# STARCOIN Specification
# Settlement data interface

Edition 03.05.1999



*Author* *O. Pannke - 3FE5*

*Status* *FINAL/CONFIDENTIAL*

*Version 1.5.1/Revision 03.05.99*

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 functional description of the STARCOIN C&A interface to the settlement bank.

## 1.2 Versions of this document

| Version | Date | Changes | Author |
|---|---|---|---|
| 1.0.0 | 16.05.97 | First version of document | pan |
| 1.1.0 | 30.10.97 | Updated Specification for implementation | pan |
| 1.1.1 | 11.11.97 | Editorial changes<br>Every record ends with CR+Lf (even if encrypted) | pan |
| 1.2.0 | 04.02.98 | Date format changed to DD.MM.YYYY to support localisation in different languages | pan |
| 1.3.0 | 28.04.98 | 2.2.2: BINDest and DestAccountNo must be of bank executing transaction | pan |
| 1.3.2 | 15.05.98 | Delimiter and padding bytes always appended to every settlement record<br>Cryptographic section detailed. | pan |
| 1.3.2 | 25.05.98 | Encrypted values and padding bytes are stored hexadecimal | pan |
| 1.4.0 | 12.10.98 | Debit-POS included | pan |
| 1.4.1 | 06.11.98 | ISO506 included to all export data<br>Format for ISO506 changed<br>NC included for IEP, ECH, POS<br>NI included for ECH | |
| 1.5.0 | 10.11.98 | ISO_506 is Char (16)<br>Release for C&A Version 2.0.0 | pan |
| 1.5.1 | 03.05.99 | Length fields of ECH and POS corrected | pan |

Tab. 1-1/ Document versions

## 1.3 Related documents

| Ref. | Name | Version | Author |
|---|---|---|---|
| [GD1] | STARCOIN - Payment scheme | 1.3.0 | pan |

Tab. 1-2 / Related documents

## 1.4 General description of settlement

### 1.4.1 Settlement process

When clearing the purse (IEP) and/or electronic cheque (ECH) load/unload/payment transactions, the STARCOIN Clearing and Administration system (C&A System) generates all necessary debit and credit advice data. These data are transferred once a day to a certain bank, called settlement bank, to manage the complete payment transactions between the banks and especially their customer-, merchant and own accounts participating to this system.

The settlement bank is authorised and trusted by all participating banks.

The settlement process is fully managed by the existing interbank payment schemes of the respective country/region and not at the discretion of STARCOIN.

### 1.4.2 Data transfer

The transport of the data from the C&A system to the settlement bank is at the discretion of the C&A system provider:

- Transport on disk:
  The settlement data files are written on a disk and transported 'manually' to the settlement bank
- On-line connection:
  The settlement data files are sent via modem e.g. to a settlement bank mailbox or by a direct connection via telephone line between two terminal programs. Due to security reasons it is not recommended to send the data via the Internet.

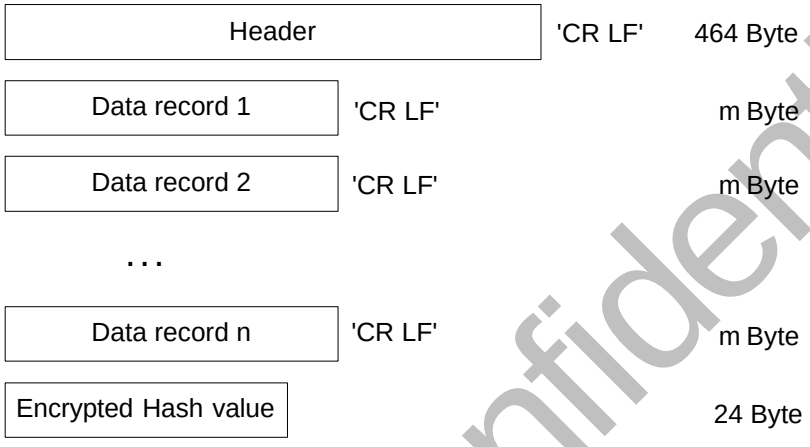
Please note, that the transfer of the data is not at the discretion of the STARCOIN C&A system. Only the settlement files are provided.

