform a collection and has to store the new NT_TK and NC from the terminal card. This data is the basis for further transactions (cf. chapter 3.5 Logging of transactions).

The files EF_TERM_CKT and EF_TERM_DIS of the terminal card hold parameters which are stored in terminal memory in parallel. If the terminal card has changed, the parameters have to be checked: The terminal may accept transactions only, if the terminal card is not locked and if it supports the 'type of transaction' held by the terminal card. The counter NT_COLL has to be taken over from the terminal card if the terminal card has changed. Special case: NT_COLL = 0 on a new terminal card means, that the terminal has to start with NT_COLL = 1.

When restarting the terminal, a check must be made whether automatic error correction (Chapter 3.4.1.9 Correction routine for IEP and ECH transactions) is required. If so, it must be done automatically or an appropriate message must be displayed (cf. Chapter 11).

These check must also be done before each transaction. This requirement is seen as fulfilled, if the check is done before the customer is invited to insert his card or before the first command to the customer card respectively. At this time an amount entered by the merchant may be rejected respectively an order of a connected cash register is answered negative according to the specified protocol.

3.3 Display of customer card balance

The remaining IEP balance is shown on the display upon insertion of the customer card only when the SHOW_CURRENT_BALANCE flag is set on the terminal card.

A customer card is recognised by the ATR. The ATR's historical bytes also include the balance of the first purse (IEP). The balance of the second purse must be read from the corresponding file in the card. When the ATR is correct, the balances can be indicated on the display. After a certain time or when the card is removed the balance(s) disappears from the display and the terminal returns into its basic state.

When the terminal recognises a wrong card or a card without a chip, it displays an error message and releases the card. Once the card is released, the error message disappears and the terminal returns to its basic or former state.

3.4 Payments

The type of payment – IEP/ECH/Debit-POS - is determined by the parameters of the terminal card and the facilities available to the customer card.

The parameters are obtained from the EF_SCN_VAR file and from the EF_TERM_DIS file of the terminal card (cf. file structure of the terminal card). Some terminal card parameters (value OPT_FUNCT in EF_TERM_DIS) define principal authorisation of the terminal for the IEP, ECH and offline POS functions, while a second parameter (IEP_POS_SWITCH) specifies the switching level (in actual currency) for the proposal of the payment type (e.g.: amounts below actual currency to be paid by IEP, amounts above the limit to be paid by offline POS). The first parameter (OPT_FUNCT) can be used to completely exclude one or more types of payment on a terminal. The terminal software must block types of payment when the hard- or software requirements are not available (e.g. no modem for an online Debit-POS) (cf.3.2).

3.4.1 Processing steps for payments

3.4.1.1 Entering the amount to be paid

The merchant enters the amount directly at the terminal. As long as the amount is not confirmed by pressing the ‘OK’ button, it can be deleted by pressing the ‘CLEAR’ button.

3.4.1.2 Inserting and checking the customer card

The customer card must be inserted in the terminal after the amount is entered and confirmed. Where this has not yet been done, the customer is prompted to insert the card. At present, for STARCOIN only such chip cards are accepted where their historical bytes have "SCN" as their content for the first three digits in response to the reset command (cf. ATR). All other cards must be refused with a message indicating that they are incorrect or faulty. Provision must also be made for error messages for a chip card inserted the wrong way round or in any other incorrect manner. It must be possible to abort the transaction at any time until the type of payment (IEP) or the PIN (ECH and POS) has been confirmed.

3.4.1.3 Selecting the type of payment depending on customer request and terminal parameters

Following ways to select the payment type are defined by now. For easy switch to a proposal of the terminal depending on the amount to be paid, variant 2 shall be prepared.

Variant 1:

If the customer card contains only one application (type of payment) or the terminal is an IEP terminal (vending machine terminals) and the customer card contains the IEP application, this type of payment is selected automatically. If the selected type of payment is available, the transaction starts without any further request.

Variant 2:

If the customer card contains more than one types of payments the terminal has to check which types of payment are available. If the applications are available depends on the balance (IEP/ECH) and on terminal card parameters. The terminal has to propose one of the possible types of paying methods with the following algorithm.

```
If AMOUNT > BAL_IEP or BAL_ECH then POS application
else if AMOUNT > IEP_POS_SWITCH then POS application
    else
        If AMOUNT > BAL_IEP then ECH  application
    else IEP application
```

Type and amount of the payment are shown on the customer-side display of the terminal and must be confirmed by the customer. If there is only one type of payment available (but the customer card contains more than one) then the customer has to confirm the selection too.

Where the customer requests it, it must be possible to change the proposed type of payment. Such a change by the customer should be possible by the same method at all terminals - to the extent permitted. Specifically, provided that the electronic purse/el. cheque is adequately filled, then the customer should be allowed to change from POS to IEP or ECH.

Changing the type of payment must be done as follows:

The amount and the proposed type of payment are shown on the display. With the ‘OK’ button the customer confirms the type and with the ‘MENU/INFO’ button the customer gets a list of all possible types. The customer can select a new one, confirm the selection and gets back to the old display were the transaction amount and the selected type of payment are shown.

3.4.1.4 Entering and checking the PIN code

This routine is performed only when off-line Debit-POS payment or the ECH payment has first been selected or determined.

The entry prompt is given after the payment amount is confirmed, card is inserted and the type of payment is selected. Entry must be made hidden, i.e. without a display of the code. It must be shown in a manner indicating the digit position of the figure just entered. The PIN code is checked through the STARCOIN function of the customer card. When the function recognises a wrong PIN code, a distinction is made whether the card is blocked (automatic blocking after n wrong attempts to enter the PIN code) or whether another try is allowed. An appropriate message must be displayed in either case.

3.4.1.5 Checking validity of the POS application

Using field AID_POS of the terminal card, the application must be found on the customer card (SELECT_FILE command). When the application is not found or is found to be faulty, no POS payment can be made. The system will automatically change over to an attempt at IEP (or ECH) payment.

After selecting the application, the command INIT_ATMPOS_REQ is executed.

Upon execution of command ATM_POS_TRX_REQ, a check must be made of the Completion Code, and any aborted payment due to limit overflow (e.g. weekly limit) must be indicated on the customer display.

Checks of completion codes of commands to the terminal card must also be made and in case of error an appropriate message has to be displayed.

3.4.1.6 Checking the validity of the purse/cheque applications (IEP/ECH application)

A search is made for the application on the customer card using field AID_IEP of the terminal card (SELECT_FILE command). When the application is not found or is faulty, no IEP or ECH payment may be made and the transaction must be aborted with a suitable message output on the display.

Please note: There are three different types of customers cards:

- IEP+POS el. purse ('DF 01') and Debit-POS ('DF 03')
- ECH+POS el. cheque ('DF 01' !!!) and Debit-POS ('DF 03')
- IEP+ECH+POS el. purse ('DF 01'), el. cheque ('DF 05') and Debit-POS ('DF 03')

Card containing either IEP+POS or ECH+POS can contain either a purse or an el. cheque in 'DF 01' (AID: DF40000001000002). The two different payment types can only

be differentiated by the POOL_ID. The MSB of the Pool Id for the el. cheque is always '1' !

The Completion Code of commands INIT_IEP_PURCHASE_REQ and DEBIT_IEP_REQ as well as the Completion Code of the terminal card commands must be checked and any error cause displayed.

3.4.1.7 Booking of payment

Actual execution and booking of the payment are performed as described in the section on the terminal payment transaction sequence. The customer card electronically signs the transaction. The sum counter on the terminal card is incremented by the amount of payment involved, and the customer card and terminal card file the transaction data in their memory.

For this, the terminal assigns a consecutive transaction counter for each POS transaction, each single IEP transaction, each ECH transaction, each terminal card parameter update and for the sum transaction (NT_COLL). The counter is assigned and incremented for each transaction that must be collected.

Even the most minor deviation from the strict structure of the sequence must cause the transaction to be aborted in line with the logging rules.

Chapter 3.5 Logging of transactions describes how the data are filed in the terminal when the payment transaction has been correctly completed and when a fault has occurred.

