Common Electronic Purse Specifications

Technical Specification

Version 2.2

May 2000

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Revision Log

Version	Date	Brief Description of Change	Affects
1.0	12/98	Initial Publication.	All
2.0	3/99	First General Publication After Security Lab Review.	All
2.1	9/99	Editorial and consistency corrections.	All
		Additional security criteria for LSAMs.	2.4 13.1.4.1 13.1.4.4 13.2.2.2 13.2.2.7 13.2.2.9 13.2.7.11 13.3 Table 90
		Additional security criteria for PSAMs.	9.2.10 (new)
		RID_{PSAM} added to PSAM certificate.	Table 11
		Required data fields for a public key certificate request and response removed.	7.3.1.8 7.3.1.9 Table 12(old) Table 13(old)
		Country code and domain added to allow processing decisions based on the location of the POS or load device and the card issuer.	18.1.22 18.1.30 Table 16 Table 44 Table 46 Table 65 Table 83 Table 94
		Support added for CEPS migrations and specific implementations.	8.6.1 8.7.3 8.7.4 10.1.1.3 18.1.7 18.1.8 18.1.10 18.1.23 18.1.49

	18.1.70 Tables 21, 26, 29, 31, 33, 34, 46, 47, 49, 54, 55, 60, 61, 67, 68, 71, 79, 80, 85, 86, 91, 92, 96, 97
CC_{TRX} added to load and currency exchange logs.	Table 29 Table 31
S_6' MAC added to aggregation records.	10.1.4.11 10.1.5.6 10.1.6.3 10.1.7.10 16.4.1.6 18.1.35 18.1.106 Table 63 Table 109
Support added to allow intermediate incremental purchase steps to take place without PSAM validation. The last step must be validated by PSAM. Encryption of S_6 and S_6' added during transaction processing.	6.7, 10.1 10.1.4.4 - 6, 10.1.4.10 -15, 10.1.4.18, 10.1.5.8 - 9, 10.1.5.11-13, 10.1.6.3, 10.1.7.1, 10.1.7.3, 10.1.7.10-11, 10.1.7.15, 10.2.2.8, 18.1.7 18.1.9 18.1.34 18.1.35 18.1.50 18.1.51 18.1.102 Tables 52,53, 55, 57, 58
DD_{SCHEME} added to load and currency	Table 83

exchange transactions.	Table 94
Size of DD fields for load and currency exchange transactions increased.	Tables 83, 84, 92, 94, 95,96, 103, 105
Script message handling during exception processing clarified.	13.2 14.2.1
Maximum exchange amount added as an advisory field return from the card issuer on currency exchange transaction.	14.2.1.3 16.3.1.7 18.1.56 Table 95
Support for account selection added to application profile.	13.1.1.7 18.1.8
Errors that require specific cardholder notification explicitly stated.	13.1.5.2 14.1.4.2 Table 102 Table 104
Issuer options for CC_{TRX} modified.	18.1.20
Restriction that prevents a POS device from supporting both aggregation and cancel last purchase removed.	9.2.10 (old) 10.2
Additional POS exception processing specified.	10.1.8.2 10.1.8.3 10.2.3.3
Setting of NAD for T=1 protocol specified.	9.2.4.1 12.2.4.1
That a PSAM may process more than one transaction at the same time stated explicitly.	9.2.9.2
Additional requirements related to unattended devices included.	12.2.4.4 13.1.1.1
Security for unlinked load modified.	2.5.3, 6.5.1.5, 6.5.1.6, 6.6, 8.7.5.8, 13.1.1.12, 13.1.4, 13.1.4.1, 13.1.4.4,

			13.1.4.6 13.2.2 13.2.2.1 to 13.2.2.7, 13.2.2.9 13.2.2.11 13.3.1.1 13.3.1.2 13.3.1.4 16.2.1.6 to 16.2.1.8 16.2.1.13 16.2.2.4 18.1.20 18.1.90 to 18.1.92 18.1.99 to 18.1.100 18.1.102 Tables 79, 80, 82, 83, 84, 85, 86, 90, 91, 94, 103, 105
2.2	5/00	Editorial and consistency corrections.	6.5.1.7, 6.6.1.1, 6.6.1.8, 7.4.1.4, 8.2.1.4, 9.2.9.2, 10.1.4.6, 17.1.1.3, 18.1.51, 18.1.100, 18.1.102, Tables 52, 53, 65, 75, 76, 83, 84, 90, 94, 100, 103, 105, 118, 119
		Rename L_{MOTISS}, $MTOT_{ISS}$ and NT_{ISS} to L_{AGGTOT}, $MTOT_{AGG}$ and NT_{AGG}	All
		Remove $VKP_{REG,ACQ}$	6.2.1.1, 18.1.113 (old),

	Table 47
Add edit of $VKP_{CA,ISS,CEP}$ to merchant acquirer processing	Table 75
Clarify data for MAC in an issuer batch	11.1.2
Correct P1 values for Credit for Load command	Table 85
Add another requirement to definition of CSN	18.1.24
Clarify definition of ID_{ISS} and ID_{CEP} to allow the data elements to be used together as a single field	18.1.41, 18.1.42
Add another requirement to definition of $VKP_{CA,ISS}$	18.1.113
Modify required derivation data for $SESSKey_{PSAM}$	10.1.4.3
Allow $NT_{BATCH,SOURCE}$ and $MTOT_{BATCH,SOURCE}$ to be the sum of multiple fields	Table 77
Change format of ID_{LDA} to BCD	18.1.44
Change REFNO from variable to 3 bytes BCD to allow for easier use in ISO	18.1.96, Tables 83, 84, 90, 94, 95, 100
Add suspect transaction indicator as a CEPS field	18.1.110, Table 90
Simplify caching of merchant acquirer certificates	6.3.3.9, Table 53

2. Document Overview

2.1 Purpose

This document is a refinement of the CEP business requirements (see reference 1) and the CEP functional requirements (see reference 2). The purpose of the Technical Specifications is to provide the specifications necessary to achieve interoperability between the entities and components of a Common Electronic Purse (CEP) system. This document must be combined with proprietary specifications to create the final specifications for an implementation of the Common Electronic Purse (CEP).

This document provides the minimum specifications for interoperability for CEP components. It contains:

- All cryptographic operations required for interoperability
- All commands and responses that constitute the interface between the CEP card and the devices that support it.
- The required functionality for the PSAM.
- The required functionality for the LSAM.
- The minimum data that must be captured during transactions that take place at a POS device or a load device.
- The minimum requirements for the consumer interface.
- The minimum data that must be passed from one entity to another as a transaction is cleared and settled.
- A description of the procedures to be used for transfer of transactions between connecting processing nodes.
- A technical description of the merchant acquirer processing for POS transactions.
- A technical description of the load acquirer processing for load and currency exchange transactions.

- A technical description of the card issuer processing for all transactions.

- A description of the funds issuer processing required by CEPS for unlinked load transactions.

- The minimum responsibilities of the card issuer in detecting fraud and minimizing risk as part of a CEP system.

- A description of the functions necessary for a scheme provider to support a CEP system.

- The role of the Certification Authority (CA) and the minimum data elements recommended to request and generate a public key certificate.

- A data dictionary, a glossary of terms and a list of acronyms.

2.2 Intended Audience

This document has two different audiences:

1. If a CEP scheme provider has chosen to create specific technical specifications for its scheme, this document, along with the functional requirements specific to that scheme, will be used by the technical design staff of the CEP scheme provider to develop the scheme specific technical specifications.

   For this audience, the document provides the CEP interoperability functions that must not be compromised by any scheme specific functionality.

2. If a CEP scheme provider has chosen not to create specific technical specifications for its scheme, this document will be used by all technical staff involved in the development, testing, operation or maintenance of one or more components of a CEP system that supports that scheme.

   For this audience, the document provides an overview of the processing of a CEP system and the minimum required interfaces between components.

2.3 Included in this Document

Included in this document are:

- The message flows between entities.
- All required data elements and their usage.
- All interfaces where a specific set of data elements is required to be passed between entities.

2.4 Not Included in this Document

Not included in this document are:

- Information about CEPS processing that is not required to support interoperability.
- Record and message formats. These will be negotiated and defined between connecting entities when the business relationship is established.
- Connectivity for clearing and settling transactions for CEP schemes and the processing of fees and charges. These are scheme specific and will be included in the detailed specifications for a specific implementation.
- All scheme-specific requirements and specifications.
- Processing for unload transactions. This transaction is an on-us transaction for card issuers. Because the unload transaction is not required for interoperability, it is outside of the scope of this document.

2.5 Reference Information

2.5.1 Requirement Numbering

Requirements in this specification are uniquely numbered with the number appearing next to each requirement.

A requirement can have different numbers in different versions of the specifications. Hence, all references to a requirement must include the version of the document as well as the requirement's number.

2.5.2 *References*

The following documents are referenced in this specification:

1. Common Electronic Purse Specifications, Business Requirements, version 6.1, dated September 1999.

2. Common Electronic Purse Specifications, Functional Requirements, version 6.3, dated September 1999.

3. ISO/IEC 7816-3, 1997-12-15 “Identification cards - Integrated circuit(s) cards with contacts- Part 3: Electronic signals and transmission protocols".

4. ISO/IEC 7816-4, First Edition 1995-09-01
“Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange".

5. ISO/IEC 7816-5, 1994
“Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers”.

6. ISO 9797, 1993-11-22
“Information technology - Security techniques - Data integrity mechanism using a cryptographic check function employing a block cipher algorithm".

7. ANSI X3.92, 1981
“Data Encryption Standard"

8. EMV, version 3.1.1, 1998-05-31
"Integrated Circuit Card Specification for Payment Systems" Europay International S.A, MasterCard International Incorporated, Visa International Service Association.

CEPS is based on the standard created by the European Committee for Banking Standards (ECBS). The ECBS standard is based on prEN 1546, *Identification Card Systems - Inter-sector Electronic Purse, 1995-1996*.

2.5.3 Notational Conventions

Hexadecimal Notation

Values expressed in hexadecimal form are enclosed in single quotes (e.g., '_'). For example, 27509 decimal is expressed in hexadecimal as '6B75'.

Letters used to express constant hexadecimal values are always upper case ('A' - 'F'). Where lower case is used, the letters have a different meaning explained in the text.

Binary Notation

Values expressed in binary form are followed by a lower case "b". For example, '08' hexadecimal is expressed in binary as 00001000b.

Operators and Functions

$\wedge$ Logical AND.

$\vee$ Logical OR.

:= Assignment (of a value to a variable).

( ) or [ ] Ordered set (of data elements).

$B_1 || B_2$ Concatenation of bytes B_1 (the most significant byte) and B_2 (the least significant byte).

$[B_1 || B_2]$ Value of the concatenation of bytes B_1 and B_2.

encrypt( )[ ] The data in the square brackets is encrypted using the key in the normal brackets.

decrypt( )[ ] The data in the square brackets is decrypted using the key in the normal brackets.

DES( )[ ] The data in the square brackets is encrypted using DES encryption and the key in the normal brackets.

DES^{-1}( )[ ] The data in the square brackets is decrypted using DES decryption and the key in the normal brackets.

DES3( )[ ] The data in the square brackets is encrypted using triple DES encryption and the key in the normal brackets. Triple DES consists of encrypting an 8-byte plaintext block X to an 8 byte ciphertext block

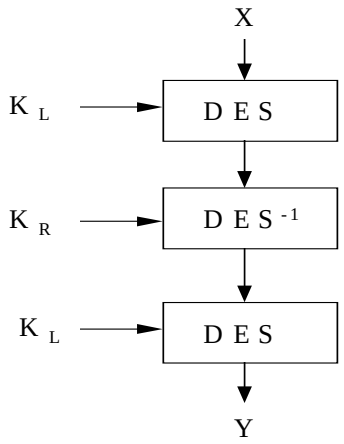
Y using a double length (16 byte) secret key K = (K_L || K_R) where K_L and K_R are DES keys. This is done as follows:

Y := DES3(K)[X] :=
$DES(K_L)[DES^{-1}(K_R)[DES(K_L)[X]]]$

X := $DES3^{-1}$(K)[Y] :=
$DES^{-1}(K_L)[DES(K_R)[DES^{-1}(K_L)[Y]]]$

The encryption process is illustrated in Figure 1.