# 2 Settlement data file structure

## 2.1 General Notations

### 2.1.1 Settlement data file structure

All three types of settlement data files consist of a fixed length header (464 byte), a varying number of data records and an encrypted hash value of 24 byte length. Depending on the security level, the data records may be also encrypted.




o:\..\setfile1.flo

• Fig. 2-1 / Settlement data file structure

### 2.1.2 Settlement data record conventions

- Settlement advices are based on fixed length of their data and separate them additionally by '::'
- Due to the fixed length format numeric values are filled with '00..00' and character values with ' ' (Space = ASCII(20)).
- All data of one settlement advice record are concatenated to a single line ended with 'CR' + 'LineFeed' (no matter if the record is encrypted or not).
- *Cursive* printed data elements may be abundant, due to anonymisation of a bank's customer towards the C&A system provider.
- Date format: DD.MM.YYYY e.g. 2. February 1998 becomes 02.02.1998
- Time format: HH:MM:SS e.g. 12:35:56. Please note, that a time contained within a settlement data record is coded as HHMMSS.

- The encrypted data are stored as hex values. Also the encrypted hash value and the padding bytes are hexadecimal values (Format: 'h').
  All other values are stored in their ASCII representation.

### 2.1.3 Settlement file Header

- For easier hashing, all header sections have a fixed length of 464 byte.

  The header of the settlement data contains identifier for the used key version:
  Version: 001/'Key version Hash enc.'/'Key version data enc.'/'Security identifier'
- 002 is now the topical version of these settlement protocol
- Key version is the version of the hash value encryption key - format N(3)
  For the settlement bank: This key version must be found in the Plug-in key card of the KCT 800 to allow decryption of the hash value.
- Key version ENC is the version of the encryption key - format N(3)
  For the settlement bank: This key version must be found in the Plug-in key card of the KCT 800 to allow decryption of the settlement data records.
- The *Security identifier* indicates the type of certificate:

  'S' signed by a hash: Header + Data + encrypted hash value

  'C' Combined: Header + Data_enc + encrypted hash value

e.g. Version: `002/002/000/S`
Version: `002/002/003/C`

### 2.1.4 Settlement data export file

The files need to be hashed/encrypted after its generation. Used file names:

| | |
|---|---|
| DAVddmmy.dat | Settlement data for IEP/ECH load/unload transactions |
| ISLddmmy.dat | Settlement data for Pool payment (IEP purchase transactions) |
| ESLddmmy.dat | Settlement data for ECH individual payment transactions |
| POS ddmmy.dat | Settlement data for Debit-POS individual payment transactions |

ddmmy is the date of the file generation.

## 2.2 Settlement data for IEP/ECH load/unload

DAVddmmy.dat

The settlement is done on individual advices for each load/unload transaction of an IEP or ECH. The provided data allow

- the transfer of the load amount from the customers account to the issuning bank pool account
- the transfer of the unload amount from the issuing bank pool account to the customers account
- transfer of the respective service charges from the concerned accounts to the system providers service charge account.

For detailed information to the flow of money, please refer to [GD1].

### 2.2.1 Header Text/Data:

| No. | Text | Size |
|---|---|---|
| 1 | *******.******* (60 *'s) + CR + Linefeed | 62 |
| 2 | *******.******* (60 *'s) + CR + Linefeed (RFU) | 62 |
| 3 | Electronic purse and electronic cheque settlement information + CR + Linefeed | 63 |
| 4 | Date: 'SystemDATE' Time: 'SystemTIME' + CR + Linefeed | 34 |
| 5 | Version: 001/'Key Version Hash'/'Key Version ENC'/'Security Identifier' + CR + Linefeed | 24 |
| 6 | Service provider: 'CAP_Name' + CR + Linefeed | 50 |
| 7 | Service charge destination BIN: 'Bank_BIN' (from CAP_BankId) + CR + Linefeed | 49 |
| 8 | Service charge destination account: 'CAP_SvcAccNo' + CR + Linefeed | 58 |
| 9 | *******.******* (60 *'s) + CR + Linefeed | 62 |
| | Full Length of header | 464 |