3.4.1.8 Error correction in general

In the event that a chip card communication error occurs during a payment transaction the system must attempt to correct the problem automatically (protocol T=0) or use protocol functions that provide for automatic corrections (protocol T=1).

For example, use must be made of the protocol feature for chip card communication that makes a new request for messages that have arrived incomplete. Corrections are allowed three retries before being finally aborted.

3.4.1.9 Correction routine for IEP and ECH transactions

A transaction for IEP/ECH payment that has proceeded until the end of step 5 (Chapter 4), may be repeated from the start. Transactions aborted between the beginning of step 6 and the end of step 9 have to be logged. They may be restarted beginning with the entry of the amount. The function TK_PSAM_CORRECT is necessary only from step 10 on. If TK_PSAM_COMPLETE results in an error, the terminal may no longer accept payment transactions.

If a fault occurs between processing of the first command DEBIT_IEP_REQ and command TK_IEPP_REQ (i.e. the terminal cannot verify whether or not the amount was

debited from the customer card), this must be logged for later filing with the system provider, to be followed by the correction routine described below.

After abortion of a transaction a reset of the terminal card has to be done before the next transaction.

The routine can be run automatically upon occurrence of a fault or after a power failure and resulting restart. The criterion for running the routine is as follows: the last transaction concerned the same customer card (same CARD_NR in ATR) as the one that is inserted, the amount was debited from the card (compare BAL_IEP in ATR), and the transaction was aborted within the sequence defined above.

Execution of the correction routine must also be logged and filed.

In case of IEP/ECH correction the single transaction record of the aborted transaction must be logged independently of the success of the correction routine. These corresponding records have to be filed immediately one after the other.

Correction routines at terminals with an interface to a cash register: The occurrence of an error causes abortion of the transaction. This abortion has to be reported to the cash register. If a correction transaction is required, the terminal has to report this to the cash register. The correction routine is started only if the cash register sends a corresponding command.

The function TK_PSAM_CORRECT

A new payment attempt is started until step INIT_IEPP_REQ. An RSA check is not necessary this time, because it has to be the same card that has been checked in the aborted transaction immediately before. The next checks and correction of sums, if any, will be performed by the TK_PSAM_CORRECT function of the terminal card

3.4.1.10 Treatment of errors

Case	Error at step	Correction transaction done			Collection record[1]	Display message after transaction has finished[2]
		YES		NO		
		OK	NOK			
A	1 - 9			X	E	“not successful” or error message
B	10	X			E+K	“successful”
C			X		E+K	“successful”
D				X	E	“not successful” or error message
E	11	X			E+K	“successful”
F			X		E+K	“successful”
G				X	E	“successful”
H	12			X	E	“successful”
I	13			X	E	“successful”

- table 3: TREATMENT OF ERRORS

Case	**Remark**
A	No correction transaction is started because neither at the customer card nor in the terminal booking took place. In case of abortion until step 6 no transaction record has to be created, from step 6 on it is mandatory.
B	IEP/ECH correction was done successfully. Customer and merchant account are correctly booked.
C	IEP/ECH correction was started and aborted. As the IEP/ECH correction may only be done if the customers purse has been debited, it is for sure that the balance of the IEP/ECH is decremented but the merchants account (pool sum on terminal card) was not credited.
D	For some reason IEP/ECH correction was not started. The merchants account (pool sum on terminal card) has not been credited - no statement can be given about the debit of the customers purse.
E	cf. case B
F	cf. case C
G	For some reason the IEP/ECH correction was not started. The merchants account (pool sum on terminal card) has not been credited - the customers purse is debited.

[1] If a correction transaction is started, the single transaction record (E) and the correction transaction record (K) have to be stored. The correction transaction record has to be transmitted directly after the single transaction record.

[2] Also for transactions which have been aborted for a longer time (e.g. after a power failure).

Case	Remark
H	If the function TK_PSAM_COMPLETE results in an error, the terminal has do shut down according to this specification (3.5.1.9). When the terminal crashes at this step, it has to check the PSAM-sum to see, whether this step was finished by the terminal card or not. If the terminal card has finished the function TK_PSAM_COMPLETE (the PSAM-sum is incremented), the error has to be marked as error at step 13, otherwise as error at step 12.
I	If the terminal fails in reading the missing data necessary for the log the error at step entry in the collection record has the value 13. All bookings have been finished correctly.

• Table 4: Treatment of errors - remarks

If the communication with a card causes an error, the error correcting measures of the protocol must be used (T=1). After three time retry, the transaction must be cancelled.

3.4.1.11 Completion of the transaction

Successful completion of a transaction is indicated and a message shown on the customer display to remind the customer to remove the card. Following removal of the card, the display must return to the "ready" message. The merchant display shows the status and amount of transaction after completion or abortion of the transaction. This message should remain on the merchant display until the next entry. When the customer card was removed too quickly or when the customer has interrupted/aborted the predefined sequence owing to a wrong entry during one of the above steps, the terminal, including customer card and terminal card, must remain in a stable state and there must be no unjustified financial advantage or disadvantage accruing to the merchant or customer.

3.5 Logging of transactions

An electronic log must at all times be made to cover all important transactions. This log is used for filing with system provider and also for statistical purposes.

3.5.1 Memory requirements

The log comprises basically the payment transactions and feedback to the sender (update confirmations) as single transactions. With regard to IEP transactions, the terminal card decides whether single transactions are to be logged or filed as summary data. For ECH and offline Debit-POS payments, each single transaction must be recorded. For an overview of data to be filed and the minimum requirements to be met by the log.

The terminal software must ensure that sufficient memory is available for all transaction data before a transaction starts. When no such guarantee can be given, the transaction

must not be started and the terminal is blocked for further transactions (with a suitable message displayed) until sufficient memory is available once again, e.g. by a transfer.

3.5.2 Preparations for transfers

Transactions must be assembled for later transfers. It must be possible to repeat transfers if an error should occur.

Completion of a collection routine is started with the chip card command "Initialise PSAM for off-line collection". This routine increments the counter on the terminal card (the NC field corresponds to the collection number). Administration of collection numbers must be performed by the terminal card. After the collection command the terminal has to make a transfer file including all transactions since the last collection.

The memory location for transactions may be freed only when it has been ensured that the current transactions have been correctly transmitted. Therefore each transfer file, containing the transactions, is answered by a specific confirmation. Only after receiving this confirmation the transactions of that specific transfer can be erased. If a transfer file is still unconfirmed after a certain time the terminal has to retransfer this transfer file automatically.

Provision must be made to allow different terminal cards to be used for operating the terminal (e.g. to change defective terminal cards). Different terminal cards mean several collections of entirely separate collection numbers.

3.5.3 Sum management for IEP transactions

For IEP transactions, the terminal card decides, on the basis of the transaction parameters and internal parameters, whether a single transaction has to be recorded. The terminal software obtains information on logging the single transaction only in the course of this transaction. Notwithstanding single transactions, it must always file the sum data for each pool on the terminal. The sum data includes a signature to allow collection in the event of failure of the terminal card. This means that, principally, each IEP transaction must be followed by an update on the sums (including electronic signature and NI counter) in the terminal memory.

Nevertheless in a standard case, the terminal must request the data again for collection because the signature for a completed collection is different from a preliminary signature. The (interim) sums and signatures available in the terminal memory are used only when the terminal card is defective.

3.5.4 Logging of aborted transactions

Security precautions for non-cash payment transactions make it necessary to record all irregularities that occur in connection with payment transactions. Aborted transactions must always be filed, even in those cases where no individual logging was provided for originally in the case of IEP transactions.

It should be noted that terminal failures may result in irregularities, so that the following procedure must be strictly adhered to:

- No transaction start unless adequate memory is available for logging.
- Payment transaction to be logged after receipt of a correct reply to the command TK_CHECK_RSA_REQ and setting of the step counter. (If the customer card does not answer or answers with a T=1 protocol error, logging can be waived.)
- Step counter (field "error during step") to be changed to the value as provided for in the chapter on the terminal payment transaction sequence and the completion code to 0 (in the case of a complete crash of the terminal software) before any other command.
- Data to be accepted into the transaction memory for each step and immediately when they are known.
- Completion code (CC) to be set after an abortion due to a specific completion code.
- Upon proper completion: Other parameters to be filled and step counter set to 0 or memory allocation freed when the single transaction need not be logged.

