STARCOIN
Concept for off-line load process

Edition 22.01.1999

Author O. Pannke - 3FE5

Status PRELIMINARY/CONFIDENTIAL

Version 0.0.1/Revision 22.01.99

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 a concept for loading customers cards at a BST off-line to the C&A system (and the card issuing bank) .

1.2 Versions of this document

Version	Date	Changes	Author
0.0.1	22.01.99	First preliminary version of document	pan

• Tab. 1-1 / Document versions

1.3 Referenced documents

Ref	Version	Date	Title	Author
[GD1]	1.1.0	17.11.98	STARCOIN Specification - Debit-POS on-line authorisation	G&D

2 Off-line load concept

2.1 Introduction and current state

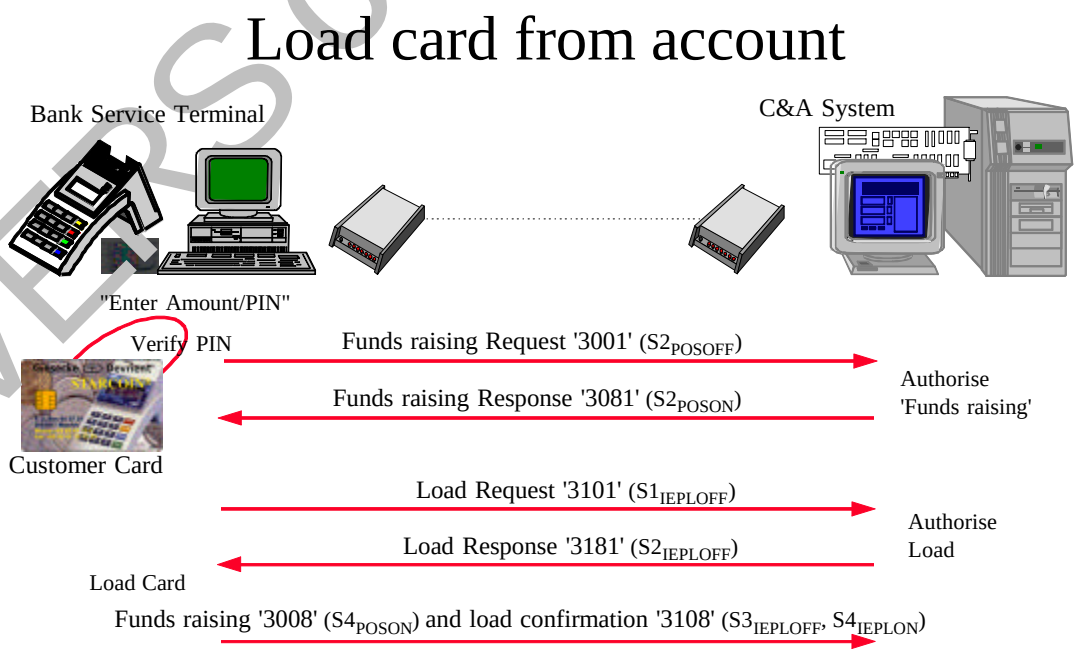
For security reasons all load processes within STARCOIN currently must be on-line to the C&A system. If required additionally a further on-line connection to the card issuing bank can be established and the authorisation of the card issuing bank and be obtained.

The process is separated into two independent units: The funds raising process and the card load process.

The funds raising allows to determine the source of the amount to be loaded. This can be the card holders account, another customers card or the bank cash account, if the card is loaded by cash. The C&A system checks several data elements including authentication signature $S2_{POSOFF}$ of the requesting card and authorises the funds raising by signature $S2_{POSON}$.

On successful funds raising the customers card can be loaded with a dedicated load operation. Also here, the C&A system validates several data elements and the request and authentication signature $S1_{IEPLOFF}$, before the load operation is authorised ($S2_{IEPLOFF}$).

For faster communication the confirmation of the funds raising and the load process are transferred together at the and of the load operation.



2.2 Remarks concerning off-line loading

2.2.1 Unlimited load by the bank

Load limits must be introduced, avoiding that one bank or a bank clerk can load unlimited amounts to customers cards:

Bank authorisation card load limits:

A parameter on the Bank Authorisation card holds an amount, which is decremented with every load done at the bank (terminal). If the amount is zero, no more off-line load operations (but still on-line load operations) can be executed. After a cycle time of one day (or one week) the amount is automatically reloaded to a certain limit and the loading can be continued.