Figure 1 - Triple DES Encryption



sign( )[ ]	The data in the square brackets is signed using the key in the normal brackets.
verify( )[ ]	The data in the square brackets is verified using the key in the normal brackets.
SHA(x,n)	The n high order bits of the results of applying the SHA-1 hash algorithm to the data string x.

Document Word Usage

The following words are used often in this document and have specific meanings:

- Must

  Defines a product or system capability which is required compelled and mandatory.

- Should

  Defines a product or system capability which is highly recommended.

- May

  Defines a product or system capability which is optional.

2.6 Document Organization

The document is organized as follows:

- Section 1 is the revision log.
- Section 2 is this section and contains an overview of the document and a list of references.
- Section 3 provides an entity overview.
- Section 4 is an overview of transactions that occur at a POS device.
- Section 5 is an overview of transactions that occur at a load device.
- Section 6 discusses the certificates and signatures used in CEP processing.
- Section 7 contains the scheme provider processes.
- Section 8 contains the non transaction related interoperability requirements for a CEP card.

- Sections 9 and 10 contain the specifications for a POS device and the transaction processing that occurs at a POS device.
- Section 11 contains the specifications for merchant acquirer processing.
- Section 12 contains the specifications for a load device
- Sections 13 and 14 contain the specifications for the transaction at the load device and load acquirer processing.
- Section 15 contains the specifications for funds issuer processing.
- Section 16 contains the specifications for card issuer processing.
- Section 17 contains the specifications for processing node transfers.
- Section 18 is the data dictionary.
- Section 19 is a glossary.
- Section 20 is a list of acronyms.

3. Entity Overview

This section describes the entities in a CEP system. The entities are:

- Merchant Acquirer.
- Load Acquirer.
- Card Issuer.
- Funds Issuer.
- Processor.
- Scheme provider.

3.1 Merchant Acquirer

The merchant acquirer is the entity responsible for establishing a business relationship with one or more CEP scheme providers to clear and settle POS transactions.

The merchant acquirer is responsible for the integrity of the POS device and the PSAM it contains. The merchant acquirer is responsible for the creation and distribution of the PSAMs. The merchant acquirer must perform the following tasks relative to processing at the POS device:

- Collect and validate all transactions and provide acknowledgments of successful collection to the POS device or to the merchant.
- Ensure that each batch of transactions is cleared and settled once and only once.
- Ensure that CA public keys, aggregation parameters, certificate revocation lists and optional blocking lists from the scheme providers are sent to the POS devices.

The merchant acquirer system should support all of the CEP requirements for POS processing, including processing that is

optional by scheme. This will facilitate adding additional schemes to its processing.

The merchant acquirer must maintain data for each scheme supported. For each scheme, the merchant acquirer must know the scheme identification, routing for transactions when a direct connection to the card issuer does not exist, whether or not the scheme supports aggregation and the length of time transactions are archived.

The merchant acquirer is responsible for making payment to the merchant and participating in settlement with the recipient of all transactions forwarded for card issuer processing.

3.1.1 PSAM Creators

While the PSAM is a merchant acquirer responsibility, not all merchant acquirers will create their own PSAMs. The entity that creates the PSAMs to be used by the merchant acquirer is referred to as the PSAM creator. Each PSAM creator, which may be a merchant acquirer, must be certified by the scheme provider. Two data fields are used to uniquely identify each PSAM creator, a RID (RID_{PSAM})[1] and a unique number assigned by the owner of the RID to the PSAM creator (the $ID_{PSAMCREATOR}$). The PSAM creator must then assign unique numbers (ID_{PSAM}) to all the PSAMs that it creates. The combination of the RID_{PSAM}, the $ID_{PSAMCREATOR}$ and the ID_{PSAM} will provide a unique number for all CEP PSAMs.

3.2 Load Acquirer

The load acquirer is the entity responsible for establishing a business relationship with one or more CEP scheme providers to manage authorization requests for load and currency exchange transactions and to clear and settle unlinked load transactions.

The load acquiring function consists of two components, the load device and the load acquirer host. The exact division of tasks between these two components will vary from load acquirer to load acquirer. In this document, the interface to the cardholder and the CEP card and the interface to the card issuer, the funds issuer and

[1] The RID may be the RID of a CEP scheme, or a RID obtained by the PSAM creator.

connecting networks are described as a single load acquirer process.

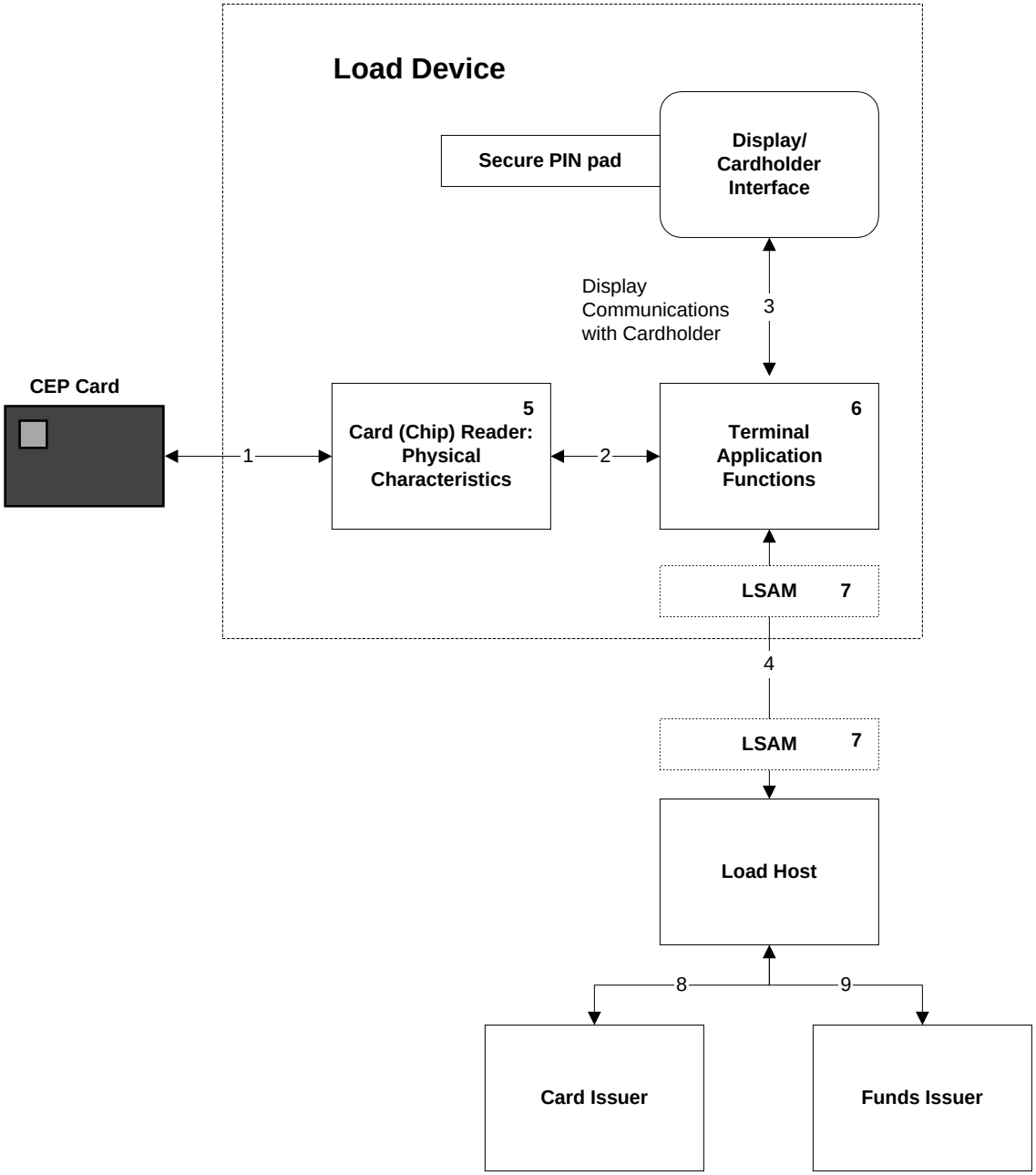
A load secure application module (LSAM) must exist under the control of a load acquirer that supports unlinked loads. The LSAM provides the cryptographic and control processing necessary to secure functioning of unlinked load transactions. The LSAM may reside within the load device or at the load acquirer host.

All interoperable load devices must have a secure PIN pad for PIN entry.

The load acquirer must keep a log of all transactions processed by its systems, regardless of completion status.

Figure 2 provides a high level diagram of the load acquirer components.

Figure 2 - Load Acquirer Components



Item 1 shows the interface with the CEP card. This interface consists of a set of commands to the card and responses to those commands. These commands and responses are defined in this document in sufficient detail to allow interoperability of all CEP cards for the load and currency exchange functions.

Item 2 is the interface between the chip card reader and other load device application functions. This interface is implementation specific and is not described in this document.

Item 3 shows the interface to the cardholder. This interface is defined as the minimum information provided to and required from the cardholder. A secure PIN pad is part of this interface.

Item 4 shows the interface to the load acquirer host. The definition of this interface is at the discretion of the load acquirer.

Item 5 is the chip card reader itself. Requirements for interoperability are provided.

Item 6 is the load device CEP application. Requirements for interoperability are provided.

Item 7 is the LSAM. Requirements for interoperability are provided. LSAMs may be located at the load device or at the load host.

Item 8 is the communication to the card issuer. This communication may include intermediate processing nodes. Interoperable requirements for authorization requests, clearing and settlement are provided.

Item 9 is the communication with the funds issuer for unlinked loads. This communication may include intermediate processing nodes. Interoperable requirements for authorization, clearing and settlement are provided.

3.3 Card Issuer

The card issuer is the entity responsible for establishing a business relationship with one or more CEP scheme providers to issue CEP cards. A card issuer may issue CEP cards for more than one CEP scheme.

The card issuer is responsible for assuring that all the CEP cards it issues contain the data elements required for acceptance at POS and load devices. The card issuer has the responsibility for the liability for all value loaded onto the CEP card and the management of the funds pool. The card issuer is responsible for managing cardholder relationships.

The card issuer is responsible for monitoring transactions received to ensure that the transaction was made by a valid CEP card issued by the card issuer.

The card issuer must:

- Authenticate the CEP card for all load and currency exchange transactions.
- Authorize funds disbursement for linked load transactions.
- Participate in the settlement process for unlinked load transactions and all POS transactions.
- Recognize and track suspect transactions, based on information received from the load acquirer.
- Update and reconcile all changes to card liability and funds pools.

3.4 Funds Issuer

The funds issuer is the entity that authorizes, clears and settles funds requests for unlinked load transactions. Definition of most of the processing for funds issuers is outside the scope of this document. While the funds request sent to the funds issuer must contain an indication that this is a CEP load transaction, no special funds issuer processing is necessary unless required by the scheme.

3.5 Processor

Although transactions may flow directly from a merchant acquirer or load acquirer to a card issuer, many times the transactions will be processed by additional nodes in the network or networks connecting the acquirer and the card issuer. These nodes are referred to as processors.

A processor can be an agent for a merchant acquirer, an agent for a load acquirer, an agent for a card issuer, an agent for a funds issuer or any combination of these entities. All processors must be certified by each scheme provider whose transactions they process.

3.6 Scheme Provider

The scheme provider is the authority responsible for establishing and enforcing the operating rules and regulations, the acceptance mark, and membership criteria. The scheme provider is the authority responsible for establishing an infrastructure for the overall functionality and security of a CEP system.

The scheme provider is responsible for establishing fraud detection and risk prevention policies and procedures for the scheme including information and reporting requirements sufficient to aid in the detection of counterfeit and other types of fraud, and ensuring that these procedures are followed. If a central data repository exists, data for the investigation of fraud must be forwarded by the card issuer.

The scheme provider is responsible for establishing policies and procedures to ensure that all transactions are secured, as defined in these requirements.

The scheme provider must establish certification policies and procedures that ensure compliance with the Common Electronic Purse Specification (CEPS) and with the scheme-specific requirements.

To ensure the delivery of all transactions performed under the scheme, the scheme provider must:

- define routing parameters and procedures for use in routing transactions when the merchant acquirer does not have an existing relationship with the card issuer, and
- establish a unique scheme identifier (AID) consisting of a RID (see reference 5, ISO 7816-5) and, optionally, a PIX selected by the scheme provider.

The scheme provider may establish other entities to process for the scheme. These are described in sections 3.6.1 and 3.6.2.