Updating parameters of the terminal card requires the following:

- Before starting the update of the terminal card parameters a collection command must be carried out
- The transaction must be logged before selecting the command TK_PAR_UPDATE_REQ with the update number and a completion code = "no reply" (‘0000’).
- The log data are completed and the completion code corrected after implementation of the command.

3.6 Transfer and acceptance of data

Data may be exchanged between the terminal and the C&A system via a chip card (called "transfer card" to denote its essential purpose) or a modem.

The first part of this chapter discusses generally valid routines for the transfer and acceptance of data and its consequences for the program sequence, starting from the assumption that it was already possible to read in the sub-files required for this purpose.

The second part of the chapter deals with the various types of transfer and covers the requirements for transferring the sub-files.

3.6.1 Transfer of transfer files

Transfer files may be transferred on a transfer card only when the transfer card has status 'S' for standard and correct mutual authentication has been performed.

All transaction records and parameter update confirmations must be transmitted. A transfer file is completed by a request for the sum records of PSAM and the collection number of the terminal card, even when the terminal card does not have the IEP/ECH function (command:: **TK_COLLECT**). The collection number thus obtained (NC) must be used. When the terminal card has the IEP/ECH function, the sums must be saved in the terminal and accepted into the sub-file.

Provision must be made to split a transfer file over several transfer cards (only when collection is implemented by means of transfer cards). For this purpose, the fields "subsequent number" and "flag completed" in the transfer file header must be noted. The sum check (XOR) and length apply for the relevant sub-file.

When preparing headers for transfer cards note that the file flag may be filled only at the end of processing.

Transfer files can automatically be assembled when a transfer card is inserted. The following transfer files must be sent:

- current data
- any transfer files not yet.
- unconfirmed transfer files (after a certain time span)

3.6.1.1 Special collection cases

3.6.1.1.1 Collection with defective terminal card

When collection with defective terminal card function is started automatically, all data to be transferred are collected from the terminal memory. They include all single transactions and the sum data from the last program start with the relevant terminal card or from the last IEP transaction. (cf. also chapter 3.2 System start)

Note for transfer cards: Collections with defective terminal card can be made only when the defective terminal card has been replaced by a new one (authentication).

3.6.2 Processing of a transfer card

A transfer card is recognised by its historical bytes in the ATR ("SCN_T"). Insertion of a transfer card automatically calls up the routine for processing the transfer card. This routine must also be selected when the terminal was blocked due to a terminal card parameter update (which incidentally allows unblocking the terminal by a new parameter update).

A message on the customer display and merchant display (if any) indicates that a transfer card has been recognised.

3.6.2.1 Reading in the status file

The file contains the card status, access conditions for the communication file and the maximum length of the communication file. It is always readable.

A faulty status file causes processing of the transfer card to be aborted and display of an error message.

3.6.2.2 Authentication of the transfer card

The authentication flag for the status file controls access to the communication file. When the flag is set to 1, a mutual authentication procedure must be performed to check correctness of the transfer card (cf. STARCOIN commands). Incorrect authentication aborts processing of the transfer card with an error message output. No reading or writing can then be done on the communication file without correct authentication.

Cards that do not require authentication may be used within limits only. Output of data (i.e. collections) is not permitted. Therefor all transfer cards with status ‘S’ have to be authenticated. Only transfer cards with status ‘U’ (update cards) can be cards without authentication.

3.6.2.3 Processing of the communication file

The communication file is made up of a discrete number of sub-files.

The general part of the header of a sub-file is standardised and applies to all sub-files. It allows skipping non-relevant sub-files.

The following rules apply for creating a sub-file on transfer cards:

- The terminal is only allowed to add sub-files, i.e. a search must be made for an end-of-file (‘FF’). The merchant terminal must not delete sub-files.

- All data of the sub-file including the remaining header must be correctly written before the file flag is set.
- XOR is determined by an XOR operation of all bytes, with allowance to be made for the file flag still to be written.
- The end-of-file (start of another sub-file) must be marked with ‘FF’.
- As the last sign handled, the file flag is set to the required value by ‘FF’. An XOR operation of all bytes of a sub-file will then always result in ‘00’ hex.

3.6.3 Data exchange via serial interface

The principles of data exchange handling have been defined to allow direct data exchange between the terminal and the system provider via modem

Terminals must be fitted for modem-to-modem connection (perhaps after retrofitting the respective terminal with the requisite hardware) and with a serial interface for direct connection. The chip card contacting unit for the customer card may be used as a serial interface. Units using such a serial interface (called "collection terminals") must be designed for maintenance and customer applications.

Changeover to another interface must be possible without any software update, i.e. just by changing the parameters (TYPE_OF_DATATRANSFER and special communication parameters).

The interfaces are not mandatory for automatic machines, for which specific concentrators may be provided for data exchange. When such concentrators are used, the machine supplier or operator must ensure that the requisite infrastructure is developed and maintained to allow data exchange.

3.6.3.1 Data exchange

The terminal transfers the following data:

- collections
- terminal status

This type of data exchange may also allow performing a software update directly by the terminal supplier, provided that the supplier has the correct signature for the new software release.

Processing of files transferred in this way is independent of the type of data exchange.

3.7 Special merchant functions

It should be possible to select these functions through the INFO or MENU key on the dealer terminal. Depending on the display capabilities, the menu must be designed to allow direct selection of each of these functions after pressing the INFO/MENU key (e.g. by entering a figure). Even less experienced users should be able to select functions by browsing through the list of functions.

3.7.1 Status of the last transaction

The result of the last transaction must be shown on the display. The initial data shown without any further keypad entries are:

- Result of the transaction
- Type of payment/transaction
- Amount of payment

Where the display dimensions do not permit showing the remaining information on the same page, it can be shown after paging down with the OK key:

Date and time of the transaction (provided that the terminal can supply the time)

3.7.2 Statistics

Statistics can be supplied for the period after the last collection of transaction data.

Statistical data may include:

- Sales (value) of all offline Debit-POS transactions with transaction number
- Sales (value) of all online Debit-POS transactions with transaction number
- Volume (sum) of online Debit-POS transactions
- All pool differences within the last collection
- Sales (value) of all ECH transactions
- Volume (sum) of ECH, pool and offline Debit-POS transactions
- Total volume of transactions

The data may be output on paper provided that a printer is hooked up to the terminal's serial interface.

3.7.3 Terminal status

This function provides data on the current status of the system. They include information on the following:

- Memory allocation with regard to transaction memory
- Transaction statistics (monitoring data)
- Settings of the terminals menu

The data must be printable provided that a printer is hooked up to the terminal's serial interface and can be displayed too.

3.7.4 Cash result

The cash result is the sum of all successful payment transactions since the last resetting of the cash result. A cash result may be made at the end of the day or when a new cashier takes over. It must be possible to view the resulting statistics separately from the collections as their underlying periods probably do not match.

The user manual of the terminal must include an instruction for the dealer to note the value of the transfer. This instruction is necessary because at a terminal without a printer the value of the transfer cannot be evaluated at a later time. A check of the remitted money is not possible at terminals without a printer. Therefor it must be possible that the terminal performs an automatic collection after resetting and optional printing the cash result.

3.7.5 Collections

3.7.5.1 Creating the collection

This function is the standard case (cf. Chapter *3.6.1 Transfer of transfer files*). Selecting the function on the menu allows output at another interface as well, as defined by the terminal parameters.

3.7.6 Terminal parameters

Selection of this menu item allows the user to see the current parameters of the terminal and terminal card and to update the parameters. It must be possible to change the following data using this function:

- Date and time of the terminal;
- Printer assignment.
- Parameters for interface and modem.
- All transactions must be output on the terminal printer, if any.
- Flag to define whether inserting the transfer card automatically initiates a collection.

- etc.

