STARCOIN Specification Debit-POS On-line Authorisation

Edition 06.04.1999

Author O. Pannke - 3FE5

Status FINAL/CONFIDENTIAL

Version 1.1.1/Revision 20.11.98

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

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

Table of content

1 Introduction

1.1 Scope of this document

This document intends to describe the on-line interface of the STARCOIN C&A System to a card issuer to authorise Debit-POS transaction amount for either Debit-POS payments or funds raising for IEP/ECH load processes.

This specification is based on ISO 8583 standard.

1.2 Versions of this document

Version	Date	Changes	Author
0.0.1	30.09.98	First version of document	pan
0.0.2	08.10.98	Pipe Interface finalised	pan
1.0.0	04.11.98	Primary account number filled by ISO_305 Value representation detailed	pan
1.1.0	17.11.98	New definition of onl. authorisation fields (bitmap number given): 26: Cluster Id (Term_ClustId) 32: Operator Id (Term_OpId) 41: Terminal serial number (Term_TermId)	pan
1.1.1	20.11.98	"Bitmap" for each message included	pan
1.1.2	22.02.99	AUTH_POS_CONF: "23" DuplNum corrected to CustCard_ISO307	pan

• Tab. 1-1 / Document versions

1.3 Referenced documents

Version	Date	Title	Author
1993-12-15	1993	ISO 8583 Financial transaction card originated messages	ISO

2 Authorisation flow

2.1 Introduction

In an electronic payment system based on chipcards, the system provider must allow the card issuing banks to control the flow of money from the customers accounts for IEP/ECH (el. purse/el. cheque) load or Debit-POS purchase transactions in real-time. Otherwise it may is possible for the cardholder to overdraw his account by debiting it in a short period of time, where the account update is delayed.

The below described command flow defines an interface between the STARCOIN Clearing & Administration (C&A) system of the system provider and the card issuing bank, to update the customers account as soon as the funds raising transaction for loading an IEP/ECH at the Bank Service Terminal or a Debit-POS purchase at a merchant terminal takes place.

The card issuing bank receives a request for the authorisation of the amount, which shall be used to load a card or do a purchase. The bank can upon its own criteria (mostly the current balance of the customers account) authorise or deny the amount. After execution (or abortion) of the transaction at the terminal, the bank receives additionally a confirmation message.

2.1.1 Important note

This documents describes the data to be exchanged between the STARCOIN C&A system and the participating bank, authorising an IEP/ECH load as well as a debit-POS payment transaction. Due to the reason, that there are various bank systems with unnumbered interfaces and platforms, G&D provides a general pipe-based interface to allow communication between the bank and the C&A system.

The described messages are based on ISO8583. The C&A system will provide the request (AUTH_POS_REQ) and confirmation message (AUTH_POS_CONF) as described. As response only the defined message (AUTH_POS_RES) is accepted.