3.6.1 Processor for the Scheme Provider

The scheme provider must have a processing function to perform the following:

- Distributing information required for security or compliance with the scheme rules and regulations.
- At the scheme provider's option, operating a central data

repository in support of its dispute management, risk management and fraud detection policies and procedures.

3.6.2 Certification Authority

The role of a certification authority(CA), established by a scheme provider, is to generate the CA keys, store the private portion of the keys securely and, based upon valid requests, generate and distribute certificates.

Certification authorities are responsible for certifying the regional or issuer and acquirer public keys.

4. POS Device Transaction Overview

Table 1 shows the transactions that are supported at a POS device and the entities involved in those transactions. Transactions where support by an entity is mandatory are marked “M”. Transactions where support by an entity is optional are marked “O”.

Table 1 - POS Device Transaction Requirements by Entity

CEP TRANSACTIONS	MERCHANT ACQUIRER	CARD ISSUER
Purchase	M	M
Incremental Purchases	O	M
Reversal of the last or only increment of a purchase	O	M
Cancel Last Purchase	O	O

4.1 Purchase

The purchase transaction is an off-line transaction initiated at a POS device, which allows a cardholder to use the electronic value on a CEP card to pay for goods or services.

Some POS devices, such as telephones, support incremental purchases. The transaction is initiated and an initial amount is debited from the CEP card. The CEP card remains inserted in the POS device and subsequent incremental purchase transactions are sent to the CEP card based on time increments or another measure of service received. Cardholder acceptance of the subsequent steps of an incremental purchase transaction is not required, however, the cardholder must be provided a mechanism to terminate additional increments.

A purchase transaction may be reversed, prior to the removal of the CEP card from the POS device, by sending a purchase reversal command to the CEP card. Only the last increment of an incremental purchase may be reversed.

4.2 Cancel Last Purchase

The cancel last purchase transaction is an off-line transaction initiated at a POS device, which allows a cardholder to be re-credited with the electronic value of the last transaction made with their CEP card.

POS devices are not required to support the cancel last purchase command. If this command is supported, the POS device must have access control to prevent unauthorized or fraudulent use of the transaction (e.g. the POS device could ask for a password or a special supervisor key or card). This transaction is only valid if the transaction to be canceled is the last transaction completed by the CEP card. If a transaction has been made after a purchase, for example, a load, the purchase transaction cannot be canceled. Additionally, the transaction to be canceled must not have been collected and must be in an active batch. Only the last step of an incremental purchase may be canceled.

5. Load Device Transaction Overview

Table 2 shows the transactions that are supported at a load device and the entities involved in those transactions. Transactions where support by an entity is mandatory are marked "M". Transactions where support by an entity is optional are marked "O".

Table 2 - Load Device Transaction Requirements by Entity

CEP TRANSACTIONS	LOAD ACQUIRER	CARD ISSUER	FUNDS ISSUER
Load	M[2]	M[3]	M
Currency Exchange	O	O	N/A

A direct connection may exist between the load acquirer and the card issuer. However, in many cases, there may be intermediate processing nodes. These intermediate processing nodes must provide a secure channel to the card issuer. Cryptographic keys must be shared between connecting processing nodes. Shared keys between the load acquirer and the card issuer are not required unless there are no intermediate processing nodes.

5.1 Load

The load transaction allows for the addition of funds onto a CEP card.

Two types of load processing are supported by CEP cards. Some card issuers require a linked load from an account at its financial institution, others allow loading from other sources of funds. If the load is to be performed from another source of funds, the cardholder indicates the source of those funds to the load device during the load process.

[2] Load devices that are available to the general public should support multiple sources of funding and support both linked and unlinked funding accounts. A load device must support at least one type of load.

[3] A card issuer can issue cards that support unlinked loads or linked loads or both.

The type of load to be performed must be selected by the cardholder and supported by the CEP card. The types of load supported by a CEP card are indicated by its application profile (AP_{CEP}). In a linked load, the funding source may be any account that the cardholder maintains at the financial institution that issued the CEP card. The issuer is responsible for the final selection of the funding account.

5.2 Currency Exchange

The currency exchange transaction is used to convert the value in one currency in a CEP application to value in another currency. The resultant value may be added to an existing slot in a CEP application or it may be used to establish a new slot. Partial currency exchanges are allowed.

The currency exchange transaction only involves the card, the acquiring function and the card issuer.

6. Certificates and Signatures

This section describes the certificates and signatures involved in the POS authentication processes. Contents of certificates and dynamic signatures are given, as well as the methods of retrieving, caching and verifying them. Both symmetric and asymmetric cryptographic techniques are used to implement these processes. Public key cryptography is used by the PSAM to authenticate itself to the CEP card and to send a digital signature containing a secret session key. Symmetric cryptography is used by the CEP card to authenticate itself to the PSAM or the card issuer.

Cryptographic methods for creating MACs and encrypting secret data are also described for all transactions.

The security flows for unlinked load transactions and validation of CEP cards by POS devices are described.

6.1 Retrieval of certificates from the CEP card

Certificates are retrieved from the CEP card using the Read Record command (see section 8.6.2). Certificate records are constructed data objects using BER-TLV encoding as described in reference 8, EMV, Annex C. The location of the certificate records is provided in the ADL retrieved from the CEP card in response to the Select command (see section 8.6.1).

6.1.1.1 The ADL must have a single, separate entry for each certificate in the CEP card. An ADL entry for a certificate must describe the location of one of the following:

- One record containing only a single certificate. The certificate encapsulates an entire public key. Table 3 provides the format of this record.

Table 3 - Certificate Record with No Remainder

Field	Contents	Length
Tag	'70'	1
Length	Length of following data	1-2
Tag	'90'	1
Length	Length of certificate	1-2
Data	Certificate	var

- One record containing two data objects (in the order specified):
  - a certificate that encapsulates only the leftmost portion of a public key, and
  - a public key remainder that contains the rightmost portion of the public key.

  Table 4 provides the format of this record.

Table 4- Format of Record with Both a Certificate and a Remainder

Field	Contents	Length
Tag	'70'	1
Length	Length of following data	1-2
Tag	'90'	1
Length	Length of certificate	1-2
Data	Certificate	var
Tag	'91'	1
Length	Length of remainder	1-2
Data	Remainder	var

- A sequence of two consecutive records in a single file. The first record contains a certificate that encapsulates only the leftmost portion of a public key. The second record contains only a public key

remainder field. The formats of the two records are given in Table 5.

Table 5 - Public Key Certificate in Two Records

	Field	Content	Length
Record 1	Tag	'70'	1
	Length	Length of following data	1-2
	Tag	'90'	1
	Length	Length of certificate	1-2
	Data	Certificate	var
Record 2	Tag	'70'	1
	Length	Length of following data	1-2
	Tag	'91'	1
	Length	Length of remainder	1-2
	Data	Remainder	var

6.1.1.2 The certificate entries in the ADL must be consecutive and must be in the order in which the certificates are to be verified.

6.1.1.3 The ADL entry for the issuer certificate can be recognized using the format code in bits b4-b1 of byte 4 of the entry. The format code for the issuer certificate is 0010b. The POS device may (optionally) cache issuer certificate data after successful verification of a CEP card signature. Thereafter, when presented with a CEP card bearing the same issuer certificate, the POS device may bypass reading of the issuer certificate and all higher level certificates. The POS device then proceeds to the next lower certificate.

The POS device can recognize a CEP card bearing a issuer certificate cached in the POS device by examining $VKP_{CA,ISS}$, $ID_{REG,ISS}$, $VKP_{REG,ISS}$ and CSN_{ISS} in the response to the Initialize for Purchase command. The $VKP_{CA,ISS}$, $ID_{REG,ISS}$, $VKP_{REG,ISS}$ and CSN_{ISS} in the response must match a $VKP_{CA,ISS}$, $ID_{REG,ISS}$, $VKP_{REG,ISS}$

and CSN_{ISS} that identifies a cached issuer certificate for the scheme. The scheme is identified by the AID of the selected application.

A similar function may be used to cache public keys in the PSAM, bypassing the need to send frequently used issuer certificates to the PSAM and also bypassing the PSAM verification of the certificate.

No provision is made for caching certificates at levels other than Issuer or Merchant Acquirer level. Of course, if the issuer or acquirer certificate or public key is cached, the processing of a corresponding regional certificate or public key is unnecessary.

6.1.1.4 Whether the POS device begins with the ADL entry following the entry for the issuer certificate or the ADL entry for the first (highest level) certificate, the POS device must read and validate certificates for all successive ADL entries until either validation fails or the last certificate ADL entry has been processed.

6.2 Processing Certificates from the POS Device

Certificates reside in the POS device or the PSAM to permit the CEP card to validate the dynamic signature created by the PSAM during purchase processing. Certificates and related information are delivered to the CEP card using the Verify Certificate command (see section 10.1.3).

6.2.1.1 In the response to the Initialize for Purchase command (see section 10.1.1), the CEP card may provide the serial number (CSN_{ACQ}) of an acquirer certificate that has already been processed and verified by the CEP card. If the key version ($VKP_{CA,ACQ}$) and serial number (and $ID_{REG,ACQ}$, if a regional CA was used) match those of a certificate used by the POS device for the selected AID, the POS device may begin delivery of certificates to the CEP card with the next certificate lower in the hierarchy than the one already processed. If this data is not provided, or if no match is found, the POS device must begin delivery with the highest certificate in the hierarchy (PKC_{ACQ} or $PKC_{REG,ACQ}$).

6.2.1.2 Delivery of certificates to the CEP card proceeds with successively lower level certificates until all certificates have been verified successfully, or until a certificate fails verification. If a certificate fails verification, normal processing of the transaction must be stopped and exception processing followed.

6.3 Verifying Certificates

6.3.1.1 Verification of a certificate begins with recovery of the certificate data using the appropriate public key, either the CA public key or the key resulting from verification of the next higher level certificate.[4] The recovery can only be done if the length of the certificate is the same as the length of the modulus of the public key used in the verification. If the lengths are different, verification has failed.

6.3.1.2 After verifying the certificate, the header (first byte) and the trailer (last byte) from the recovered data must be checked. The header must be '4A' or '6A' and the trailer must be 'BC'. If not, verification of the certificate has failed.

6.3.1.3 The hash value in each certificate is always a 20 byte field immediately preceding the last (trailer) byte of the certificate. The hash value must be verified according to the following procedure:

1) The certificate data must be recovered using the appropriate key, either the CA public key or the key recovered by verifying the next higher level certificate.
2) Data must be concatenated in the following order (left to right):
    a) All data beginning with the format code in the certificate (which is always the second byte of the certificate) up to and including the last byte before the hash total, in the order in which it appears in the certificate.

[4] Caching of certificate data does not change this. It simply provides a faster means of determining the data from the higher level certificate.

b) The Public Key Remainder field (PKR), if it exists.

3) The hash algorithm indicated (SHA-1 is the only hash algorithm supported) is applied to the concatenation, producing a 20 byte result.

4) This result is compared to the hash value in the certificate. If they are unequal, certificate verification is unsuccessful.

6.3.2 The CEP Card Certificate Hierarchy

6.3.2.1 A regional certificate is optional in the hierarchy of certificates used to authenticate the CEP card. If the regional certificate exists, it is verified using the CA public key ($PK_{CA,ISS}$). The recovered data has the format described in Table 6.

6.3.2.2 The POS device must check that the regional certificate number is not in the scheme provider's certificate revocation list. If it is, the certificate has been revoked, and validation has failed.

Table 6 - Format of the Issuer Regional Certificates

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field ($PKR_{REG,ISS}$), '4A' - if there is no associated remainder field	1
Format Code	Certificate Format, value '01'	1
$ID_{REG,ISS}$	Identifier of the region, assigned by the scheme provider.	4
CED	Certificate expiration date (MMYY)	2
$CSN_{REG,ISS}$	Binary number unique to this certificate assigned by the certification authority	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{REG,ISS}$	Identifies the algorithm used to verify the next lower level certificate	1
$LPKM_{REG,ISS}$	Identifies the length of the regional public key modulus in bytes	1
Filler	'00'	1
$PKM_{REG,ISS}$	Regional public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{CA,ISS}$-36. If the length of the modulus is > $LPKM_{CA,ISS}$-36, the rightmost bytes (beginning in position $LPKM_{CA,ISS}$-35) are kept in $PKR_{REG,ISS}$.	$LPKM_{CA,ISS}$ - 36
Hash Result	Hash of certificate data	20
Trailer	'BC'	1

6.3.2.3 In addition to checking the header, trailer, and hash results in the regional certificate, the POS device must check that the certificate expiry date (CED) is not earlier than the current date. If this check fails, the certificate has failed validation.