Other limits control the maximum off-line authorised amount, the maximum cumulated off-line auth. amount (resetted at any on-line connection) and the maximum number of off-line authorisations.

Maximum load balance

The terminal card holds a load balance which is decremented by each load process. If the balance is zero (or mostly before) the bank can apply at the C&A provider to upload more value to that amount. If the bank can grand for the loaded money, the C&A provider will send a secured update command and reloads the balance.

2.2.2 Load restriction on own cards or all cards

Not all banks may be allowed to load cards of any other bank. The process must offer a restriction, which allows to restrict the load operation to cards, which have been issued by that bank only.

For the reason, that the number of participating bank may become very high, the management should not be complicated and the memory of the cards is restricted, this feature should either allow "own cards only" or "all cards" and not any possible combination.

2.2.3 Granting for the funds raising

Like for the on-line load process, the funds raising transaction can be executed:

- With the BAC: Load off-line by cash (from bank cash account)
- With the customer's card: Load off-line from cardholders account
- With another customer's card: Load off-line from another customer's account

2.2.4 Responsibilities

For the reason, that now the bank is the authorisation instance of the loaded amount, even more care must be taken by this instance to avoid misuse of the Bank Service terminal and bank authorisation card. For the reason, that an authorisation of the C&A system and the card issuer is not made, one can load a customers card without considering the real balance of money on the cardholders account.

The system provider must be aware, that allowing off-line load operations is a security risk, even that all processes are cryptographically well secured, because of the delay between the load operation and the reflection on the bank account. The risk can be well reduced by a funds raising authorisation of the card issuing bank. Due to missing on-line connection, this would restrict the loadable cards to bank own ones.

2.2.5 C&A system update

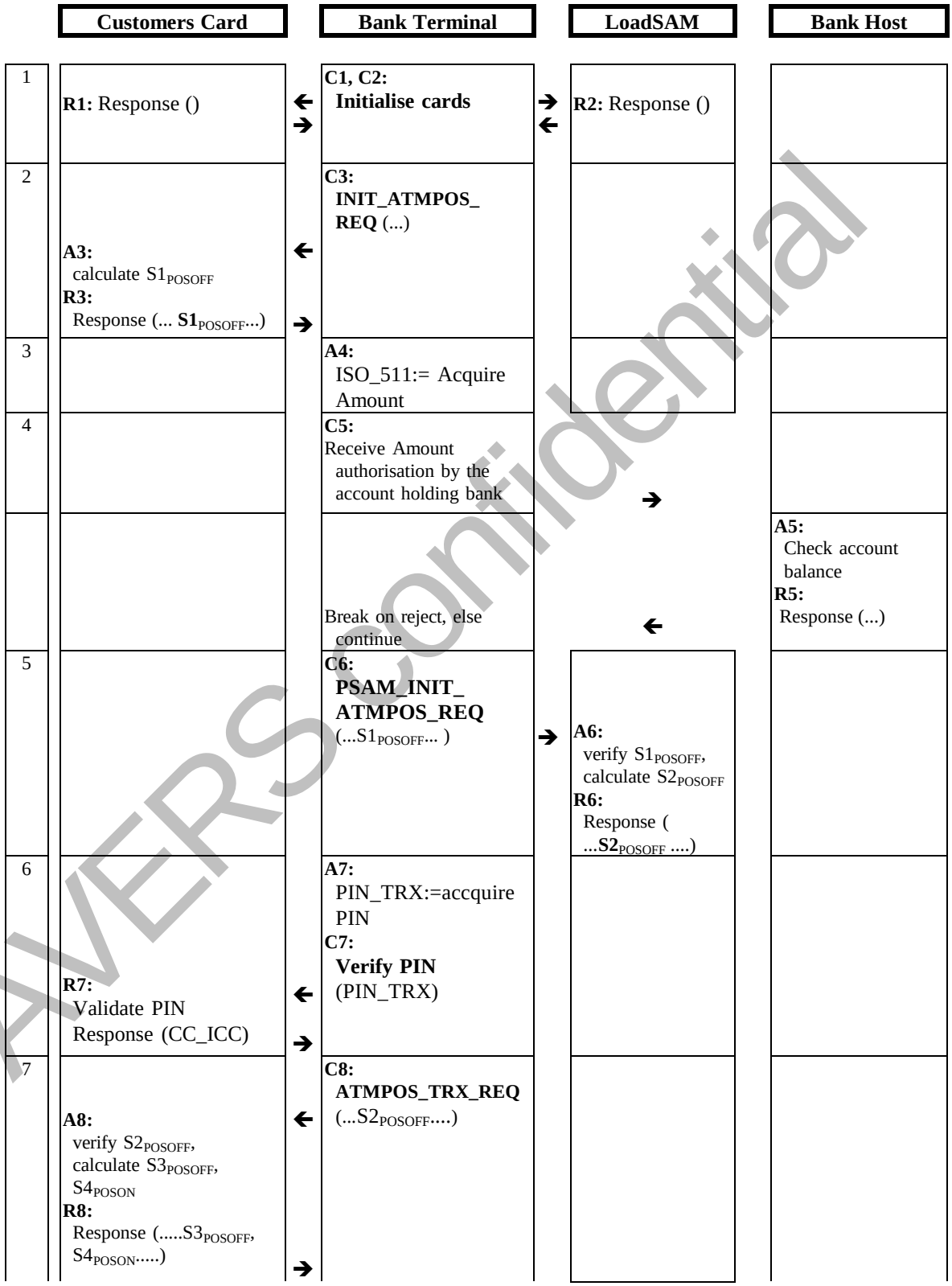
The C&A system runs its own accounting scheme, the clearing and settlement and plausibility checks. One some time, it must be informed by the executed load operations, to allow the clearing and generation of the settlement advices for the participating banks.