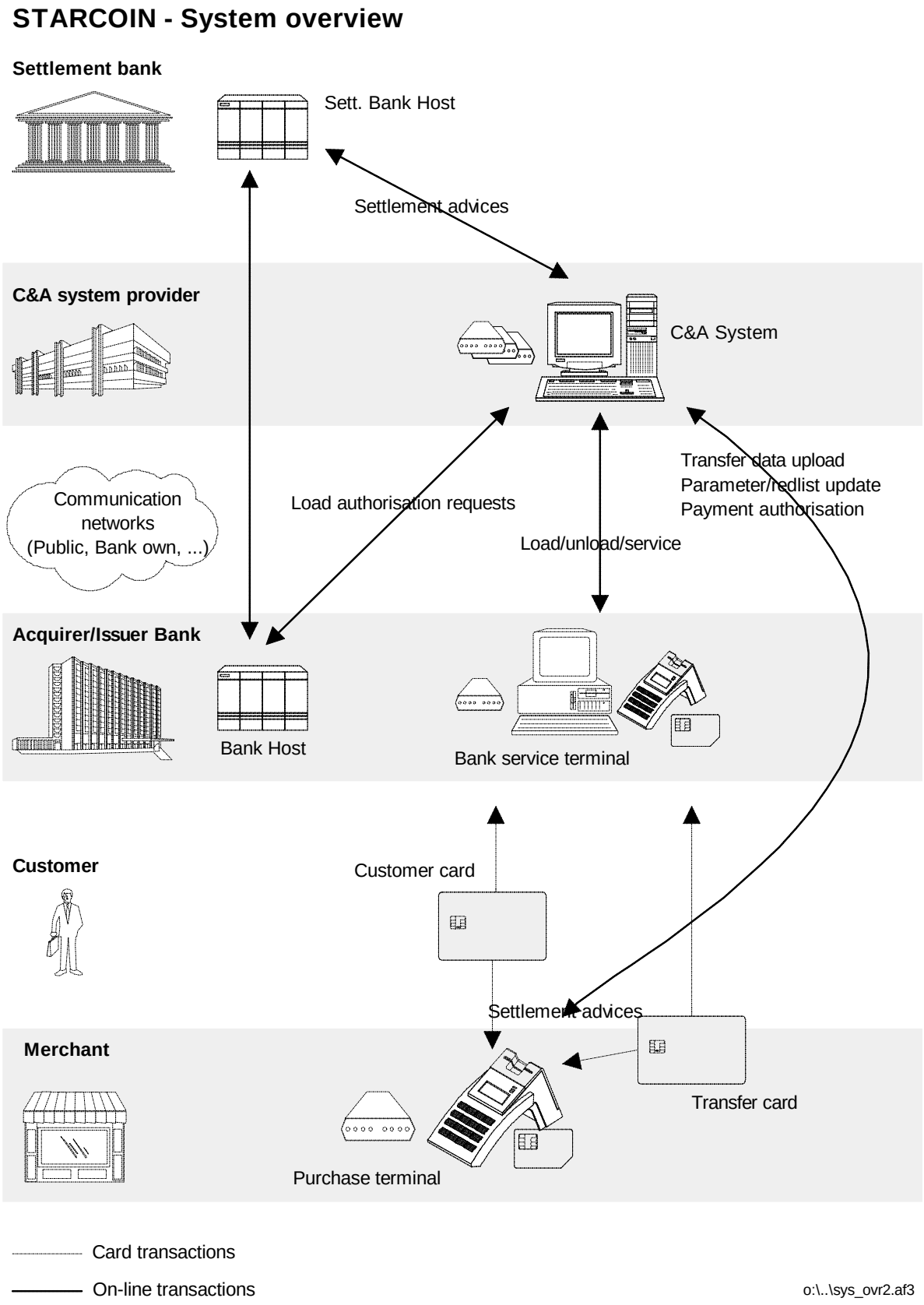
If further data elements are required to satisfy the respective bank data exchange scheme, all messages may be changed by the system provider and/or the participating banks. G&D can offer engineering support to adapt the messages to the specific needs if required.

Also the security scheme is at the discretion of the system provider and the participating banks. The STARCOIN C&A system only provides the interface. Any MACing and/or

encryption must be executed by external software. Also here G&D can offer engineering support to adapt the messages to the specific needs if required.

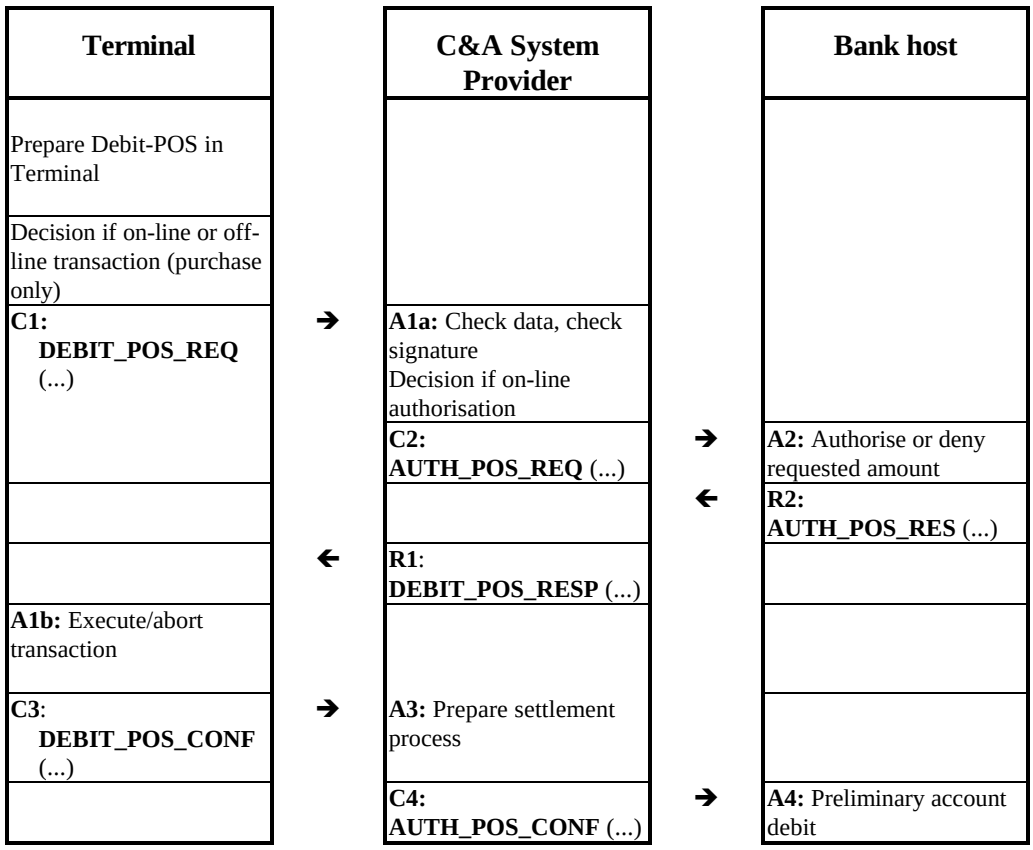
The implementation of reliable communication including the set up of the communication (modem, network,...) and the required security mechanisms is at the discretion of the system provider and the related banks. If required, G&D can offer engineering support for specification and implementation works.