### 2.2.2 Exported Settlement data

There is one record generated for every load/unload transaction:

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | DbAdv_No | N(8) | Unique Number identifying for each Debit Advice |
| | Delimiter | (2) | '::' |
| 2 | DbAdv_Type | N(2) | Type to indicate whether it is for a LOADING (01) transaction or UNLOADING (02) transaction |
| | Delimiter | (2) | '::' |
| 3 | DbAdv_IEPType | N(2) | Type indicating whether the Debit Advice is for IEP(01) or ECH(02) |
| | Delimiter | (2) | '::' |
| 4 | DbAdv_CustTransDateTime | Date(18) | Date and Time on which the load/unload transaction took place<br>(Format: DD-MM-YYYY HHMMSS)<br>Date and Time are separated by 2(!) Spaces (ASCII Hex '20') |
| | Delimiter | (2) | '::' |
| 5 | DBAdv_IEPECH | N(14) | Customer card IEPECH No |
| | Delimiter | (2) | '::' |
| 6 | DbAdv_CustCardNr | N(20) | Customer card number |
| | Delimiter | (2) | '::' |
| 7 | *DbAdv_BankCustId* | Char(20) | Bank specific customer Id. If the customer account number is absent, this is the only relation to the customers account. |
| | Delimiter | (2) | '::' |
| 8 | DbAdv_TermId | N(5) | Unique identifier for the terminal executing the load/unload transaction. |
| | Delimiter | (2) | '::' |
| 9 | Term_ISO506 | N(10) + Char(8Char(16) | Bank specific identifier for a terminal |
| | Delimiter | (2) | '::' |
| 10 | DbAdv_BINSrc | N(15) | BIN of source account (debited account, see 11.) |
| | Delimiter | (2) | '::' |

| | | | |
|---|---|---|---|
| 11 | *DbAdv_SourceAcctNo* | N(20) | The Account from which money is to be debited.<br>UNLOAD (cash or account):<br>• Bank pool Account No. (IEP)<br>• ECH Account Number (ECH)<br>LOAD:<br>• Customer account No (from account)<br>• Bank Cash Account No (by cash) |
| | Delimiter | (2) | '::' |
| 12 | DbAdv_BINDest | N(15) | BIN of destination account (credited account, see 13.) |
| | Delimiter | (2) | '::' |
| 13 | *DbAdv_DestAccountNo* | N(20) | The Account where money is to be credited.<br>UNLOAD:<br>• The Customer Account No. at issuing bank (to account)<br>• Executing bank cash account (to cash)<br>LOAD:<br>• Bank Pool Account No. (IEP)<br>• ECH account number (ECH) |
| | Delimiter | (2) | '::' |
| 14 | DbAdv_Amt | N(10) | Amount that has been transacted with the customer card for this advice |
| | Delimiter | (2) | '::' |
| 15 | DbAdv_BINSvcSrc | N(15) | BIN of service charge account (debited account) |
| | Delimiter | (2) | '::' |
| 16 | DbAdv_SvcAccountNo | N(20) | Service Charge Account No from which the amount is to be debited. If bank is paying the charges, this will be the bank service charge account no. else this will be the customer Account number or the bank cash acc. no. |
| | Delimiter | (2) | '::' |
| 17 | DbAdv_SvcCharge | N(10) | Amount that has been calculated as the service charge (If any) for this customer card and for this advice |
| | Delimiter | (2) | '::' |
| 18 | Padding | h (8) | '00 00 00 00 00 00 00 00' |
| | Full length: | 272 | |

A 'CR LF' is appended to every record if it is stored in the settlement file.

### 2.2.3 Settlement data encrypted hash value for IEP/ECH load/unload

The encrypted hash value is appended at the end of the settlement file.