6.3.2.4 Issuer certificates are identified by a format code of '02' in the recovered data. Issuer certificates have the format specified in Table 7.

6.3.2.5 The POS device must check the CED in the data recovered from the issuer certificate. If it is earlier than the current date, certificate validation has failed.

6.3.2.6 The POS device must check that the issuer certificate number is not in the scheme provider's certificate revocation list. If it is, the certificate has been revoked, and validation has failed.

6.3.2.7 The POS device must check that the ID_{ISS} recovered from the issuer certificate is the same as the $ID_{ISS,CEP}$ in the response to the Initialize for Purchase command. If it is not, validation of the certificate has failed.

Table 7 - Format of the Issuer Certificate

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field (PKR_{ISS}), '4A' - if there is no associated remainder field	1
Format code	Certificate Format ('02')	1
ID_{ISS}	Issuer ID	4
CED	Certificate expiration date (MMYY)	2
CSN_{ISS}	Binary number unique to this certificate assigned by the certification authority or the region	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{ISS}$	Identifies the algorithm used to verify the next lower level certificate	1
$LPKM_{ISS}$	Length of the modulus of the issuer public key	1
Filler	'00'	1
PKM_{ISS}	Issuer public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{CA,ISS}$-36 (or $LPKM_{REG.ISS}$-36). If the length of the modulus is > $LPKM_{CA,ISS}$-36 (or $LPKM_{REG.ISS}$-36), the rightmost bytes (beginning in position $LPKM_{CA,ISS}$-35 (or $LPKM_{REG.ISS}$-35)) are kept in PKR_{ISS}.	$LPKM_{CA,ISS}$-36 or $LPKM_{REG,ISS}$-36
Hash Result	Hash of certificate data.	20
Trailer	'BC'	1

6.3.2.8 Card certificates are identified by a format code of ‘04’. Data recovered from a card certificate has the format specified in Table 8.

6.3.2.9 The POS device must check that CED in the data recovered from the certificate is not earlier than the current date. If it is, certificate validation has failed.

6.3.2.10 In a purchase transaction, the POS device must check that the ID_{ISS} recovered from the card certificate is the same as the $ID_{ISS,CEP}$ in the response to the Initialize for Purchase command response. If it is not, validation of the certificate has failed.

6.3.2.11 In a purchase transaction, the POS device must check that the ID_{CEP} recovered from the card certificate is the same as the ID_{CEP} in the response to the Initialize for Purchase command response. If it is not, validation of the certificate has failed.

Table 8 - Format of the Card Certificate

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field (PKR_{CEP}), '4A' - if there is no associated remainder field	1
Format code	Certificate Format ('04')	1
ID_{ISS}	Issuer ID	4
ID_{CEP}	Identifier of the CEP card	6
CED	Certificate expiration date (MMYY)	2
CSN_{CEP}	Binary number unique to this certificate assigned by the issuer	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{CEP}$	Identifies the algorithm used with the public key of the CEP card	1
$LPKM_{CEP}$	Length of the modulus of the card public key	1
Filler	'00'	1
PKM_{CEP}	Card public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{ISS}$-42. If the length of the modulus is > $LPKM_{ISS}$-42, the rightmost bytes (beginning in position $LPKM_{ISS}$-41) are kept in PKR_{CEP}.	$LPKM_{ISS}$-42
Hash Result	Hash of certificate data	20
Trailer	'BC'	1

6.3.3 The PSAM Certificate Hierarchy

6.3.3.1 The CEP card contains a CA public key ($PK_{CA,ACQ}$) for the purpose of authenticating the PSAM in the POS device. The CEP card contains only a single such key. The POS device must contain the necessary certificates for use with the $PK_{CA,ACQ}$ in each CEP card supported by the POS device.

6.3.3.2 The POS device must determine the correct set of certificates to be used for a transaction by examining $VKP_{CA,ACQ}$ returned by the CEP card in response to the

Initialize for Purchase command and the AID of the application selected.

6.3.3.3 A regional certificate is optional in the hierarchy of certificates used to authenticate the PSAM. If the regional certificate exists, it is verified using the CA public key ($PK_{CA,ACQ}$) in the CEP card. The recovered data has the format described in Table 9.

6.3.3.4 In a purchase transaction, the CEP card must check that the $ID_{REG,ACQ}$ recovered from the regional certificate is the same as the ID_{REG} in the Verify Certificate command. If it is not, validation of the certificate has failed.

Table 9 - Format of the Acquirer Regional Certificates

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field ($PKR_{REG,ACQ}$), '4A' - if there is no associated remainder field	1
Format Code	Certificate Format, value '81'	1
$ID_{REG,ACQ}$	Identifier of the region, assigned by the scheme provider. Right justified in the field and preceded with '00's.	4
CED	Certificate expiration date (MMYY)	2
$CSN_{REG,ACQ}$	Binary number unique to this certificate assigned by the certification authority	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{REG,ACQ}$	Identifies the algorithm used to verify the next lower level certificate	1
$LPKM_{REG,ACQ}$	Identifies the length of the regional public key modulus in bytes	1
Filler	'00'	1
$PKM_{REG,ACQ}$	Regional public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{CA,ACQ}$-36. If the length of the modulus is > $LPKM_{CA,ACQ}$-36, the rightmost bytes (beginning in position $LPKM_{CA,ACQ}$-35) are kept in $PKR_{REG,ACQ}$.	$LPKM_{CA,ACQ}$ - 36
Hash Result	Hash of certificate data	20
Trailer	'BC'	1

6.3.3.5 Acquirer certificates are identified by a format code of '82' in the recovered data. Acquirer certificates have the format specified in Table 10.

6.3.3.6 In a purchase transaction, the CEP card must check that the $ID_{PSAMCREATOR}$ from the recovered data is the same as the $ID_{PSAMCREATOR}$ provided in the Verify Certificate command. If it is not, validation of the certificate has failed.

Table 10 - Format of the Acquirer Certificate

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field (PKR_{ACQ}), '4A' - if there is no associated remainder field	1
Format Code	Certificate Format ('82')	1
RID_{PSAM}	RID used by the PSAM creator	5
$ID_{PSAMCREATOR}$	Identifier of the PSAM creator assigned by the owner of the RID_{PSAM}	4
CED	Certificate expiration date (MMYY)	2
CSN_{ACQ}	Binary number unique to this certificate assigned by the certification authority or the region	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{ACQ}$	Identifies the algorithm used to verify the next lower level certificate	1
$LPKM_{ACQ}$	Length of the modulus of the acquirer public key	1
Filler	'00'	1
PKM_{ACQ}	Acquirer public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{CA,ACQ}$-41 (or $LPKM_{REG,ACQ}$-41). If the length of the modulus is > $LPKM_{CA,ACQ}$-41 (or $LPKM_{REG,ACQ}$-41), the rightmost bytes (beginning in position $LPKM_{CA,ACQ}$-40 (or $LPKM_{REG,ACQ}$-40)) are kept in PKR_{ACQ}.	$LPKM_{CA,ACQ}$-41 or $LPKM_{REG,ACQ}$-41
Hash Result	Hash of certificate data	20
Trailer	'BC'	1

6.3.3.7 PSAM certificates are identified by a format code of '84'. Data recovered from a PSAM certificate have the format specified in Table 11.

6.3.3.8 In a purchase transaction, the CEP card must check that the ID_{PSAM} from the recovered data is the same as the ID_{PSAM} provided in the Verify Certificate command. If it is not, validation of the certificate has failed.

Table 11 - Format of the PSAM Certificate

Field	Contents	Length
Header	Certificate Header '6A' - if there is an associated remainder field (PKR_{PSAM}), '4A' - if there is no associated remainder field	1
Format Code	Certificate Format ('84')	1
RID_{PSAM}	RID used by the PSAM creator	5
$ID_{PSAMCREATOR}$	Identifier of the PSAM creator, assigned by the owner of RID_{PSAM}	4
ID_{PSAM}	Identifier of the PSAM	4
CED	Certificate expiration date (MMYY)	2
CSN_{PSAM}	Binary number unique to this certificate assigned by the PSAM creator	3
ALGH	Identifies the algorithm used to create the hash value. '01' indicates SHA-1, and is the only algorithm supported.	1
$ALGP_{PSAM}$	Identifies the algorithm used to verify the dynamic signature created by the PSAM	1
$LPKM_{PSAM}$	Length of the modulus of the PSAM public key	1
Filler	'00'	1
PKM_{PSAM}	PSAM public key modulus or the leftmost bytes of the modulus. Padded to the right with 'BB' if the length of the modulus is less than $LPKM_{ACQ}$-45. If the length of the modulus is > $LPKM_{ACQ}$-45, the rightmost bytes (beginning in position $LPKM_{ACQ}$-44) are kept in PKR_{PSAM}.	$LPKM_{ACQ}$-45
Hash Result	Hash of certificate data	20
Trailer	'BC'	1

6.4 Dynamic Signature Verification

The PS_2 created by the PSAM serves two purposes. It allows the CEP card to authenticate the PSAM and it transmits a session key ($SESSKey_{PSAM}$) to the CEP card to be used for subsequent authentication between the CEP card and the PSAM. The creation of the PS_2 and the digital signature (DS) it contains is described in section 10.1.4.

6.4.1.1 The CEP card must apply its private key and the associated algorithm to PS_2 in order to recover the encrypted digital signature (DS). The data recovered is described in *Table 51 - Format of the Data Recovered from the PS2*. The CEP card then applies the public key of the PSAM (PK_{PSAM}) with the algorithm and exponent encoded by $ALGP_{PSAM}$ (from the PSAM Certificate) to recover the data described in *Table 52 - Format of the Data Recovered from DS*.

6.4.1.2 After recovering this data, the CEP card must check the contents of the DS hash (see *Table 53 - Contents of the DS Hash*) for validation. If this validation fails, PS_2 has failed validation. If validation is successful, the CEP card extracts $SESSKey_{PSAM}$ from the recovered data and uses this 16 byte key with triple DES for symmetric cryptographic exchange of the S_2 and S_3 MACs in the remainder of the transaction. If a Cancel Last Purchase transaction is used to cancel the last or only step of this transaction, $SESSKey_{PSAM}$ is also used for MACs in that transaction.

6.5 Cryptographic Mechanisms

6.5.1.1 Asymmetric cryptography must comply with Annexes E and F of the EMV IC Card Specification, reference 8.

6.5.1.2 Symmetric cryptographic methods used for S_1, S_2, and S_3 in load and currency exchange transactions are at the discretion of the card issuer, but the use of DES with a 16 byte key (triple DES) is recommended. Alternative methods must provide at least equivalent strength.

6.5.1.3 The mechanism for generating the S_1, S_2, and S_3 MACs in POS transactions must be the ISO optional process 1

as described in reference 8, EMV annex E1.2 and in ISO 9797, reference 6. The MAC key used must be a double length key.

6.5.1.4 In POS transactions, cryptographic methods used for S_6 are at the discretion of the issuer. Cryptographic methods used for S_4 and S_5 are at the discretion of the Merchant Acquirer. For all these MACs, the use of DES with a 16 byte key (triple DES) is recommended. Alternative methods must provide at least equivalent strength.

6.5.1.5 Encrypting of R_1 in unlinked load transactions should use triple DES, but encrypting with single DES is sufficient where necessary to pass R_1 through networks and arrive at the issuer in a key known to the issuer. Migration to triple DES is encouraged where possible.

See section 6.6 for a definition of R_1.

6.5.1.6 R_1 must be used, as described in reference 8, EMV, to create the following MAC for unlinked load transactions:

- MAC_{LSAM}, sent by the load acquirer to the card issuer in the load request.

For MAC_{LSAM} only the 4 most significant bytes are transmitted.

6.5.1.7 The SHA-1 hash algorithm must be used to create the hash values (H_{CEP}, H_{LSAM} and $H2_{LSAM}$) used for unlinked load security. These hashes are described below.