2.1.2 System overview



2.1.3 Message flow

The following transaction flow gives an overview to the communication between the terminal, the C&A System and the Bank host:



- **C1**

  The bank or merchant terminal sends a request for an authorisation to the C&A system. This request is done for IEP/ECH load as well as for Debit-POS (on-line) payment.

- **A1a**

  The C&A system checks all relevant data elements and the signature.
  Upon the bank specific authorisation limit, the authorisation request for the card issuing bank is prepared.

- **C2**

  The authorisation request is provided in the interface.
  Additional data elements may be added, MACing and encryption done and the communication set up and the data sent to the bank host by the system provider.

- **A2**

  Upon bank own parameters the authorisation request is accepted or denied and the respective message prepared.

- **R2**
  The authorisation response is sent back to the C&A system.
- **R1**
  The C&A system prepares the response to the terminal upon the received authorisation or denial and sends it to the terminal.
  If the authorisation was denied, the C&A system confirms the denial to the bank host (steps C3 and A3 are not executed)
- **A1b**
  If authorised, the terminal executes the transaction (load or purchase) and prepares the confirmation.
  If the authorisation was denied, the transaction is aborted here.
- **C3**
  The bank or merchant terminal sends a request for load/payment confirmation to the C&A system.
- **A3**
  The transaction data are prepared for (later) settlement and the authorisation confirmation is provided in the interface. Additional data elements may be added, MACing and encryption done and the data sent to the bank host by the system provider.
- **A4**
  Upon valid transaction data the account of the cardholder can be preliminary debited. The final debit shall only be done, after the settlement advice from the settlement bank has been received.

2.1.4 Communication error handling

Please note, that an on-line authorisation system can only work on the basis of stable and reliable communication lines.

If communication problems occur, the transaction can be aborted without crediting/debiting of the card, until A1 has been sent successfully, because no value transfer has been taken place yet.

- **Terminal - C&A System**
  1. If the communication is corrupted by any means, before DEBIT_POS_RES has been received, the transaction is aborted and may be resumed upon the discretion of the bank, merchant and customer.

2. If the communication is corrupted after DEBIT_POS_RES has been received, but before DEBIT_POS_CONF could be sent, the transaction will be finalised and an off-line transaction record will be generated, which is transferred to the C&A system with the next data transfer.

- **C&A System - Bank Host**

3. After requesting for load/payment authorisation the terminal is setting a timer (1...999 seconds), which can be defined in the terminal configuration. If DEBIT_POS_RES (R1) can not be received before time-out or the communication is corrupted before, the transaction is aborted and may be resumed upon the discretion of the bank, merchant and customer.
4. As soon as AUTH_POS_REQ has been sent, the C&A system is setting a timer (1...999 seconds), which can be defined in the system configuration. If AUTH_POS_RES (R2) can not be received before time-out or the communication is corrupted before, the transaction is aborted and the C&A system sends an abort message to the terminal.