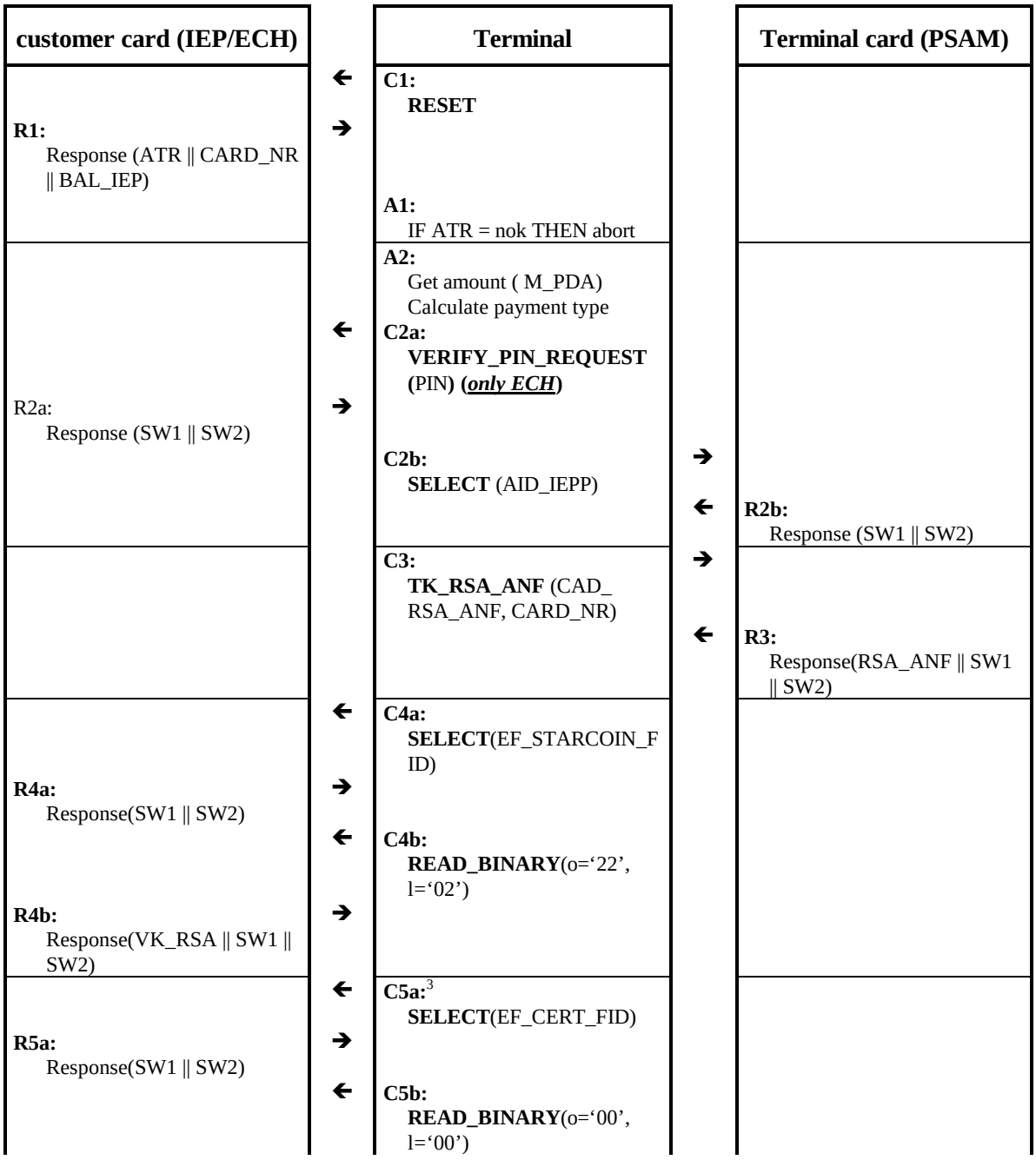
3.8 Principles of software extension

Provisions should be made to foresee the use of other terminal cards and an update of the software at some future date (e.g. to integrate new security requirements). The following principles apply:

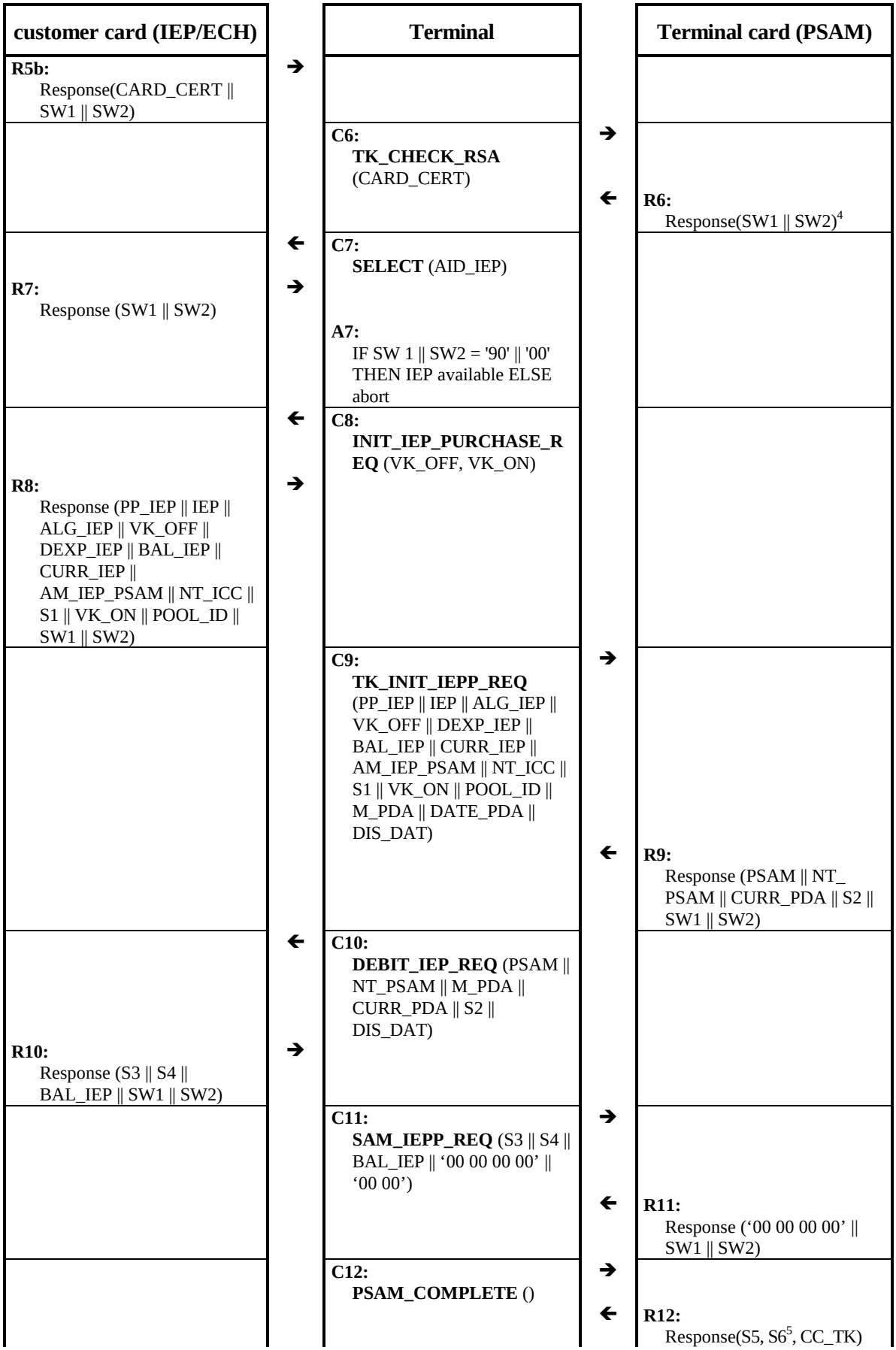
- Provision must be made for at least 2 terminal cards (SAMs).
- It must be possible to insert each terminal card into each card reader (no fixed assignment).
- One customer card must always be processed by just one terminal card.
- Each terminal card has a specific software allocated to it in the terminal which must be module-separated from the software for other terminal cards.
- It must be possible to assign two different software releases (old and new version) to one terminal card.
- It must be possible to replace by a new software each software for processing a terminal card and each independent module of the basic software through the channel used for transfer (except transfer cards). The documentation must include a detailed description of this process (and the modules used).
- It must be possible to load a software for processing a new terminal card through the same channel as is used for transfer. This process (and inclusion of the new terminal card) must be described in detail in the documentation.
- No existing transaction data must be lost during a software update.
  The terminal may run other applications than those specified here, provided that authorisation has been obtained for the software.