H_{CEP} := SHA([ID_{LACQ}|| ID_{LDA}| |ID_{ISS}|| ID_{CEP}|| NT_{CEP}|| R_{CEP}], 80)

H_{LSAM} := SHA([ID_{LACQ}|| ID_{LDA}|| ID_{ISS}|| ID_{CEP}|| NT_{CEP}|| R_{LSAM}], 64)

$H2_{LSAM}$:= SHA([ID_{LACQ}| |ID_{LDA}|| ID_{ISS}|| ID_{CEP}|| NT_{CEP}|| $R2_{LSAM}$], 64)

6.6 Unlinked Load Security Flow

Figure 3 below shows the flow of data that provides the security for unlinked load transactions. The data elements listed in that flow are as follows:

6.6.1.1 The H_{CEP} that is sent from the CEP card to the LSAM in the response to the Initialize for Load will provide proof to the LSAM of a valid error from the CEP card in the response to the Credit for Load command. The issuer must be able to determine the value of R_{CEP}, a component of H_{CEP}, from the data sent for the transaction and must verify that the correct H_{CEP} is held by the LSAM. See 6.6.1.8.

6.6.1.2 The S_1 MAC that is sent from the CEP card to the card issuer is used by the card issuer to authenticate the CEP card as valid.

6.6.1.3 The H_{LSAM} that is sent from the LSAM to the card issuer is used to distinguish between an approved load and a declined load request. It must be included in the S_2 MAC of an approved request and not included in the S_2 MAC of a declined request.

6.6.1.4 The $H2_{LSAM}$ that is sent from the LSAM to the card issuer will be used by the card issuer to verify a completion message for a transaction where the S_2 MAC was not sent to the CEP card.

6.6.1.5 R_1 is generated by the LSAM and encrypted under a key that allows secure transport to the card issuer. R_1 provides a session key between the load acquirer and the card issuer for this transaction.

6.6.1.6 The MAC_{LSAM} provides protection for the transaction data, H_{CEP}, H_{LSAM}, $H2_{LSAM}$ and S_1. It also provides a guarantee that the load acquirer owes the transaction amount to the card issuer.

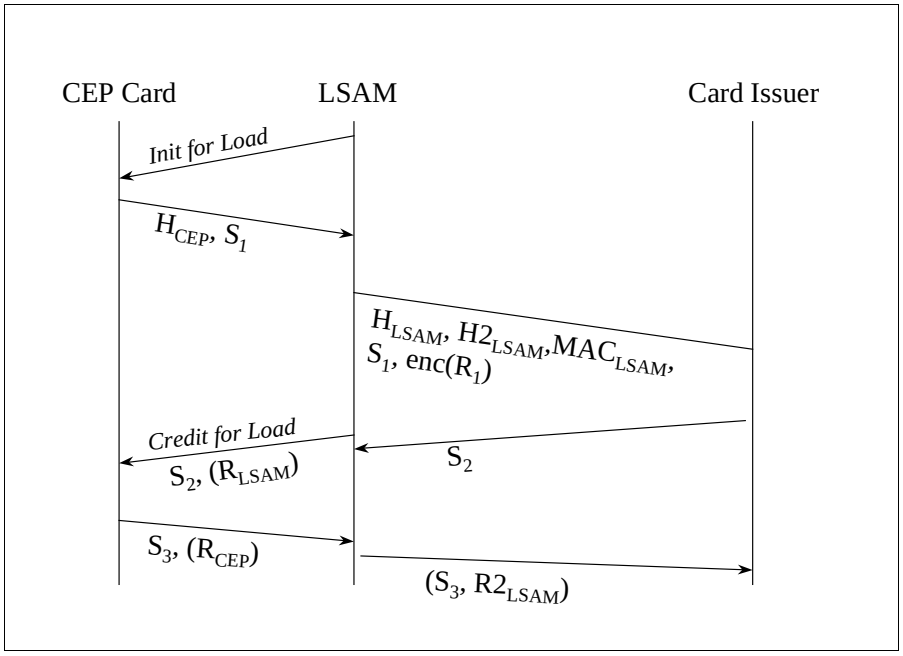
6.6.1.7 The R_{LSAM} is sent to the CEP card if an approval is received from the card issuer. This allows the CEP card to verify the S_2 MAC. The H_{LSAM} must be included in the S_2 MAC for approved transactions. The R_{LSAM} is

not sent to the CEP card if an decline is received from the card issuer. The H_{LSAM} must not be included in the S_2 MAC for declined transactions.

6.6.1.8 The R_{CEP} is sent by the CEP card to LSAM in the response to the Credit for Load command if there was an error. See 6.6.1.1.

6.6.1.9 The $R2_{LSAM}$ is sent to the card issuer in case of an error. The $R2_{LSAM}$ negates the guarantee of the H_{LSAM} and the load acquirer no longer owes the transaction amount to the card issuer.

Figure 3 - Security Flow for Unlinked Load



6.7 Security Flow for POS Device Validation of CEP Cards

A purchase transaction must be validated by a PSAM before the transaction can be completed. For incremental purchases in some terminal infrastructures (e.g. payphones where the PSAM is remote

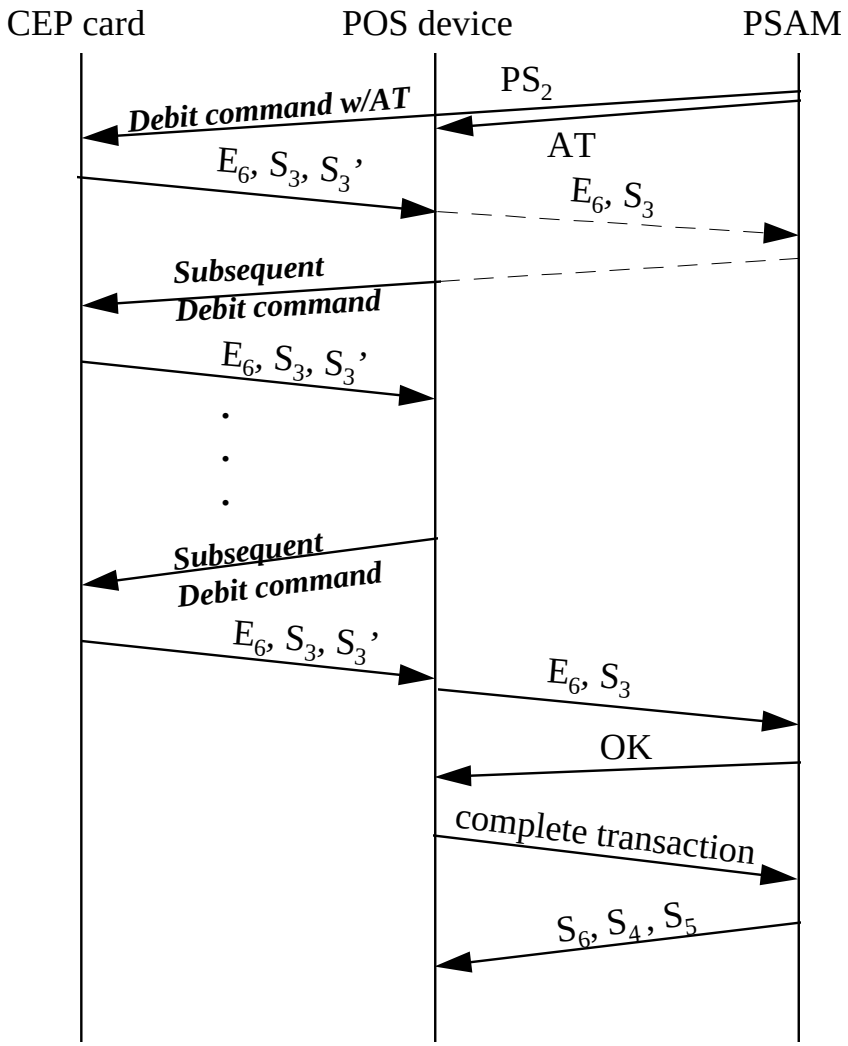
and inaccessible during voice communications), a merchant acquirer may decide to:

- Have the PSAM validate the card during the first increment.
- Have intermediate validation done by a POS device until all increments of a purchase transaction are completed.
- Have the validation of the final increment done by the PSAM.

Figure 4 below shows the flow of the data that provides the security for incremental purchase transaction when intermediate validation of the CEP card is done by the POS device and the PSAM validates the CEP card at the completion of the last increment.

Intermediate card validation by the POS device is optional for both the CEP card and the PSAM. CEP card support for this feature is indicated in the AM_{CEP} field.

Figure 4 – Purchase Security Flow for POS Device Validation of CEP Cards



6.7.1.1 The PSAM must generate an authentication token (AT) to allow the POS device to validate the CEP card on purchase increments not validated by the PSAM. The AT is sent to the POS device in a manner consisted with the PSAM/POS device protocol and to the CEP card in the PS_2 MAC.

6.7.1.2 The CEP card responds with an encrypted S_6 (E_6), an S_3 to allow PSAM validation of the CEP card and an S_3' based on the AT to allow POS device validation of the CEP card.

6.7.1.3 The POS device should allow the PSAM to validate the CEP card once and then may process subsequent debit commands, validating the CEP card using the S_3'.

6.7.1.4 The PSAM must validate the CEP card on the final increment.

6.7.1.5 When all increments of the purchase have been completed, the POS device informs the PSAM that the transaction is complete, and the PSAM returns the unencrypted S_6 MAC, the S_5 MAC and, if it is created at the time, the S_4 MAC.

7. Scheme Provider Procedures

This section describes the scheme provider's responsibilities which support the establishment of an infrastructure for the overall functionality and security of a CEP system. These responsibilities include both administrative and processor functions for defining:

- The scheme's rules and regulations.
- The certification criteria and procedures.
- The establishment of a certification authority and its responsibilities.
- The rules and guidelines for risk management.
- The operating rules and parameters.
- The dispute management process.
- The transaction routing procedures.

7.1 Operating Rules and Regulations

7.1.1.1 The scheme provider must:

- Develop and maintain an acceptance mark (brand) and a corresponding application identifier (AID).
- Develop operating rules and regulations for the scheme.
- Provide documentation to participating entities, including vendors and suppliers, who wish to develop scheme-specific CEP compliant systems.
- Establish rules and procedures which ensure that the entire process between merchants, merchant acquirers, card issuers and processors is auditable and reconcilable.

- Establish rules and procedures which ensure that the entire process between load acquirers, funds issuers, card issuers and processors is auditable and reconcilable.

7.1.1.2 The scheme provider must determine operational policies and procedures which support:

- Interaction with a Certification Authority for the generation of public key certificates.
- Component and system certification.
- Risk management and fraud detection.
- The distribution of data supporting operating rules used to control required processing.
- The definition and distribution of aggregation parameters, which are listed in *Table 14 - Aggregation Parameters*.
- The distribution of CA public keys.
- The distribution of issuer certificate revocation lists, and card blocking lists.

7.2 Certification

The scheme provider is responsible for defining certification requirements which support the objectives of the Common Electronic Purse Specification (CEPS), to:

- Ensure that consistency exists in the acceptance environment.
- Provide a CEP interoperable environment for different technology platforms or schemes.

7.2.1.1 The scheme's certification specifications must conform to the CEP certification requirements which will be documented separately. A scheme's certification specifications must cover all components and entities of the system, including:

- CEP cards.
- Purchase Secure Application Modules (PSAM).
- POS devices.
- Load devices.
- LSAMs
- Secure PIN pads
- Merchant acquirer processing systems.
- Card issuer processing systems.
- Funds issuer processing systems
- Load acquirer processing Systems.
- Card vendors, including but not limited to, chip manufacturers, card manufacturers, chip embedders and personalizers.
- Terminals and devices
- Terminal and device vendors (optional for a scheme).
- Certification authority.

7.2.1.2 The scheme must track all certified components, participants, and certification status and make this information available to load acquirers, merchant acquirers or card issuers as needed.

7.3 Certification Authority Management

7.3.1.1 The scheme provider must establish a certification authority (CA) and ensure that it is certified as such.

7.3.1.2 Where a regional certification authority does not exist, the scheme provider is responsible for the interface

between a certification authority (CA) and card issuers and PSAM creators.

7.3.1.3 Where a regional certification authority does exist, the scheme provider is responsible for the interface between a certification authority (CA) and the regional certification authority.

7.3.1.4 The scheme provider must arrange to have one or more scheme RSA key pairs for CEP card verification generated ($SK_{CA,ISS}$ and $PK_{CA,ISS}$) and assigned version numbers ($VKP_{CA,ISS}$).