2.2 Exchanged Messages

2.2.1 Legend for abbreviations

a	alphabetical characters (A through Z and a through z, 1byte per character us
n	numeric digits 0 through 9 (2 digits per byte - BCD)
s	special characters (1 byte per character used - ASCII)
an	alphabetic and numeric characters (1byte per character used - ASCII)
as	alphabetic and special characters (1byte per character used - ASCII)
ns	numeric and special characters (1byte per character used - ASCII)
ans	alphabetic, numeric and special characters (1byte per character used - ASCI
MM	Month, 01 through 12 (2 digits per byte - BCD)
DD	Day, 01 through 31 (2 digits per byte - BCD)
YY	Year, 00 through 99. Please note: 95..99 = 1995..1999! 00..94 = 2000..2094
hh	Hour, 00 through 23 (2 digits per byte - BCD)
mm	Minute, 00 through 59 (2 digits per byte - BCD)
ss	Second, 00 through 59 (2 digits per byte - BCD)
VAR	variable length data element
3	Fixed to length of three characters, digits,...
..17	Variable length up to 17 characters, digits,... . The field is preceded by a 1 by

LenDefining the variable length of a ...x field (see above). Len is 01..99 (1 byte BCD).

Please note: All fixed length 'n' data elements are assumed to be right justified with leading zeroes. Al with trailing spaces ('20'). All data elements are counted from left to right, i.e. the leftmost position is

2.2.2 Authorisation request (AUTH_POS_REQ)

#	Bit-No	Name	Description	Format
1	-	Message Id	Identifier for 'Authorisation request'	n 4
2	-	Bitmap	Bitmap signifying the presence (1) or absence (0) of the data elements associated with that bit.	h 32
3	2	Primary account number	Identifier for the bank and the customers account	n..20 (+2)
4	3	Processing code	Affected account indicator	n 6
5	4	Amount	Tx Amount requested for authorisation (max. 4294967295)	n 12 '00 xx xx xx xx xx'
6	11	Systems trace audit number	Unique serial number of this authorisation sequence	n 6
7	12	Date and time (local tx)	Date/time of tx originator	n 12 'YYMMDDhhmm00'
8	13	Date effective	Customers card activation date	n 4 'YYMM'
9	14	Date expiration	Customers card expiration date	N 4 'YYMM'
10	22	Point of service data code	Identifier for card accepting terminal capabilities, environment and security	h 12
11	23	Card sequence number	Number distinguishing between separate cards with the same account number	n 3 '0xxx'

12	24	Function code	Indicating the specific purpose of the message	n 3 '0xxx'
13	26	Card acceptor business code	Classifying the card acceptor business type (cluster id)	n 4
14	32	Acquiring institution id code	Code identifying acquirer (id for the merchant)	n..15 (+2) 'yy xx..xx'
15	34	Primary account number, extended	Bank identification number.	n..18 (+2) 'yy xx..xx'
16	40	Service code	Id for service availability	n 3 (0xxx)
17	41	Card acceptor terminal id	Terminal serial number	n 10
18	49	Currency code	Used currency code	n 3 (0xxx)

2.2.3 Authorisation response (AUTH_POS_RES)

Please note: All fields are mandatory!

#	Bit-No	Name	Description	Format
1	-	Message Id	Identifier for 'Authorisation request'	n 4
2	-	Bitmap	Bitmap signifying the presence (1) or absence (0) of the data elements associated with that bit.	h 32
3	2	Primary account number	Echoed from '1104'.	n..20
4	3	Processing code	Echoed from '1104'.	n 6
5	4	Amount	Echoed from '1104'.	n 12 '00 00 xx xx xx xx'
6	11	Systems trace audit number	Echoed from '1104'.	n 6
7	12	Date and time (local tx)	Echoed from '1104'.	n 12 'YYMMDDhhmm00'
8	30	Original Amount	Requested amount (see Amount) || Authorised amount	n 24 '00 xx xx xx xx xx 00 xx xx xx xx xx'
9	32	Acquiring institution id code	Code identifying acquirer	n..15 (+2) 'yy xx..xx'
10	34	Primary account number, extended	Echoed from '1104'.	n..18 (+2) 'yy xx..xx'
11	39	Action code	Action to be taken (and reason)	n 3

				'0xxx'
12	41	Card acceptor terminal id	Echoed from '1104'.	n 8
13	49	Currency code	Echoed from '1104'.	n 3 '0xxx'

- **Action code - authorising value:**
  The C&A system will respond to the calling merchant/bank terminal with the author

Code	AI	Name	Description
000	00	Full Amount authorised	Card issuer authorises the requ amount. This amount is given i 'Original Amount - Authorised (Pos. #8, second half)

- **Action code - denial values:**
  Please note, that the C&A system will in any of these cases return an authorisation d terminal.