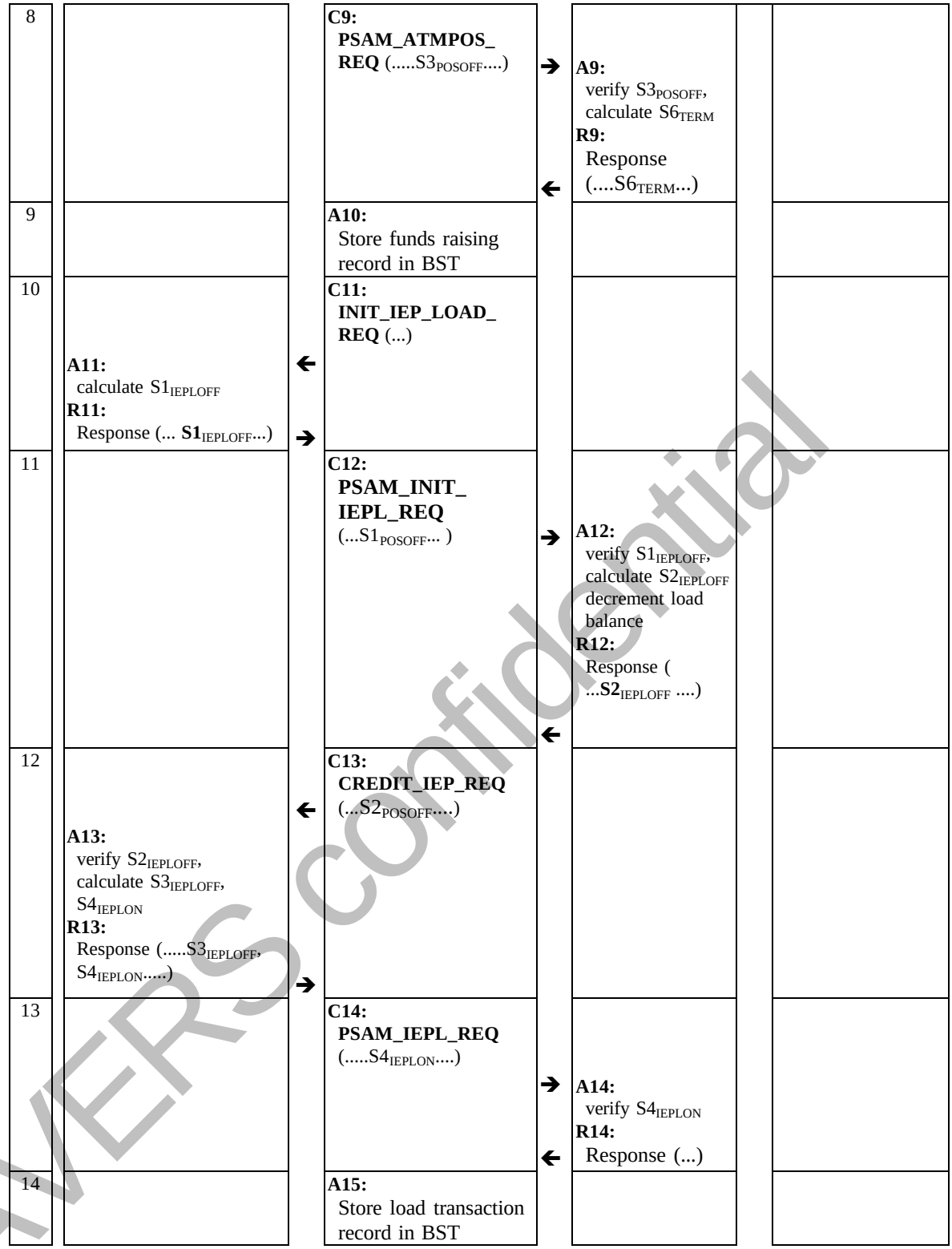
2.2.6 On-line capability of the BST

To provide the necessary transfers of off-line load transaction records to the C&A system and allow the C&A system to confirm received records and update the maximum load balance to the bank, it is assumed, that the BST can establish an on-line connection to the C&A system (e.g. via modem)! The off-line feature is only used to reduce to on-line connections to a minimum. A data transfer via transfer cards, is currently not foreseen.

2.3 Possible solution

2.3.1 Off-line load transaction flow





Remarks:

1. Reset sequence, read necessary data elements from both cards.
2. Initialise funds raising transaction at customers card, $S1_{POSOFF}$ is calculated and returned.
3. Amount is entered at the BST

4. If required/possible: The BST connects to the bank host and receives an authorisation for the requested amount. It is highly recommended to use format and structure of the funds raising request of the C&A system (ISO 8583 compatible) [GD1].
5. Initialise funds raising transaction at terminal card, $S1_{POSOFF}$ is validated and if successful, $S2_{POSOFF}$ is returned.
6. Enter and verify the customers card PIN.
7. Validate $S2_{POSOFF}$. Execute the funds raising transaction on the customers card (POS log record is stored on the card). Calculate $S3_{POSOFF}$ and $S4_{POSON}$. $S4_{POSON}$ is stored in the funds raising record for later validation in the C&A system.
8. Validate $S3_{POSOFF}$ and calculate $S6_{TERM}$ Finalise the funds raising transaction on the terminal card. $S6_{TERM}$ is stored in the funds raising record for later validation in the C&A system.
9. Store the relevant funds raising transaction data in the BST for later upload to the C&A system.
10. Initialise load operation on the customers card. $S1_{IEPLOFF}$ is calculated and returned.