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | UnLoadSettHash | h (24) | Encrypted Hash securing all transferred IEP/ECH load/unload settlement data (including header and 'CR LF' at the end of every record) |

## 2.3 Settlement data for Pool clearing (IEP purchase)

ISLddmmy.dat

The settlement is done on every cumulated pool for each merchant account. The provided data allow

- the transfer of the differential cumulated pool amout from issuning bank pool account to the merchant terminal account.
- transfer of the respective service charges from the concerned accounts to the system providers service charge account.

For detailed information to the flow of money, please refer to [GD1].

### 2.3.1 Header

| No. | Text | Size |
|---|---|---|
| 1 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| 2 | *******.....******* (60 *'s) + CR + Linefeed (RFU) | 62 |
| 3 | Pool settlement information for el. purse purchases (61) + CR + Linefeed | 63 |
| 4 | Date: 'SystemDATE' Time: 'SystemTIME' + CR + Linefeed | 34 |
| 5 | Version: 001/'Key Version Hash'/'Key Version ENC'/'Security Identifier' + CR + Linefeed | 24 |
| 6 | Service provider: 'CAP_Name' + CR + Linefeed | 50 |
| 7 | Service charge destination BIN: 'Bank_BIN' (from CAP_BankId) + CR + Linefeed | 49 |
| 8 | Service charge destination account: 'CAP_SvcAccNo' + CR + Linefeed | 58 |
| 9 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| | Full Length of header | 464 |

### 2.3.2 Exported settlement data

This data record is sent once for every merchant account.

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | IEPStl_No | N(8) | Unique Number identifying for each Credit settlement Advice |
| | Delimiter | (2) | '::' |
| 2 | IEPStl_SrcPoolBIN | N(15) | Bank Id number from where the money is to be Debited (BIN of Bank Pool of the customer bank) |
| | Delimiter | (2) | '::' |
| 3 | IEPStl_SrcPoolAccNo | N(20) | Source account from where the money is to be Debited (Bank Pool Account number of the customer Bank) |
| | Delimiter | (2) | '::' |
| 4 | IEPStl_MrcBIN | N(15) | Merchant Bank Id for IEP settlement |
| | Delimiter | (2) | '::' |
| 5 | IEPStl_MrcAccountNo | N(20) | Destination account where the money is to be credited (Bank Account number of the Merchant) |
| | Delimiter | (2) | '::' |
| 6 | IEPStl_Amt | N(10) | Amount that has been transacted with the Merchant for this advice |
| | Delimiter | (2) | '::' |
| 7 | IEPStl_SvcBIN | N(15) | Identification number of the bank holding the service account which is debited. |
| | Delimiter | (2) | '::' |
| 8 | IEPStl_SvcAccNo | N(20) | Number of the account which is debited with the service charge |
| | Delimiter | (2) | '::' |
| 9 | IEPStl_SvcCharge | N(10) | Amount that has beencalculated as the service charge for this Merchant and for this advice |
| | Delimiter | (2) | '::' |
| 10 | IEPStl_ISO506 | Char (16) | PSAM number and merchant terminal id as unique terminal idenifiers |
| | Delimiter | (2) | '::' |
| 11 | IEPStl_NC | N(5) | Transfer counter of terminal card (as reference) |
| | Delimiter | (2) | '::' |
| 12 | Padding | h(8) | '00 00 00 00 00 00 00 00' |
| | Full length | 184 | |

A 'CR LF' is appended to every record if it is stored in the settlement file.

### 2.3.3 Pool settlement data encrypted hash value

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | PoolSettHash | h (24) | Encrypted hash securing all transferred pool settlement data (including header and 'CR LF' at the end of every record) |

## 2.4 Settlement data for ECH individual transaction clearing

ESLddmmy.dat

The settlement is done on every single ECH purchase transaction. The provided data allow

- the transfer of the individual recorded ECH purchase amout from customers ECH account to the merchant terminal account.
- transfer of the respective service charges from the concerned accounts to the system providers service charge account.