4 Payment transaction sequences in the terminal

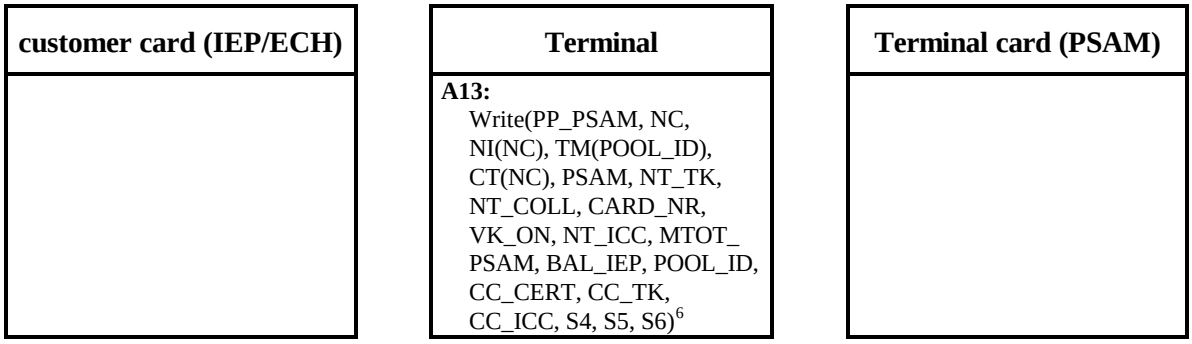
4.1 Payments by IEP/ECH



[3] Steps **4a** to **6** are executed only when the terminal card requests asymmetric check in RSA_ANF (in **R3**).



[4] Corresponds to CC_CERT.

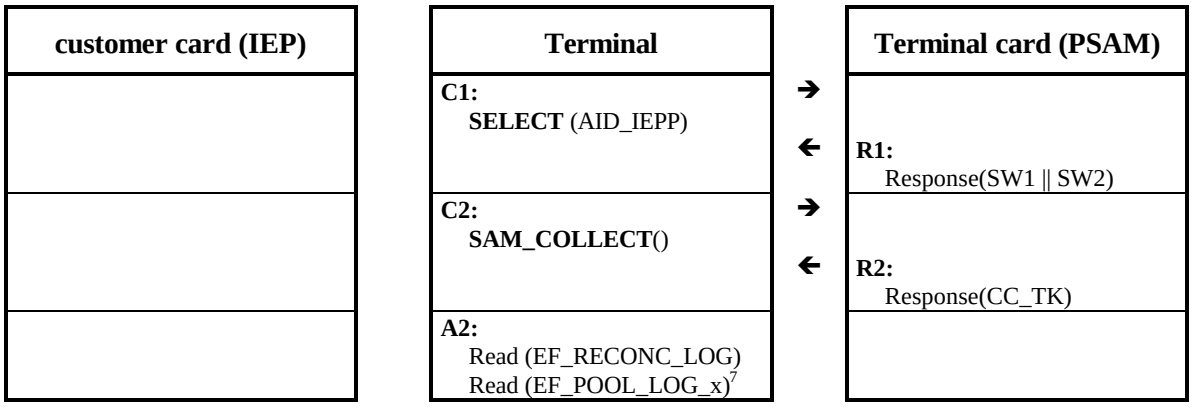


- Figure 1: IEP/ECH payment sequence in the terminal

[5] S6 is calculated and sent only when a single transaction has been created.
[6] The terminal must read in all data required for logging but not yet received, using READ_BINARY.

4.2 Off-line collection of a PSAM sum

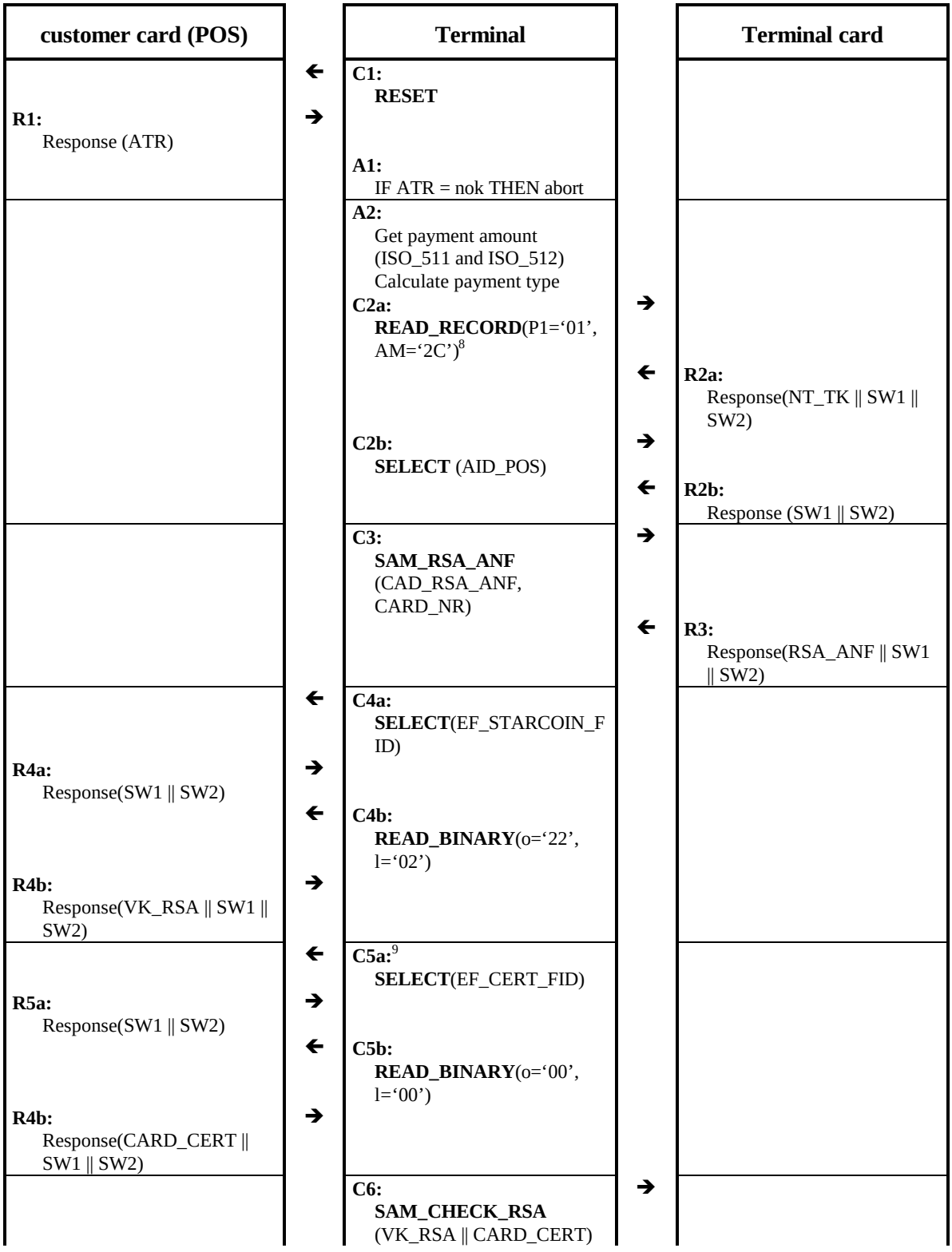
The offline collection is executed any time the accounting at the end-of-day has to be executed.