Code	AI	Name	Description
002	11	Partial amount authorised	Card issuer authorises a part of requested amount. This partial is given is 'Original Amount - Authorised Amount' (Pos. #8, s half). This for information of the carc only!!! The transaction is stopp the terminal and must be resum the beginning, if the card holde

			to use the new amount!
100	43	Authorisation denied	no specific reason given
102	03	Suspected fraud	Card is suspected to be frauded
104	07	Restricted card	Card is not allowed for this on-authorisation.
110	11	Invalid Amount	Amount exceeds max. limit, or corrupted.
115	43	Requested function not supported	The requested bank is (currentl able to authorise the transactio
116	11	Not sufficient funds	Balance on account to low for
121	11	Exceeds withdrawal amount limit	Balance on account to low for l
122	03	Security violation	Security (implemented by the s provider) is violated.
129	03	Suspected counterfeit card	Issuing bank assumes card to b counterfeited.

2.2.4 Authorisation confirmation (AUTH_POS_CONF)

#	Bit-No	Name	Description	Format
1	-	Message Id	Identifier for 'Authorisation request'	n 4
2	-	Bitmap	Bitmap signifying the presence (1) or absence (0) of the data elements associated with that bit.	h 32
3	2	Primary account number	Echoed from '1104'.	n..20 (+2)
4	3	Processing code	Echoed from '1104'.	n 6
5	4	Amount	Echoed from '1104'.	n 12 '00 00 xx xx xx xx'
6	11	Systems trace audit number	Echoed from '1104'.	n 6
7	12	Date and time (local tx)	Echoed from '1104'.	n 12 'YYMMDDhhmm00'
8	13	Date effective	Echoed from '1104'.	n 4 'YYMM'
9	14	Date expiration	Echoed from '1104'.	n 4 'YYMM'
10	22	Point of service data code	Echoed from '1104'.	h 12
11	23	Card sequence number	Echoed from '1104'.	n 3 '0xxx'
12	24	Function code	Echoed from '1104'.	n 3

				'0xxx'
13	26	Card acceptor business code	Echoed from '1104'.	n 4
14	32	Acquiring institution id code	Echoed from '1104'.	n..15 (+2) 'yy xx..xx'
15	39	Action code	Action to be taken (and reason)	n 3 '0xxx'
16	40	Service code	Echoed from '1104'.	n 3 '0xxx'
17	49	Currency code	Echoed from '1104'.	n 3 '0xxx'

- **Action code for confirmation of positive authorisation value:**
  The C&A system has received the confirmation of the terminal about successful tran

Code	Name	Description
000	Transaction successfully executed	The C&A system has sent the authorisation and received the confirmation of successful execution.
181	Terminal Confirmation indicates error	The authorisation response was sent, but the confirmation indicated, that the transaction was not executed. No preliminary account debit.
182	Terminal confirmation not received	The authorisation response was sent, but the confirmation could not be received.
183	C&A System error	The C&A system was not able to process the response due to internal

		errors

Very important note:
The card issuing bank can now debit the customers account by the authorised value
But the 'official' debit must only be done after the reception of the settlement advice
finally the valid execution of the transaction.

- **Action code - confirmation of denial values:**
  The C&A system has received the denial from the card issuing bank and confirms, tl
  been rejected.

Code	Name	Description
100	Authorisation denied	no specific reason given
191	Response could not be sent	The response to the denial could not be sent from the C&A system to the terminal and the transaction was aborted.