For detailed information to the flow of money, please refer to [GD1].

### 2.4.1 Header

| No. | Text | Size |
|---|---|---|
| 1 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| 2 | *******.....******* (60 *'s) + CR + Linefeed (RFU) | 62 |
| 3 | Settlement information for el. cheque purchases (61) + CR + Linefeed | 63 |
| 4 | Date: 'SystemDATE' Time: 'SystemTIME' + CR + Linefeed | 34 |
| 5 | Version: 001/'Key Version Hash'/'Key Version ENC'/'Security Identifier' + CR + Linefeed | 24 |
| 6 | Service provider: 'CAP_Name' + CR + Linefeed | 50 |
| 7 | Service charge destination BIN: 'Bank_BIN' (from CAP_BankId) + CR + Linefeed | 49 |
| 8 | Service charge destination account: 'CAP_SvcAccNo' + CR + Linefeed | 58 |
| 9 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| | Full Length of header | 464 |

### 2.4.2 Exported Settlement data

There is one record generated for every ECH payment transaction.

| No | Table_DataElement | Format (Length) | Short descrption |
|---|---|---|---|
| 1 | ECHStl_No | N(8) | Unique Number identifying for each Credit Settlement Advice |
| | Delimiter | (2) | '::' |
| 2 | *ECHStl_BankCustId* | Char(20) | Bank specific customer Id (if not available, source account numbers ECHAcctNo and SvcAccNo must be available) |
| | Delimiter | (2) | '::' |
| 3 | ECHStl_TermId | N(5) | Unique identifier for a terminal |
| | Delimiter | (2) | '::' |
| 4 | ECHStl_ECHSrcBIN | N(15) | Bank Id number of the card holders bank |
| | Delimiter | (2) | '::' |
| 5 | ECHStl_ECHAcctNo | N(20) | Source account from where the money is to be Debited (Bank ECH Account number of the customer Bank) |
| | Delimiter | (2) | '::' |
| 6 | ECHStl_MrcBIN | N(15) | Merchant Bank Id for ECH settlement |
| | Delimiter | (2) | '::' |
| 7 | ECHStl_MrcAccountNo | N(20) | Destination account where the money is to be credited (Bank Account number of the Merchant) |
| | Delimiter | (2) | '::' |
| 8 | ECHStl_Amt | N(10) | Purchase amount that has been transacted at the merchant terminal for this advice |
| | Delimiter | (2) | '::' |
| 9 | ECHStl_SvcBIN | N(15) | Identification number of the bank which is debited with the service account |
| | Delimiter | (2) | '::' |
| 10 | *ECHStl_SvcAccNo* | N(20) | Number of the account which is debited with the service charge, if absent, relation to account must be done via BankCustId. |
| | Delimiter | (2) | '::' |
| 11 | ECHStl_SvcCharge | N(10) | Amount that has been calculated as the service charge for this advice |
| | Delimiter | (2) | '::' |
| 12 | ECHStl_ISO506 | Char(16) | PSAM number and merchant specific terminal id |

| | | | |
|---|---|---|---|
| | Delimiter | (2) | '::' |
| 13 | ECHStl_NC | N(5) | Transfer counter of terminal card (as reference) |
| | Delimiter | (2) | '::' |
| 14 | ECHStl_NI | N(5) | Transfer record counter of terminal card (related to NC; as reference) |
| | Delimiter | (2) | '::' |
| 15 | Padding | h (4) | '00 00 00 00' |
| | Full length | 216 | |

A 'CR LF' is appended to every record if it is stored in the settlement file.

### 2.4.3 ECH purchase settlement data encrypted hash value

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | ECHSettHash | h (24) | MAC securing all transferred ECH purchase settlement data (including header and 'CR LF' at the end of every record) |

## 2.5 Settlement data for Debit-POS clearing

POSddmmy.dat

The settlement is done on every single Debit-POS purchase transaction. The provided data allow

- the transfer of the individual recorded Debit-POS purchase amout from customers account to the merchant terminal account.
- transfer of the respective service charges from the concerned accounts to the system providers service charge account.