• Figure 2: Off-line collection of a PSAM sum

[7] File EF_POOL_LOG_x has several instances which represent the various pools. They must all be read by the terminal.

4.3 Off-line Debit-POS payment

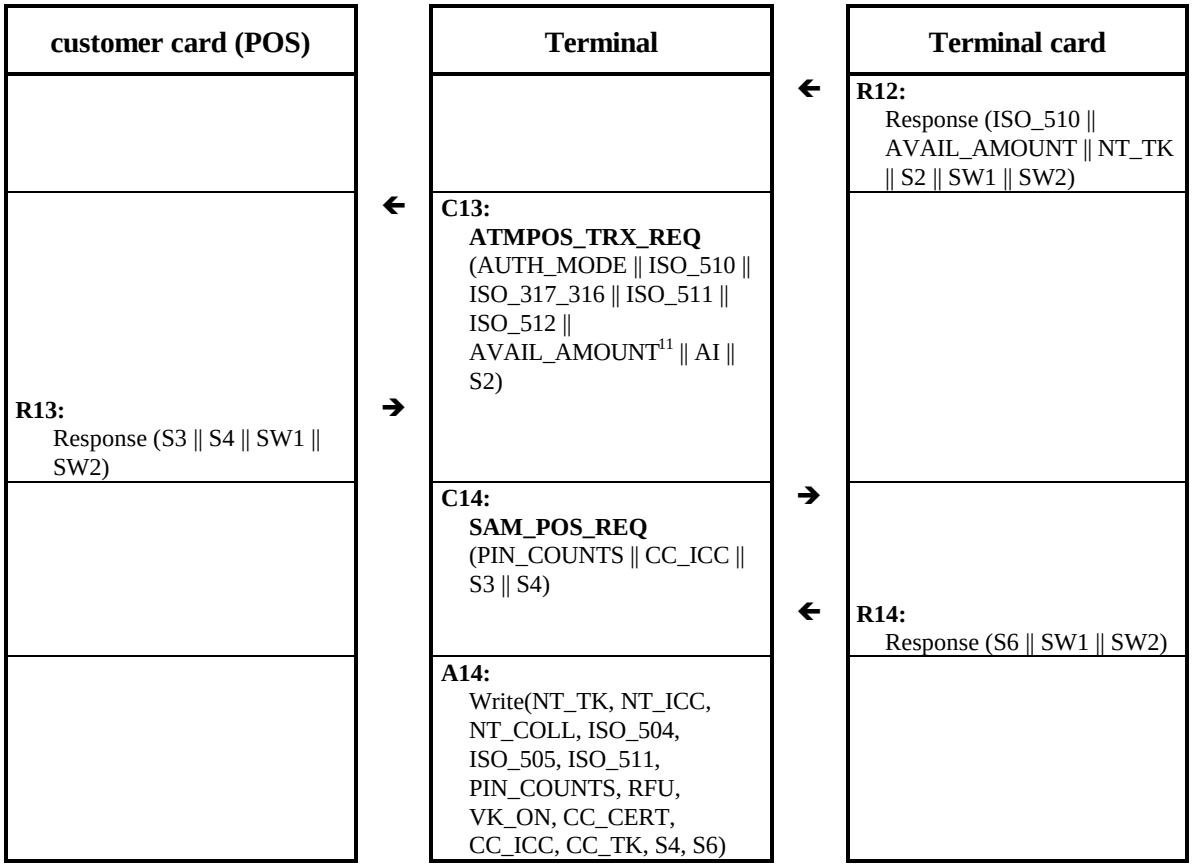


[8] Here the record containing NT_TK is read with implicite selection. If the terminal holds NT_TK in its memory, it is not necessary to read it again.

[9] Steps **4a** to **6** are executed only when the terminal card requests asymmetric check in RSA_ANF (in **R3**).

customer card (POS)		Terminal		Terminal card
			←	**R6:** Response(SW1 || SW2)[10]
	←	**C7:** **SELECT** (AID_POS)		
R7: Response (SW1 || SW2)	→	**A7:** IF SW 1 || SW2 = '90' || '00' THEN POS application available ELSE abort		
		C8:	→	
		A8:	←	**R8:**
	←	**C9:** **SAM_INIT_POS_REQ** (AUTH_MODE || VK_OFF || VK_ON || NT_TK || ISO_504 || ISO_505 || ISO_506)		
R9: Response (AUTH_MODE || ISO_305 || ISO_307 || ISO_310 || AWS || LKZ || DUPL_NUM || SECTOR_ID || ISO_403 || ISO_405 || ISO_407 || ISO_410 || ISO_411 || ISO_317_316 || ISO_401 || ISO_402 || ISO_404 || ISO_406 || ISO_406_TERM || ISO_408 || ISO_409 || VK_ON || VK_OFF || NT_ICC || PIN_REMAIN || S1 || SW1 || SW2)	→			
		A10: Find PIN_TRX		
	←	**C11:** **VERIFY_PIN_REQ** (PIN_TRX)		
R11: Response(SW1 || SW2)	→			
		C12: **SAM_INIT_POS_REQ** (ISO_305 || ISO_307 || ISO_310 || AWS || LKZ ||DUPL_NUM || ISO_403 || ISO_405 || ISO_407 || ISO_410 || ISO_411 || ISO_317_316 || ISO_401 || ISO_402 || ISO_404 || ISO_406 || ISO_406_TERM || ISO_408 || ISO_409 || VK_ON || VK_OFF || NT_ICC ||S1 || ISO_504 || ISO_505 ||ISO_511 || ISO_512 || AUTH_MODE || AI)	→	

[10] Corresponds to CC_CERT.



• Figure 3: Debit-POS off-line payment sequence in the terminal

Enter transaction amount (**A2**):

The entered tx amount

- must be > 0
- can be entered with minor units as defined in DF_POS.EF_POSPAR.ISO_317_316 (most significant nibble)
- has to be confirmed (e.g. by inserting the customers card)

During the entry of the amount, the user can cancel the transaction. When confirming, he can change the entered value.

The answer of the terminal card to SAM_RSA_ANF (**C3**) must be ’96 20’ for terminal cards verison 1.1 and ’90 00’ for terminal cards version 2.2.

TK_CHECK_RSA must only be executed, if response (**R3**) was ’90 00’.

Initialise offline Debit-POS transaction (INIT_POS_REQ,**C9**):

[11] Must be identical with ISO_510 for offlinePOS payment!

VK_OFF (corresponds to VK_POS_OFF of the terminal card), VK_ON (corresponds to VK_POS_ON of the terminal card) and ISO_506 are read from the terminal card during the initialisation routine.

AUTH_MODE is '08' for Debit-POS offline

ISO_504 and ISO_505, the transaction date and time are defined at the beginning of the transaction by the terminal.

NT_TK is the current transaction counter of the terminal card, read during the initialisation routine. Please note, that NT_TK must be incremented by '+1' in the command SAM_INIT_POS!

PIN entry and validation (**A10, C11**):

The entered PIN is sent with VERIFY_PIN_REQ to the customer card. If VERIFY_PIN_RESP = o.k. ('90 00'), the PIN is correct and the transaction can be continued.

If the completion code is '63 Cx' (x indicating the number of remaining trials), the cardholder must be informed to reenter the PIN or to cancel the transaction.

If the completion code is '63 C0' or any other value, the PIN is blocked and the transaction must be aborted.

The decision if on-line or offline Debit-POS transaction depends on several parameters. Offline is only allowed, as long all of the following statements are true:

- ISO_511 <= ISO_401_{ICC}
- ISO_511 <= ISO_401_{TK}
- ISO_402 > ISO_403
- ISO_504 - ISO_405 < ISO_404
- ISO_511 + ISO_407 <= ISO_406
- ISO_511 + ISO_407 <= ISO_406_{TERM}
- ISO_511 <= ISO_411
- ISO_511 <= ISO_408

SAM_POS_REQ validates S1 of the customers card and calculates S2 for off-line authentication.