7.3.1.5 The scheme provider must arrange to have one or more scheme RSA key pairs for PSAM verification ($SK_{CA,ACQ}$ and $PK_{CA,ACQ}$) generated and assigned version numbers ($VKP_{CA,ACQ}$).

7.3.1.6 The scheme provider must distribute the public key portions of the scheme RSA key pairs for CEP card authentication ($PK_{CA,ISS}$), along with their version numbers, to all merchant acquirers or PSAM creators.

7.3.1.7 The scheme provider must distribute the public key portions of the scheme RSA key pairs for PSAM verification ($PK_{CA,ACQ}$), along with their version numbers, to all card issuers.

7.3.1.8 The certification authority must receive the request for a public key certificate from the PSAM creator, card issuer, or regional certification authority, along with that entity's public key.

7.3.1.9 The certification authority must send the certificate(s) to the requesting PSAM creator, card issuer, or regional certification authority along with sufficient information to allow the recipient to identify the certificate.

7.4 Risk Management

7.4.1.1 The scheme provider must maintain a certificate revocation list and periodically distribute that list to all merchant acquirers accepting the brand.

7.4.1.2 The scheme provider must establish rules to ensure that the merchant acquirer loads the certificate revocation list into all POS devices under its control.

7.4.1.3 The notification of the certificate revocation list must include, at a minimum, the data elements listed in Table 12.

Table 12 - Data Elements Required for Certificate Revocation List

Field	Content / Source	Length
$CSN_{REG,ISS}$ or CSN_{ISS}	Regional or Issuer Certificate Serial Number	3
DTRM	Date transmitted, for audit use only - YYMMDD	3
ID_{ISS}	Issuer identification - zero if certificate being revoked is a regional certificate	4
$ID_{REG,ISS}$	Identifier of the region - zeros if regional certificate is not used	4
RID_{CEP}	Scheme identification	5
$VKP_{CA,ISS}$	CA Public Key version number	1
$VKP_{REG,ISS}$	Regional public key version number - only required if both the identifier of the region and the id of the issuer are present	1

7.4.1.4 The scheme provider may establish a central data repository for the investigation of invalid card issuer MAC(s) (S_6). The minimum required data that must be provided is the full transaction detail as received from the merchant acquirer and defined in section 11.

A scheme may require additional information.

7.4.1.5 The scheme provider may establish a central data repository to be used for fraud detection and risk analysis. The process and the data to be provided must be determined by the scheme.

7.4.1.6 The scheme provider should define procedures which allow it to gather information to monitor component performance, including consumer cards, PSAMs, LSAMs, devices, and certified processing systems.

7.4.1.7 The scheme provider may maintain a card blocking list and periodically distribute that list to all merchant acquirers accepting the brand.

7.4.1.8 If the scheme provider maintains and distributes a card blocking list, the scheme provider should establish rules to ensure that the merchant acquirer loads the card blocking list into all POS devices under its control.

7.4.1.9 The notification of the card blocking list must include the minimum data elements in Table 13.

Table 13 - Data Elements Required for the Card Blocking List

Field	Description	Length
DTRM	Date transmitted	3
ID_{CEP}	Beginning card serial number (of the range to be blocked)	6
ID_{CEP}	Ending card serial number (of the range to be blocked)	6
ID_{ISS}	Issuer Identification	4
RID_{CEP}	Scheme Identifier	5

7.5 Operating Rules

7.5.1.1 The scheme provider must determine the operating rules which must be implemented by the participants, whether card issuer, merchant acquirer or load acquirer. The operating rules cover:

- Use of a regional public key.
- Use of aggregation.
- Use of truncation.
- Use of a central data repository to investigate invalid MACs.
- Use of a central data repository for fraud analysis

and risk management.

- Centralized card activity reporting in support of global product usage.

7.5.1.2 The scheme provider must specify the maximum period of time between the issuance of a CEP card and its expiration dates.

7.5.1.3 The scheme provider must specify the period for which POS and on-line transaction logs, including MACs, must be kept.

7.6 Aggregation Parameters

Aggregation is optional on the part of both the POS device and the CEP card. The CEP card must communicate to the POS device whether or not aggregation is allowed in the card purchase options (CPO) field. The card process for making its decision is at the discretion of the issuer, and must be documented in proprietary specifications.

7.6.1.1 The scheme provider must determine whether or not to support the use of aggregation.

7.6.1.2 If aggregation is supported, then the scheme provider must determine the value to be used for the detail transaction percentage for the POS device when aggregation is supported. This parameter is explained in Table 14.

Table 14 - Aggregation Parameters

Field	Description	Length
NT_{PCT}	Detail Transaction Percentage. The percentage of detail transactions that a scheme requires from a POS device certified to perform aggregation. For example, if this parameter is set to 10, 90% of transactions may be aggregated.	1

7.6.1.3 The scheme provider must establish procedures for the distribution of this aggregation parameter, including periodic updates if required.

7.7 Dispute Management

7.7.1.1 If the scheme has a dispute resolution process to resolve any issues relating to invalid S_6 MACs, the scheme provider must establish procedures for invoking the dispute management process. The card issuer initiates the dispute process. The merchant acquirer participates in the dispute process. Intermediate processing nodes may be involved in a scheme's dispute process.

7.8 Transaction Flows

7.8.1.1 The scheme provider must establish rules which ensure the routing, security and integrity of all transaction transfers between the acquirers and card issuers. Actual network addressing required for the routing of transactions between entities is outside the scope of this document.

8. CEP Card Requirements

This section discusses CEP card requirements that are either transaction independent or cross transactions. The sections on POS device transaction processing and load device transaction processing contain additional CEP card requirements.

8.1 Compatibility

8.1.1.1 The Common Electronic Purse (CEP) application must be implemented only in cards that comply with reference 8, EMV version 3.1.1 Part I and Application Selection as specified in EMV Part III.

8.1.1.2 The CEP card must support either T=0 or T=1 as described in reference 8, EMV.

8.1.1.3 The CEP should support deactivation of the CEP application. The CEP card may also support the ability to temporarily lock and unlock the CEP application.

8.2 Multiple Currencies

8.2.1.1 The CEP card must support one or more currencies. Each currency occupies a “slot” within the CEP application. The slots are configurable in terms of the currency supported. The currency for an individual slot is determined during personalization, load, or currency exchange. It is an card issuer’s decision as to which currencies may be assigned to slots in the CEP, and as to which slots are reconfigurable.

8.2.1.2 A single currency must not occupy more than one slot.

8.2.1.3 The CEP card must limit each slot to a maximum balance. The maximum balance for each slot is established when a currency is assigned to the slot and is determined by the card issuer. The maximum balance may be altered during on-line transactions.

8.2.1.4 The CEP card must not allow a slot to exceed the maximum balance determined by the card issuer. The

CEP card must detect and must reject any command that attempts raise the new balance above the maximum permitted value.

8.2.1.5 A card issuer may identify a slot with a currency code that cannot be changed. The CEP card must manage processing of this slot.

8.3 Interface to Terminals

8.3.1.1 The CEP card must interface with the four types of terminals described in sections 8.3.2 through 8.3.5.

8.3.2 Load Devices

The load device, installed by the load acquirer, provides service to the CEP card for loading new value into the CEP card or exchanging value on the CEP card by establishing an on-line communication channel between the CEP card and the card issuer's secure application module (ISAM). Load devices are further described in section 12.

8.3.3 POS Devices

The POS device is installed at a merchant location. It is used by the cardholder to purchase goods or services in return for payment realized as a reduction of the balance within the CEP card in the currency being used for the transaction. POS devices are further described in section 9.

8.3.4 Monitoring Devices

Monitoring devices enable the cardholder to read various data from the CEP card, such as slot balances and data from the most recent transactions. This functionality may also be provided by other devices, such as load or POS devices.

8.3.5 Personalization Devices

The process of personalizing the CEP application is outside the scope of this document.

8.4 General Status Conditions

8.4.1.1 The CEP card must return status conditions (SW1 and SW2) in response to all commands sent to it. General status conditions are listed in Table 15. Status conditions that are specific to a command are listed with the command itself.

Additional codes to those specified in this document may occur in response to a command, and will be taken to mean failure of the command.

Except as noted in this document, or if proprietary processing is being performed, an SW1SW2 other than ‘9000’ must result in termination of the transaction.

Table 15 - General Status Conditions for all Commands

SW1	SW2	Meaning
'90'	'00'	Normal processing, data may be present in the response field
'61'	'xx'	For T=1 in [EMV'96]. Normal processing. Length of returned data is xx.
'65'	'81'	Memory failure
'67'	'00'	Wrong length
'69'	'85'	Conditions of use not satisfied
'6A'	'80'	Incorrect parameters in the data field
'6A'	'81'	Function not supported
'6A'	'86'	Incorrect parameters P1-P2, no further information
'6A'	'87'	Lc inconsistent with P1-P2
'6D'	'00'	Instruction not allowed
'6E'	'00'	Class not allowed
'91'	'01'	CEP application is not activated[5]
'91'	'06'	CEP application has been deactivated[6]

8.5 Transaction preparation

Before CEP transactions are initiated, a common set of commands to the CEP card which reset the CEP card and select the application must be performed. This processing is only required once for a session with a specific CEP card. For example, if a cardholder performs a currency exchange followed by a load, the processing in this section is only done once, before the currency exchange transaction.

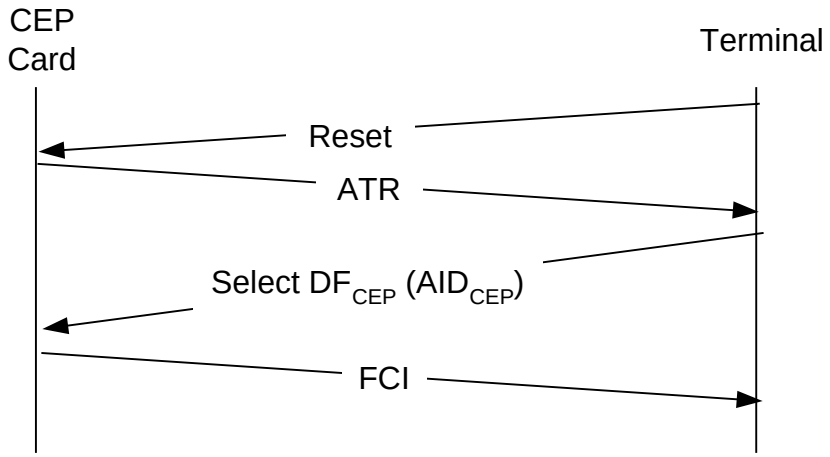
[5] The CEPS application must be activated by the card issuer before the application can be used. This is usually done during the personalization process.

[6] An activated CEPS application can be deactivated by the card issuer.

8.5.1 Message Flow

Figure 5 shows the message flow between the terminal (a load or POS device) and the CEP card prior to starting a CEP transaction.

Figure 5 - Message flow that precedes CEPS transactions



8.5.2 Reset

8.5.2.1 Once the CEP card is inserted into a load or POS device, a reset must be initiated. The Answer to Reset (ATR) is covered in reference 8, EMV Part 1.

8.5.3 Application Selection

8.5.3.1 Application selection must be performed as specified in reference 8. EMV. The variant of the Select command response that must be used is described in section 8.6.1. The response to the Select command described contains additional information not required by EMV.

8.6 ISO/IEC Commands

These commands are described in reference 4, ISO/IEC 7816-4 and also in reference 8, EMV.

8.6.1 Select

8.6.1.1 The Select command is coded according to EMV, reference 8.

8.6.1.2 The reply to the Select command consists of the File Control Information (FCI) as shown in Table 16, the status conditions in the response must conform to reference 8, EMV Part II.

Table 16 - Response to Select Command

Tag	Description	Length	M/O
'6F'	Indicates FCI template	var	M
'84'	DF Name	5-16	M
'A5'	FCI Proprietary template	var	M
'50'	Application Label	1-16	O
'87'	Application priority	1	O
'5F2D'	Language Preference	2-8	O
'9F11'	Issuer Code Table Index	1	O
'9F12'	Application Preferred Name	1-16	O
'BF0C'	Issuer discretionary data	var	M
'C9'	Application Profile (AP_{CEP})	2	M
'DF10'	Application Data Locator (ADL)	var	M
'9F08'	Application version number (AVN)	2	M
'5F28'	Country code of the card issuer ($CNTRY_{ISS}$).	2	M
'C0'	Domain of the card issuer (DOM_{ISS}) – if not present, '00' should be used as DOM_{ISS}.	1	O
'8F'	Version of the CA public key used to authenticate the card ($VKP_{CA,ISS}$) - mandatory for cards that support off-line enciphered PIN.	1	O
SW1 SW2	Status bytes	2	M

8.6.1.3 If a CEP card is able to process proprietary (non CEPS) data, there will be implementation specific data returned in the FCI that indicates to the POS or load device that this CEPS card processes proprietary data. The specific implementation must also be specified in the FCI data. The tag(s) used to identify the use of proprietary data by a specific implementation must follow the tag assignment conventions specified in reference 8, EMV.