For detailed information to the flow of money, please refer to [GD1].

### 2.5.1 Header

| No. | Text | Size |
|---|---|---|
| 1 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| 2 | *******.....******* (60 *'s) + CR + Linefeed (RFU) | 62 |
| 3 | Settlement information for Debit-POS purchases (61) + CR + Linefeed | 63 |
| 4 | Date: 'SystemDATE' Time: 'SystemTIME' + CR + Linefeed | 34 |
| 5 | Version: 001/'Key Version Hash'/'Key Version ENC'/'Security Identifier' + CR + Linefeed | 24 |
| 6 | Service provider: 'CAP_Name' + CR + Linefeed | 50 |
| 7 | Service charge destination BIN: 'Bank_BIN' (from CAP_BankId) + CR + Linefeed | 49 |
| 8 | Service charge destination account: 'CAP_SvcAccNo' + CR + Linefeed | 58 |
| 9 | *******.....******* (60 *'s) + CR + Linefeed | 62 |
| | Full Length of header | 464 |

### 2.5.2 Exported Settlement data

There is one record generated for every Debit-POS payment transaction.

| No | Table_DataElement | Format (Length) | Short descrption |
|---|---|---|---|
| 1 | POSStl_StlNo | N(8) | Unique Number identifying for each Debit-POS Settlement Advice |
| | Delimiter | (2) | '::' |
| 2 | *POSStl_BankCustId* | Char(20) | Bank specific customer Id (if not available, source account numbers POSAcctNo and SvcAccNo must be available) |
| | Delimiter | (2) | '::' |
| 3 | POSStl_ISO506 | Char(16) | Unique identifier for a terminal (PSAM number and merchant terminal id) |
| | Delimiter | (2) | '::' |
| 4 | POSStl_NTTK | N (10) | Unique tx number (def. by terminal card) |
| | Delimiter | (2) | '::' |
| 5 | POSStl_DateTime | Date (18) | Purchase date and time<br>(Format: DD-MM-YYYY HHMMSS)<br>Date and Time are separated by 2 spaces (ASCII hexvalue: '20') |
| | Delimiter | (2) | '::' |
| 6 | POSStl_Amount | N(10) | Purchase amount that has been transacted at the merchant terminal for this advice |
| | Delimiter | (2) | '::' |
| 7 | POSStl_POSSrcBIN | N(15) | Bank Id number of the card holders bank |
| | Delimiter | (2) | '::' |
| 8 | POSStl_POSAcctNo | N(20) | Source account from where the money is to be Debited (customer bank account) |
| | Delimiter | (2) | '::' |
| 9 | POSStl_MrcBIN | N(15) | Merchant Bank Id for POS settlement |
| | Delimiter | (2) | '::' |
| 10 | POSStl_MrcAccountNo | N(20) | Destination account where the money is to be credited (Bank Account number of the Merchant) |
| | Delimiter | (2) | '::' |
| 11 | POSStl_SvcBIN | N(15) | Identification number of the bank which is debited with the service account |
| | Delimiter | (2) | '::' |
| 12 | *POSStl_SvcAccNo* | N(20) | Number of the account which is debited with the service charge, if absent, relation to account |

| | | | |
|---|---|---|---|
| | | | must be done via BankCustId. |
| | Delimiter | (2) | '::' |
| 13 | POSStl_SvcCharge | N(10) | Amount that has been calculated as the service charge for this advice |
| | Delimiter | (2) | '::' |
| 14 | Padding | h (3) | '00' |
| | Full length | 224 | |

A 'CR LF' is appended to every record if it is stored in the settlement file.

### 2.5.3 POS purchase settlement data encrypted hash value

| No | Table_DataElement | Format (Length) | Short description |
|---|---|---|---|
| 1 | POSSettHash | h (24) | MAC securing all transferred POS purchase settlement data (including header and 'CR LF' at the end of every record) |

3132333435

--- end of document ---