ISO_305, ISO_307, ISO_310, AWS, LKZ, DUPL_NUM, SECTOR_ID, ISO_403, ISO_405, ISO_407, ISO_410, ISO_411, ISO_317_316, ISO_401, ISO_402, ISO_404, ISO_406, ISO_406_TERM, ISO_408, ISO_409, VK_ON_POS (corresponds to

VK_ON), VK_OFF_POS (corresponds to VK_OFF), NT_ICC and S1 are retrieved from INIT_ATMPOS_RESP of the customers card.

AUTH_MODE is always '08' (for offline Debit-POS)!

ISO_504 and ISO_505 are the tx date and time.

ISO_511 is the transaction amount entered before.

ISO_512 is read from the terminal card during initialisation (DF_POS.EF_ATMPOS.ISO_512).

AI is '00'

With ATMPOS_TRX_REQ the transaction is executed on the customers card.

ISO_317_316 comes from INIT_ATMPOS_RES, AUTH_MODE is '04' (for online Debit-POS), ISO_512 is retrieved from the initialisation routine, ISO_510 and ISO_511 contain the tx amount, AI is contained in DEBIT_POS_RES and AVAIL_AMOUNT and S2 can be read from TK_INIT_POS_RES. Please note, that AVAIL_AMOUNT, ISO_510 and ISO_511 must be identical!

Please note:

- If ATMPOS_TRX_RES has been correctly received from the customers card, the transaction is valid (!!!) and shall be finalised by the terminal, even if the customers card is removed at that very moment.
- If an error occurs up to this moment, the transaction is aborted with the respective error code and the last executed command is stored in 'Error in step'.

For detailed information, please refer to chapter "Faults during online Debit-POS transaction".

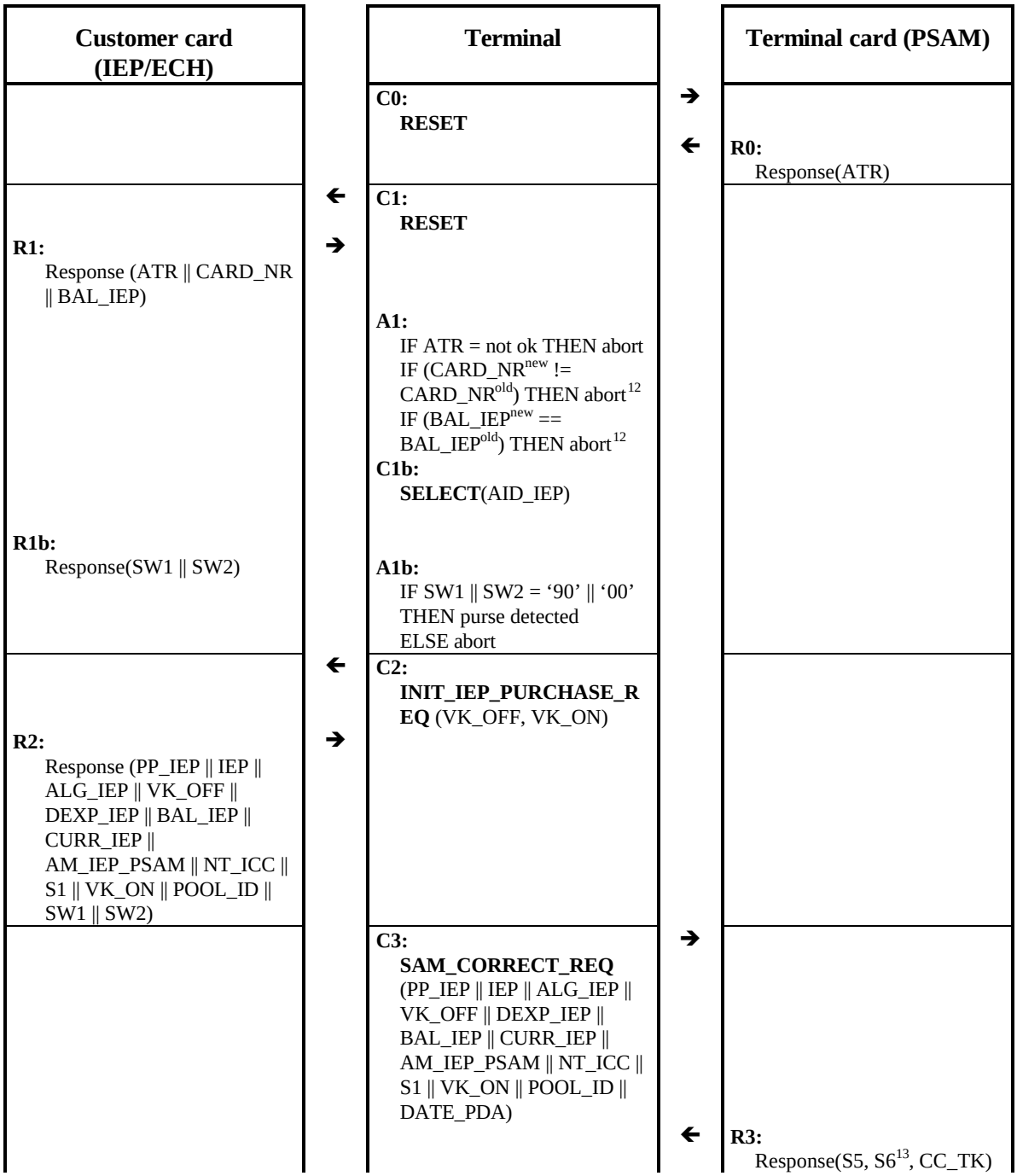
With SAM_POS_REQ (**C14**) S3 is validated.

Finally all relevant transaction data need to be written into the terminal memory.

4.4 IEP/ECH correction

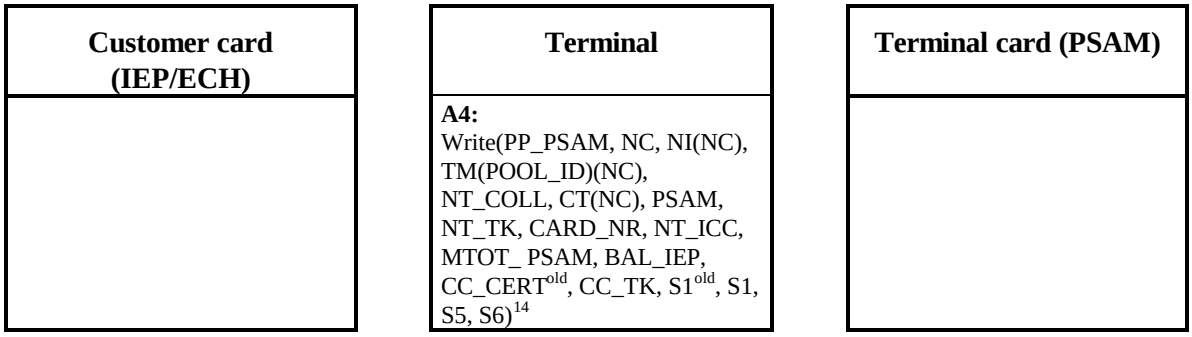
The correction transaction is necessary in case of card withdrawal or power loss during the execution of an IEP or ECH transaction.

Parameters of incomplete transactions are shown as xxx^{old}, xxx^{new} indicate the parameters of the correction transaction.



[12] Error recovery not possible and not necessary in this case!

[13] S6 is always calculated in this case!



- Figure 4: IEP/ECH correction sequence

[14] The terminal must read in all data required for logging which it has not yet received, using READ_BINARY.

5 Data transfer

This chapter is yet to be provided.

6 Card commands

This chapter is yet to be provided.

7 Transfer Card

The transfer card is used to transfer data when communication by telephone or via a serial interface is not possible.

The transfer card is recognised by its historical bytes in the ATR ("SCN_T").

7.1 Status file

The transfer card holds a status file, which is selected as an elementary file from the master file by the file identifier ’00 01’. The status file has a length of 12 bytes and can be read without authentication (READ always).

For writing the status file the same access conditions have to be met as for writing the communication file. That means writing is permitted only after mutual authentication.

The file contains the card status, access conditions to the communication file and the maximum length permitted for the communication file.