3 Interface

3.1 Introduction

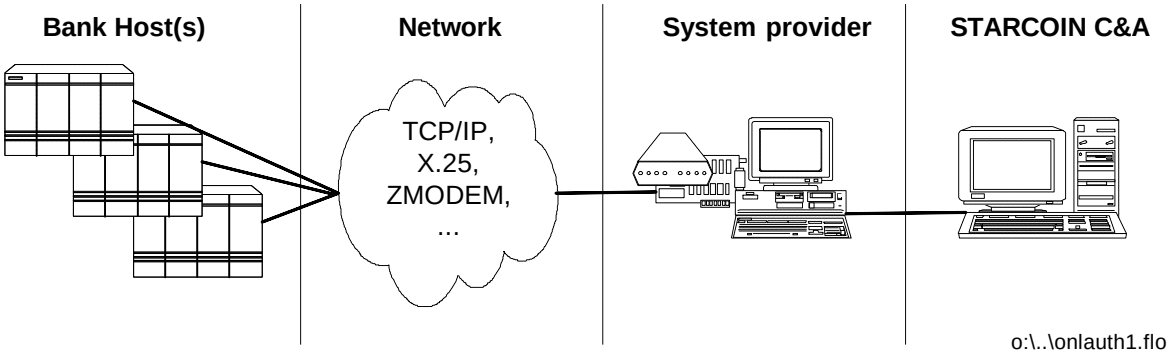
This section describes the proposed communication interface to the card issuing bank for on-line authorisation between the C&A System and the Bank Host. To keep the interface open and simple for communication it is foreseen to use the Windows NT Named Pipes.

Named pipes are used to transfer data between unrelated processes and across a network between computers. Typically, a server process creates a named pipe with a well-known name. Client processes that can get the name of the pipe can open the other end of the pipe, subject to access restrictions specified by the pipe's creator. After they are connected, the server and client can exchange data by performing read and write operations on the pipe.

Manipulation of named pipes is similar to reading and writing to file handles. Remote access to named pipes is provided through the network redirector. Processes on the local computer can use named pipes to communicate with each other without going through networking components.