11. Initialise load operation on terminal card: Validate $S1_{IEPLOFF}$ and calculate $S2_{IEPLOFF}$. The load balance, which controls the maximum cumulated load amount of a bank, which has been granted, is decremented by the load amount, which has been authorised during the funds raising transaction.
12. Load the electronic purse or the electronic cheque on the card after validation of $S2_{IEPLOFF}$. Calculate $S3_{IEPLOFF}$ and $S4_{IEPLON}$. Both are later validated in the C&A system clearing process.
13. The terminal card validates $S4_{IEPLON}$ for additional security of the loading bank.
14. Store the off-line load transaction record in the BST for later transfer to the C&A system.

2.3.2 Off-line load transaction records

The transaction record for the fundsraising transaction has the same format and structure than the Debit-POS off-line record used in such payments.

For the the load process, a new structure has to be defined, but the format is kept similar to the known ones.

2.3.3 Data transfer

The data transfer will be executed the same way it is currently done for the payment transaction records. A new subfile will be defined, identifying the off-line load data records.

2.4 Required Adaptations

2.4.1 Bank Terminal Card

The bank terminal card must support:

- Authorisation of the funds raising transaction
- Authorisation of the load transaction
- Load balance management
- Providing relevant data for off-line load records

2.4.2 C&A System

The C&A system must be able to

- receive the 'end of day' transfer
- clear and settle the off-line load transactions
- update the load balance

2.4.3 Bank Service Terminal

The BST must be improved for

- Managing the new type of load transaction
- Provide interface to bank's database to check cardholders account (optional)
- Managing the off-line load transaction records
- Off-line load tx record transfer to the C&A system

--- end of document ---