Content of status file:

Designation	Length (in bytes)	Type	Comment/feature
Card status	1	ASCII	„S“ Standard (for data transfer in both directions) "U" Update card (only for communication to the terminal, e.g. for printer texts update,...). "L", 'FF' Empty (new) card
Flag line	1	binary	Bit line: Bit 7: (= MSB) Authentication flag 1 = authentication required to read and write the communication file 0 = not required Bits 6-0: RFU, partly used by bank application
Length of communication file	2	binary	Length of communication file in bytes

Designation	Length (in bytes)	Type	Comment/feature
Terminal-Id	8	binary/BCD/ binary	Format: 'BB BB BB BB CC CC SS SS' Depending on the data to be transferred, the terminal id, the cluster id and the terminal sub-number are used by the bank terminal. The vendor terminal may ignore this data.

? Table 5: STATUS FILE OF TRANSFER CARD

7.2 Communication file

The communication file is an elementary file selected from the master file by the file identifier '00 02' and consisting of several sub-files.

Reading and Writing of the communication file is possible only if the access conditions defined in the status file are met.

The communication file has the following structure:

Designation	Length (in bytes)	Type	Comment/feature
Subfile 1	5-n	binary	The length of the sub-file is defined in its header (cf. section on 7.3 Header of the transfer sub-file and 7.4 Header of the other sub-files).
Subfile 2	5-n	binary	
...			One transfer card may have a discretionary number of sub-files (0-n), limited only by the size of the communication file.
Subfile n	5-n	binary	last sub-file
File end marking	1	binary	'FF'

? Table 6: SUBFILES IN THE COMMUNICATION FILE

File end marking is not necessary when the end-of file is identical with the physical end as shown in the status file.

The following rules apply for creating a sub-file:

- A search must be made for the end-of-file, which is shown by a byte of 'FF' at the place of the first byte of a new sub-file.
- All data including the remaining part of the header must be correctly written before the file flag is set.

- XOR is found by an XOR operation of all bytes, allowing for the file flag still to be written.
- The file end mark ‘FF’ must be entered after the end of the sub-file, i.e. at the beginning of the new sub-file, unless it is the physical end of the communication file.
- The last character to be set is the file flag of ‘FF’. An XOR operation of all bytes of a sub-file will then always produce ‘00’ hex.

7.3 Header of the transfer sub-file

Designation	Length (in bytes)	Type	Comment/feature
File flag	1	ASCII	„A“ collection
Collection type	1	binary	‘01’ RFU ‘02’ Terminal with modem ‘03’ RFU ‘04’ RFU ‘05’ transfer card
Version number	1	binary	'02'
NC	2	binary	transfer number
Terminal-ID	8	binary /BCD/ binary	Format: ‘BB BB BB BB CC CC SS SS’
PSAM	4	binary	
PP_PSAM	3	BCD	Purse provider identifier for a PSAM
Flag line	1	binary	Bit 7: Copy flag 1 = copy of transfer file 0 = original Bit 6: Flag for defective terminal card 1 = collection because of defective terminal card 0 = collection with terminal card Bit 5: used by the banks Bit 4-0: RFU, currently always 0
Date and time	5	BCD	YYMMTTHHMM if existing, otherwise 0

Designation	Length (in bytes)	Type	Comment/feature
CAD_CODE	3	binary	Current terminal hardware and software release 1. byte vendor-ID (assigned by system provider) 2. byte 1. Nibble: hardware version 2. byte 2. nibble and 3. Byte: software version
Last parameter update	2	binary	UPDATE_TK_NO of the last successful parameter update
File length	2	binary	in bytes incl. Header
XOR	1	binary	control byte on all data incl. Header
Subsequent file number	1	binary	starting with 1. A sub-file may be devided onto many transfer cards.
Finished flag	1	binary	‘00’ = subsequent file has to be processed ‘01’ = finished

? Tabelle 7: HEADER OF THE TRANSFER SUBFILE

Please note:

- An XOR operation of all bytes of a sub-file - including the XOR byte - will then always produce ‘00’.
- The "binary" field type generally means **"high byte first - low byte last"**!

7.4 Header of the other sub-files

The header of the sub-files of the transfer card are similar to the header (structure) of the corresponding files for collection via remote file transfer. The fields *file length, XOR-check, subsequent file number* and *finished flag* are added after the release number (position 3).

Designation	Length (in Bytes)	Type	Remark
File flag	1	ASCII	„R“ Redlist „P“ Parameter update for terminal card „Q“ or „q“ Receipt „B“ Resend request „S“ Software- and parameter update

Designation	Length (in Bytes)	Type	Remark
			for terminal use
release number	1	binary	'01'
File length	2	binary	in bytes incl. Header
XOR-check	1	binary	Checksum over all data incl. Header
Subsequent file number	1	binary	Starting with 1. A sub-file may be divided onto many transfer cards.
Finished flag	1	binary	'00' = subsequent file has to be processed '01' = finished
...			see corresponding file structure for remote file transfer

? Tabelle 8: HEADER OF OTHER SUBFILES

7.5 Authentication of the transfer card

7.5.1 Process flow overview

Transfer Card		Terminal		Terminal card
	←	**Get_Card_Data_Req** ()		
Response (CardData)	→			
	←	**Get_Challenge_Req** ()		
Response (R_ICC)	→			
		Generate random number R_Term		
		Select_MF ()	→	
		Crypt_Data_1 (R_Term || R_ICC || CardData)	→	
			←	Response (Crypt_Data_TK)
	←	**Mutual_Authenticate_Req** (P2='0C'; Crypt_ Data_TK)		
Response (Crypt_ Data_KK)	→			
		Select_MF ()	→	
		Crypt_Data_2 (R_ICC || R_Term)	→	
			←	Response (Crypt_Data_TK')

	Compare Crypt_ Data_KK to Crypt_Data_TK' not equal: transfer card not authenticated equal: transfer card authenticated	

? table 9: AUTHENTICATION OF TRANSFER CARDS

7.5.2 Operating system commands

GET_CARD_DATA, GET_CHALLENGE, SELECT and MUTUAL_AUTHENTICATE are STARCOS operating system commands. Please refer to the STARCOS S 1.2 Manual for reference.

7.5.3 CRYPT_DATA command

This command is used to encrypt and decrypt data in the terminal card

7.5.3.1 Request

Pos	Id	Name	Inhalt	Format	Länge
1	CLA	Class of Instruction	'B0'	hex	1
2	INS	Instruction Byte	'F8'	hex	1
3	DI	Direction	'00'	hex	1
4	KID	Key Identifier	'5C'	hex	1
5	Lc	Length of Command Data		hex	1
6	CRYPT_DATA	Data		hex	n
7	Le	Length of expected Response Data	'00'	hex	1

? table 10: CRYPT_REQEST

CRYPT_DATA is the data to be encrypted in the terminal card. In the table in chapter 7.5.1 Process flow overview CRYPT_DATA is used twice:

CRYPT_DATA_1

Pos	Id	Name	Inhalt	Format	Länge
1	R_TERM	random number generated by the terminal		hex	8
2	R_ICC	random number generated by the ICC		hex	8
3	CARD_DATA	card data		hex	8

? table 11: CRYPT_DATA in step C5

CRYPT_DATA_2

Pos	Id	Name	Inhalt	Format	Länge
1	R_ICC	random number generated by the ICC		hex	8
2	R_TERM	random number generated by the terminal		hex	8

? table 12: CRYPT_DATA in step C7

7.5.3.2 Response

Pos	Id	Name	Inhalt	Format	Länge
1	Data	Data	en-/decrypted data	0-140h	1
2	CC_ICC	Completion Code from ICC		4h	1

? table 13: CRYPT_RESPONSE

7.5.3.3 Completion Codes

6700	WRONG_LENGTH	Wrong length in Lc or Le
6900	WRONG_STATE	
6983	KEY_LOCKED	
6985	CONDITIONS_NOT_OK	
6A00	ITEM_NOT_FOUND	File or record not found, wrong file structure
6B00	WRONG_P1_P2	Wrong parameters P1-P2
9000	OK	Transaction terminated successfully