8.6.1.4 A POS or load device must not send proprietary data to a CEP card unless the FCI information from the CEP card indicates that the device and the CEP card share a common implementation. If a CEP card receives proprietary data in error, the CEP card must respond with an SW1SW2 of '6A80' (Incorrect parameters in the data field).

8.6.1.5 A CEP card must not send proprietary data to a POS or load device unless the device has sent the card proprietary data indicating that the device and the CEP card share a common application or is responding to an inquiry command. If a POS or load device receives proprietary data in error the transaction must be terminated.

8.6.2 Read Record

8.6.2.1 The CEP card must support the Read Record command. This command is used by devices to read non-secret data that resides in record files (fixed or variable). The form of the Read Record command to be used with the CEP application must identify the file from which the data is to be read using the Short File Identifier (SFI), and must specify the precise record number to be read without reliance upon the current record pointer.

8.6.2.2 The CEP card must not allow the Read Record to be used against files containing secret data.

8.6.2.3 The Read Record command must be coded as shown in Table 17. The format of the response is shown in Table 18.

Table 17 - Read Record Command format

Field	Content	Length
CLA	'00'	1
INS	'B2'	1
P1	Record Number	1
P2	SFI || 100b	1
Le	'00'	1

Table 18 - Read Record Response Format

Name	Description	Length
TAG	'70' - data is TLV encoded	1
LEN_{DATA}	Length of data	1-2
Data	Record read from file	LEN_{DATA}
SW1 SW2	Status bytes	2

8.6.2.4 The CEP card must support use of the Read Record command for reading the public key certificates (PKC). The Application Data Locator (ADL) specifies the location of these records. The format of the records is in *Table 3 - Certificate Record with No Remainder*, *Table 4- Format of Record with Both a Certificate and a Remainder*, and *Table 5 - Public Key Certificate in Two Records*. The status conditions are in Table 19.

Table 19 - Status Conditions for Read Record command

SW1	SW2	Meaning
'64'	'00'	State of non-volatile memory unchanged
'62'	'81'	Part of returned data may be corrupted.
'67'	'00'	Wrong length (Le field not present)
'69'	'81'	Command incompatible with file organization
'6A'	'81'	Function not supported
'6A'	'82'	File not found
'6A'	'83'	Record not found

8.7 Non-transaction Commands

This section describes non-ISO/IEC commands that do not relate to a specific transaction type. These commands must be supported by all CEP cards.

8.7.1 CEP Inquiry - Slot Information

The CEP Inquiry command supports the reading of slot data.

8.7.1.1 To read the slot information for a specific currency, the command must be coded as described in Table 20. The format of the response is given in Table 21. Status conditions for this form of the command are given in Table 22.

8.7.1.2 When processing a CEP Inquiry command for a specific currency, the CEP card searches all slots in any order to locate the slot containing the currency specified in the command. Data from the slot is returned in the response. If there is no slot in the CEP card containing the currency, the CEP card returns only status information indicating whether or not an empty slot is available for assignment to the currency specified.

Note: This information may be used by a load device to determine actions to be taken during a load or

currency exchange transaction.

Table 20 - CEP Inquiry Command Format- Specific Currency

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1 P2	The arithmetic sum of '8000' + Currency code (CURRC)[7]	2
Le	'00'	1

Table 21 - Format of Slot Information

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$CURR_{CEP}$	Currency	3
BAL_{CEP}	Balance	4
$BALmax_{CEP}$	Maximum balance	4
$CALPHA_{CEP}$	Alphabetic currency code	3
PDATA	Proprietary implementation data	var

Table 22 - Status Conditions for CEP Inquiry- Specific Currency

SW1	SW2	Meaning
'94'	'09'	Currency not found; slot available
'94'	'0A'	Currency not found; no slot available

8.7.1.3 Table 23 describes how the CEP Inquiry command must be coded for obtaining slot information when the currency is not known.

[7] For example, if the currency is '0840', the value of P1P2 would be '8000' plus '0840' or '8840'.

The status conditions for this form of the command are in Table 24. The format of the information retrieved from a slot is given in Table 21.

8.7.1.4 To see the information from all slots, a device issues the command first with P2= ‘00’, then repeats the command with P2= ‘01’ until the CEP card returns status ‘6A83’. At this point, the CEP card has returned the information from all slots.

8.7.1.5 If P2 = ‘00’, the CEP card returns the slot information from the “first slot”. The meaning of “first slot” is up to the CEP card- it need not be the first physical slot nor have any particular sequence in the CEP card.

8.7.1.6 The CEP card must reject the command if P2 = ‘01’ and the command was not preceded by another CEP Inquiry command coded according to Table 23. The SW1SW2 for this condition is ‘9580’.

8.7.1.7 When P2 = ‘01’, the CEP card must return information from a slot different from any slot returned by a previous command. That is, when the device issues a command with P2 = ‘00’ followed by a succession of commands with P2 = ‘01’, the CEP card must return information from each slot exactly once until all slot information has been returned. After the last slot information has been returned, the CEP card must respond to the next command with only status information ‘6A83’.

8.7.1.8 The slots may be returned by the CEP card in any order.

8.7.1.9 If any command not conforming to Table 23 is received, the command sequence is broken and must be restarted. That is, the next command coded according to Table 23 must have P2 = ‘00’, and the “first slot” data will be returned in the response. The SW1SW2 for this condition is ‘9580’.

Table 23 - CEP Inquiry Command Format –Any Currency

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1	'10'	1
P2	'00' First slot '01' Next slot	1
Le	'00'	1

Table 24 - Status Conditions for CEP Inquiry - Any Currency or Transaction Log

SW1	SW2	Meaning
'6A'	'83'	Slot not found or all data returned
'95'	'80'	Command out of sequence

8.7.2 CEP Inquiry - Reference Currency

In the case of a load for a new currency in a CEP card, the load device may wish to display some guidance to the cardholder as to the maximum amount that the card issuer will permit to be loaded. This is optional on the part of the load device, but might reduce the probability of rejection of the load transaction by the card issuer.

To allow the load device to calculate an approximate maximum balance for the new currency, the card issuer may insert into the CEP card the currency code of a "reference currency" and the maximum balance, expressed in terms of the reference currency, allowed for loading a new currency. The load device may retrieve the reference currency information using the variation of the CEP Inquiry command described in this section. If the reference currency is recognized by the load device, it converts the reference currency value into the load currency using conversion rates provided by the load acquirer, and display the result to the cardholder as an approximate maximum load amount.

The intent for the displayed amount is for guidance only. It does not represent the precise amount that the card issuer will permit to be loaded, and the load device should not limit the cardholder to the displayed amount.

The choice of the reference currency is at the discretion of the card issuer, but a common currency should be selected to maximize the likelihood that load devices worldwide will recognize it.

The use of this feature is optional on the part of both the load acquirer and the card issuer.

The format of the CEP Inquiry command to retrieve the reference currency information is given in Table 25.

Table 25 - CEP Inquiry Command to Retrieve Reference Currency

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1	'11'	1
P2	'00'	1
Le	'00'	1

The data in the response when the CEP card supports a reference currency must be coded as described in Table 26. Up to three reference currencies and their maximum balance may be returned, If no reference currency is supported, the SW1SW2 in the response must be '9401'. If no reference currency is supported, proprietary data (PDATA) must not be included in the response.

Table 26 - Reference Currency Information

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$REFCURR_{CEP}$	Currency code of the first reference currency	3
$REFBALmax_{CEP}$	Approximate maximum balance permitted for a new currency, expressed in terms of the first reference currency	4
$REFCURR_{CEP}$	Currency code of the second reference currency (optional)	3
$REFBALmax_{CEP}$	Approximate maximum balance permitted for a new currency, expressed in terms of the second reference currency (must be present if the second reference currency is present)	4
$REFCURR_{CEP}$	Currency code of the third reference currency (optional)	3
$REFBALmax_{CEP}$	Approximate maximum balance permitted for a new currency, expressed in terms of the third reference currency (must be present if the third reference currency is present)	4
PDATA	Proprietary implementation data	var

Status conditions for a rejected CEP Inquiry for the reference currency are given in Table 27.

Table 27 - Status Conditions for CEP Inquiry for a Reference Currency

SW1	SW2	Meaning
'94'	'01'	Reference Currency not supported

8.7.3 CEP Inquiry - Transaction Logs

The CEP Inquiry command can be used to review the contents of the CEP card transaction logs. Different data is logged for different transaction types. The status conditions for all variants of the command are listed in *Table 24 - Status Conditions for CEP Inquiry*. The CEP card may return more data than is listed in Table 29, Table 31, or Table 33. The device should ignore this additional data.

If a non CEP application shares a transaction log with a CEP application, then some of the fields in the response to these commands may be zeros for entries created by the non CEP application.

8.7.3.1 The setting of P2 for all variants of the command must be as described below:

- To see the information from all transactions, a device issues the command first with P2= '00', then repeats the command with P2= '01' until the CEP card returns status '6A83'. At this point, the CEP card has returned the information from all transactions.

- The CEP card must reject the command if P2 = '01' and the command was not preceded by another CEP Inquiry command for the same transaction type. SW1SW2 must be set to '9580' if this occurs.

8.7.3.2 To read transaction information for a Load transaction, the CEP Inquiry command is coded as shown in Table 28. The format of the information retrieved for a Load transaction is given in Table 29. The data returned in the response to this command may include unload transactions.

Table 28 - CEP Inquiry Command Format – Load Transaction

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1	'01'	1
P2	'00' - Most recent transaction '01' - Preceding transaction	1
Le	'00'	1

Table 29 - Format of Log Information for Load Transactions

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
TI_{CEP}	Transaction type	1
$DTHR_{LDA}$	Transaction date and time	5
$CURR_{CEP}$	Currency	3
ID_{LACQ}	Acquirer ID	4
ID_{LDA}	Load device identifier	6
M_{LDA}	Transaction amount	4
NT_{CEP}	Transaction number	2
BAL_{CEP}	Balance of the slot after completion	4
$BALmax_{CEP}$	Maximum balance of slot after transaction	4
CC_{TRX}	Completion code of the transaction	2
PDATA	Proprietary implementation data	var

8.7.3.3 To read transaction information for a currency exchange transaction, the CEP Inquiry command is coded as shown in Table 30. The format of the information retrieved for a currency exchange transaction is given in Table 31.

Table 30 - CEP Inquiry command format – Currency Exchange Transaction

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1	'04'	1
P2	'00' - Most recent transaction '01' - Preceding transaction	1
Le	'00'	1

Table 31 - Format of Currency Exchange Transaction Log Information

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
TI_{CEP}	Transaction type	1
$DTHR_{LDA}$	Transaction date and time	5
$CURR_{SOURCE}$	Currency	3
ID_{LACQ}	Acquirer ID	4
ID_{LDA}	Load device identifier	6
M_{LDA}	Transaction amount (in source currency)	4
$CURR_{TARGET}$	Target currency	3
NT_{CEP}	Transaction number	2
$BAL_{TARGET,OLD}$	Target slot balance before transaction	4
$BAL_{SOURCE,NEW}$	Source slot balance after transaction	4
$BAL_{TARGET,NEW}$	Balance of the target slot after completion	4
$BALmax_{TARGET}$	Maximum balance of slot after transaction	4
CC_{TRX}	Completion code of the transaction	2
PDATA	Proprietary implementation data	var

8.7.3.4 To read transaction information for a purchase or cancel last purchase transaction, the CEP Inquiry command is coded as shown in Table 32. The format of the information retrieved for a purchase or a cancel last purchase transaction is given in Table 33.