3.2 Description of interface

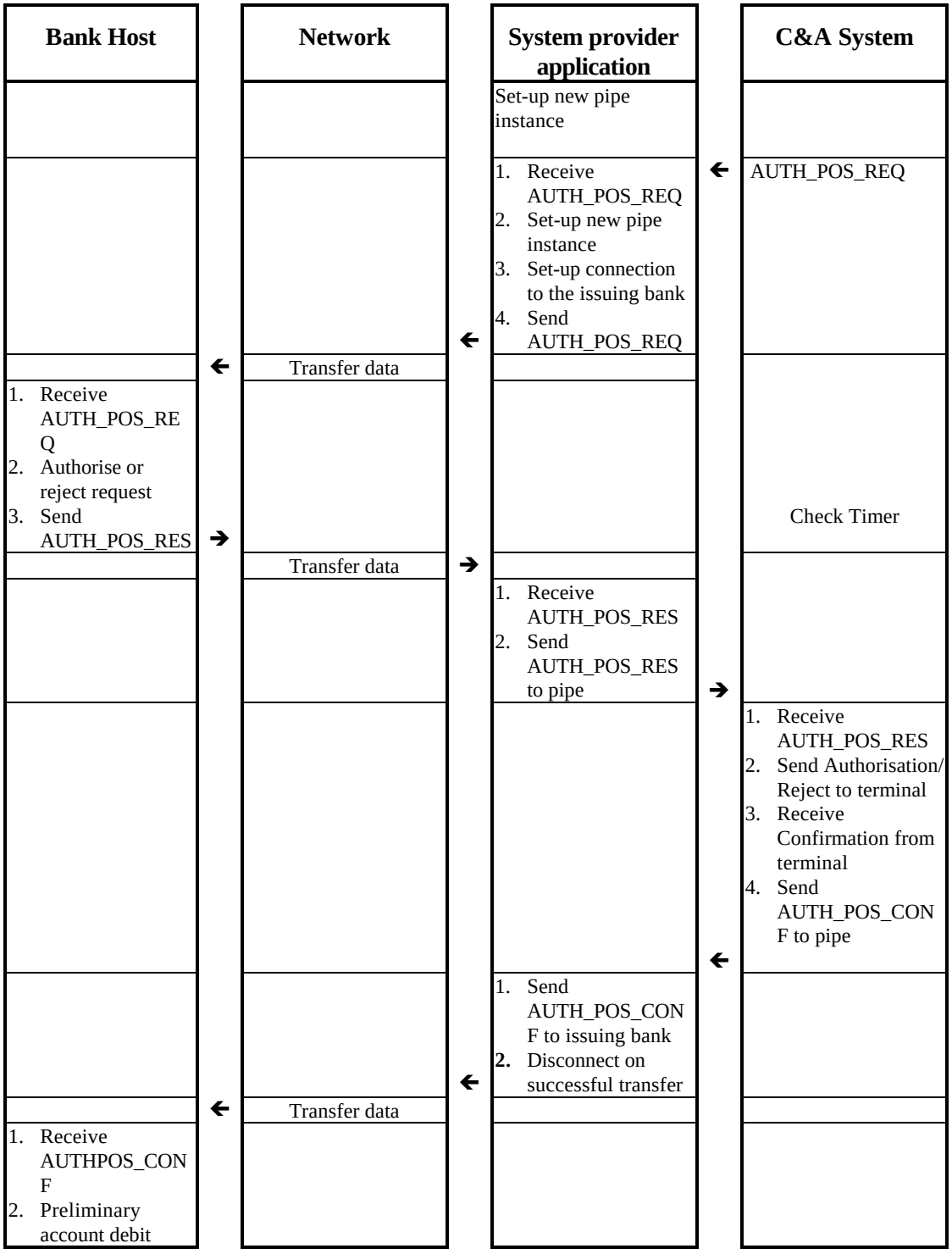
3.2.1 Connection overview



To set-up the Named Pipes interface between the C&A System and the System provider application, which establishes the connection to the card issuing bank, the Client-Server model will be used. Here the C&A System will act as the Client and the Bank Host will

act as the Server. As seen by the C&A System, there will be Input and Output activities to the Named Pipe created by the Bank Host.

3.2.2 Authorisation flow pipe management



The system provider application (not the STARCOIN application !) creates a pipe and after receiving message (AUTH_POS_REQ) on this pipe, it has to create a new instance of this pipe for future inputs by the C&A System. The instance of the pipe where the

message was received is the pipe where the response message (AUTH_POS_RES) has to be sent.

The name of the Named Pipe is usually**QAuthPos.** This name and location can be changed to the value defined in the INI file.

All pipes transfer a message. The mode PIPE_READMODE_MESSAGE has to be used.

The STARCOIN C&A System generates a message in the output pipe. The system provider application and the Bank Host Program processes the message and sends the response to the same instance of the pipe where the message was received. In case of an error either error response or no response is sent. If the C&A System doesn't receive the response within the time-out interval mentioned in the INI file parameter TIME_OUT, the pipe is closed.

3.2.3 INI File - AUTHPOS.INI

Bankhost.ini is an ASCII File located in the windows directory. This file consists of the chapter GENERAL.

Syntax:

[GENERAL]

[AUTHPOS_PIPE=pipe_name_and_location]

[TIME_OUT=pipe_timeout_in_seconds]

Chapter [GENERAL] is mandatory.

AUTHPOS_PIPE: Named pipe used to communicate between the C&A System and the system provider application . Default name is\\.**pipe\QAuthPos.**

TIME_OUT : 1 to 999 seconds. After sending the AUTH_POS_REQ message, the C&A System waits for TIME_OUT seconds for AUTH_POS_RES response message. After this time the pipe closes (and the C&A system rejects the authorisation request of the calling terminal).

3.2.4 Sample code for pipe connection done C&A System

```
HANDLE hConnectToPipe(unsigned char *szPname)
{
HANDLE hPipe;
BOOL bSuccess;
/* attempt to connect to pipe instance */
hPipe = CreateFile(szPname, GENERIC_READ | GENERIC_WRITE, 0, NULL,
```

```
OPEN_EXISTING, 0, NULL);
bSuccess = WaitNamedPipe(szPname, NMPWAIT_USE_DEFAULT_WAIT);
if(!bSuccess)
{
    iProcessError();
    hPipe=NULL;
}
return hPipe
}
```

3.2.5 Sample code for Pipe Write

```
DWORD dwWriter(WRITER_PARAMS *writer_params)
{
BOOL bSuccess;
//Write data to the pipe pointed to by the handle  writer_params->hPipe
bSuccess = WriteFile(writer_params->hPipe, writer_params->ucpData,
writer_params->iDataSize, &dwWritten, OVERLAPPED_IO ? &ol : NULL);
if (!bSuccess)
    iProcessError();
return dwWritten;
}
```

3.2.6 Sample code for Pipe Read

```
DWORD dwReader(READER_PARAMS *reader_params)
{
BOOL bSuccess = 0;
DWORD dwRead=0;
bSuccess = ReadFile(reader_params->hPipe, reader_params->ucpData, reader_params-
>iDataSize, &dwRead, NULL);
if (!bSuccess)
    iProcessError();
return dwRead;
}
```

--- end of document ---