Table 32 - CEP Inquiry Command Format – Purchase or Cancel Last Purchase Transaction

Field	Content	Length
CLA	'90'	1
INS	'5C'	1
P1	'02' - Purchase and Cancel last Purchase	1
P2	'00' - Last transaction '01' - Preceding transaction	1
Le	'00'	1

Table 33 - Format of Log Information for a Purchase or a Cancel Last Purchase Transaction

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
TI_{CEP}	Transaction type	1
$DTHR_{PDA}$	Transaction date and time	5
$CURR_{PDA}$	Currency	3
AM_{CEP}	Authentication method - zero for Cancel Last Purchase	1
NT_{CEP}	Transaction number	2
RID_{PSAM}	RID used by the PSAM creator	5
$ID_{PSAMCREATOR}$	Identifier of the PSAM creator	4
ID_{PSAM}	Identifier of the PSAM	4
ID_{ACQ}	Acquirer ID	4
NT_{PSAM}	Transaction number from PSAM	4
$MTOT_{CEP}$	Transaction amount - equal to M_{PDA} for cancel last purchase and single step purchases	4
M_{PDA}	Amount of the last step	4
BAL_{CEP}	Balance of the slot after completion	4

CC_{CEP}	Completion code	2
LOC_{PDA}	The location of the POS device - may be zero	6
$CNTRY_{PDA}$	Country of the POS device	2
DOM_{PDA}	Domain of the POS device	1
PDATA	Proprietary implementation data	var

8.7.4 Implementation Specific Inquiries

8.7.4.1 Specific implementations may add variants of the CEP Inquiry command by using settings of P1 with values of '2x'.

8.7.5 Get Previous Signature

8.7.5.1 The Get Previous Signature command must be coded according to Table 34. The response to a successful Get Previous Signature is the same as the response to the original transaction (see *Table 55 - Debit for Purchase and Subsequent Debit Response Format*, *Table 86 - Credit for Load Response Format* and *Table 97 - Currency Exchange Response Format*). If the command is unsuccessful, only SW1 SW2 is returned. The status conditions are listed in Table 35.

8.7.5.2 The Get Previous Signature command must only be used to retrieve previously created signatures. It must not be used to generate new signatures.

Table 34 - Coding of Get Previous Signature

Field	Content	Length
CLA	'90'	1
INS	'5A'	1
P1	'00'	1
P2	'01' - Purchase transaction '02' - Load or Currency Exchange transaction	1
L_C	Length of command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
NT_{CEP}	Transaction number of the desired MAC	2
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 35 - Status Conditions for Get Previous Signature

SW1	SW2	Condition
'94'	'04'	Value out of range (signature not available)
'94'	'07'	P2 conflicts with type of transaction

8.7.5.3 The CEP card must support the Get Previous Signature command for at least the last purchase, load or currency exchange transaction.

8.7.5.4 If P2 conflicts with the type of transaction corresponding to NT_{CEP}, the CEP card must reject the command with SW1 SW2 = '9407'.

8.7.5.5 If the value of NT in the command is not equal to a transaction with a signature available, the CEP card must not return any signature and must set SW1 SW2 = '9404'.

8.7.5.6 The CEP card must not return a signature for a purchase transaction that completed with an error, or a command that did not complete (that is, the balance of the slot

was not altered). In this case, the appropriate value for SW1 SW2 is ‘9404’.

8.7.5.7 Once a signature is made available for the Get Previous Signature command, it must remain available at least until the operational phase of the next transaction has begun, that is, the signature must be available until the next Credit for Load, Currency Exchange, Debit for Purchase, or Credit for Cancellation command has been received. If the signature is no longer available, the appropriate value for SW1 SW2 is ‘9404’.

8.7.5.8 If the value of NT in the command represents a load transaction in which R_{LSAM} was included in the Credit for Load command, P1 was set to ‘01’, P2 was set to ‘00’ and the command did not complete successfully (a successful completion will result in an SW1SW2 of ‘9000’ with the first byte of CC_{TRX} b8 = 1) the CEP card must return both S_3 and R_{CEP}.

8.7.5.9 If the value of NT in the command represents a load transaction that did not complete successfully, no signature(s) would have been generated and none will be returned in the response. In this case, the appropriate value for SW1 SW2 is ‘9404’.

8.7.5.10 If the value of NT in the command represents a currency exchange transaction, the CEP card must not return any signature other than S_3.

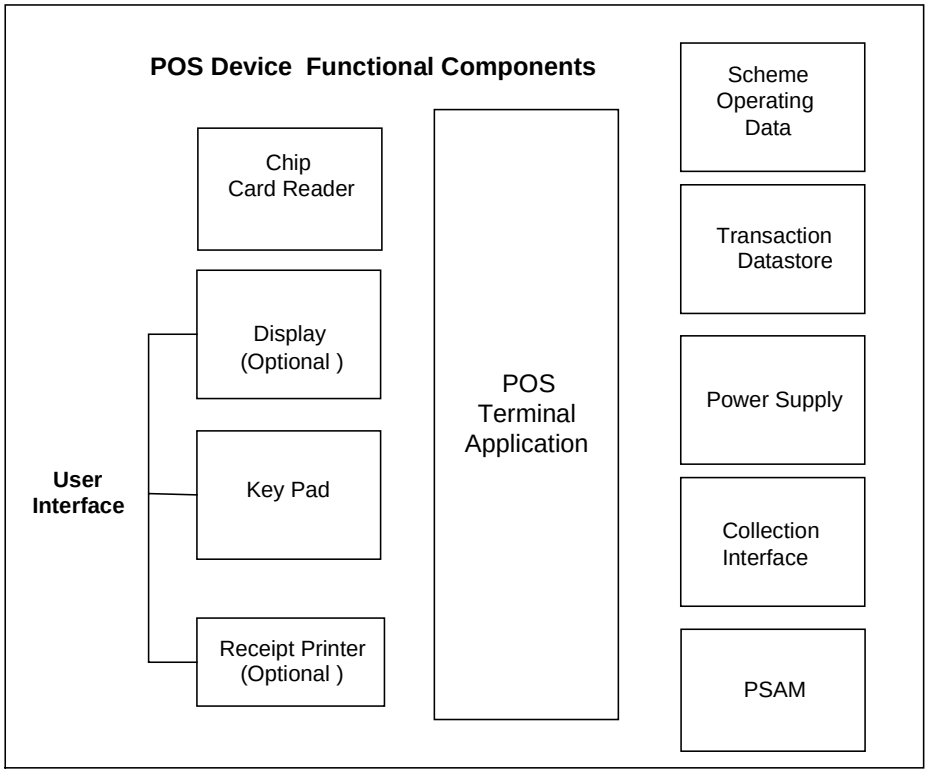
8.7.5.11 If the value of NT in the command represents a currency exchange transaction where no signature was generated, none will be returned in the response. In this case, the appropriate value for SW1 SW2 is ‘9404’.

9. POS Device Characteristics

9.1 Overview of a POS Device

Figure 6 illustrates the functional components of a CEP POS device.

Figure 6 - The POS Device



POS devices may operate in both attended and unattended environments. In an attended environment, a third party, for example, a clerk at a cash register in a store, enters data for the CEP transaction. In an unattended environment, for example, a vending machine, or a home computer, the CEP transaction is automated for the cardholder.

The POS device has a collection interface to the merchant acquirer using agreed upon message formats and communications protocols. The minimum data transmitted is included in these specifications.

9.2 Requirements

9.2.1 Scheme Specific Data

9.2.1.1 POS devices that follow these specifications are able to support the acceptance, by the merchant, of cards from multiple CEP schemes. However, business relationships between the merchant, the merchant acquirer, and the particular scheme provider determine whether a particular POS device accepts a scheme's CEP cards.

9.2.1.2 Each POS device must maintain a list of the AIDs that it supports.

A POS device that supports multiple AIDs must have the ability to select an application by comparing the set of AIDs supported in the device, and the set of AIDs present on the CEP card. In some cases interaction with the cardholder may be required in making the final decision on which application to select. The process of application selection must follow reference 8, EMV.

9.2.1.3 The POS device must contain CEPS operating data necessary for each scheme accepted at the device. The CEPS operating data for a scheme is shown in *Table 36 - CEPS Operating Data for a Scheme.*

9.2.2 Compliance with Standards

9.2.2.1 The POS device must comply with the requirements stated in these specifications. Additionally, the terminal standards in reference 8, EMV and any country or local governing standards must be complied with. If a country or local standard is more stringent than, or conflicts with, requirements in these specifications, then the country or local standard overrides any of these requirements. Additional standards include:

- Electromagnetic standards.
- Country-specific electrical and modem standards.
- Procedures for cardholder interface screens, buttons,

and keyboards.

9.2.3 Card Acceptance

9.2.3.1 Device hardware and software must be capable of interacting with the CEP applications described in this document.

9.2.4 Card Reader

9.2.4.1 The POS device must have an integrated circuit card (ICC) reader that is compatible with reference 8, EMV Part 1. The card reader must support both T=1 and T=0 protocols. When T=1 is used, the NAD address sent to the CEP card must be set to zero.

9.2.4.2 The ICC reader must let cardholders retrieve their cards either manually or automatically at the completion or termination of a purchase or a cancel last purchase transaction.

9.2.4.3 In environments where the card is accessible to the consumer during a transaction, the POS device must be capable of determining that a card has been removed before the completion of the transaction and terminate processing if this occurs.

9.2.4.4 The POS device may secure the CEP card in the reader to reduce the likelihood of the card being accidentally removed or moved around during the transaction.

9.2.4.5 The POS device should endeavor to maximize the data transmission rate between it and the CEP card to the highest value mutually supported. The process to determine this rate must follow the process described in reference 8, EMV.

9.2.5 Display and Cardholder Interface Design

9.2.5.1 A POS device may support language selection. If it supports language selection, the processing described in reference 8, EMV must be followed.

9.2.5.2 The following information should be provided to the

cardholder:

- Visual or audible status confirmation of the transaction, for example, completed or canceled.

- Exception messages.

If the application profile (AP_{CEP} - obtained when the application is selected) allows a spontaneous display, the following information should be provided to the cardholder automatically:

- CEP slot balance before the transaction.

- CEP slot balance after the transaction.

If the application profile (AP_{CEP}) does not allow a spontaneous display, the above information should be provided to the cardholder upon request.

Other slot data may be provided to the cardholder, but this is not required. The POS device should also display the currency being used in the transaction. This display does not need to be an electronic display. If a POS device supports multiple currencies, the currency being used for the transaction must be displayed. If a currency identifier is displayed, how that currency is displayed is at the discretion of the merchant acquirer. Use of the alphabetic currency code ($CALPHA_{CEP}$) in the slot of the CEP card is not required.

9.2.5.3 The POS device must permit termination of the current transaction, allowing removal of the card, up until the time the cardholder accepts the transaction amount.

9.2.6 Split Transaction Processing

9.2.6.1 A POS device may permit the cardholder to complete a CEP purchase transaction with a combination of two or more CEP cards, or a CEP card and an additional form of payment such as cash or a traditional bank card (i.e. a debit or credit card). The implementation of this feature is at the discretion of the merchant.

9.2.7 Power Failure

9.2.7.1 If the CEP card is fully contained within the POS device, the device must eject the card in case of a power failure.

9.2.8 Data Store Requirements

9.2.8.1 Each POS device must maintain a data store for uncollected transactions. The timing of the deletion of a collected batch is outside of the scope of this document.

9.2.8.2 The POS device must log transactions regardless of completion status. The minimum data elements to be logged are described in section 10.1.7 and 10.2.2.

9.2.8.3 Each POS device must maintain a data store containing, at a minimum, the scheme operating data listed in Table 36. Unless specifically listed as being stored in the PSAM, the location of this data is at the discretion of the POS device designer.

Table 36 - CEPS Operating Data for a Scheme

Field	Contents	Length
RID_{CEP} or AID_{CEP}	The identifier of the scheme owning the CEP card performing a transaction **-** If this field is the RID of the scheme, a list of valid AIDs must be included - **the RID must be in the PSAM**	5-16
ID_{ACQ}	Acquirer ID	4
	Data for each currency supported by the POS device. see Table 37	var
	Public key data for CEP card authentication - see Table 38	var
	Public key data for PSAM authentication - see Table 39	var
	Optional Blocking List Entries - see Table 40	var
	Issuer Certificate Revocation List Entries - see Table 41	var
	Optional Aggregation Parameters -see Table 42	var

Table 37 - Data For Each Currency Supported by the POS Device

Field	Contents	Length
CURR	A currency supported by the POS device	3
$MTOTmax_{CURR}$	For each currency supported by the POS device, the maximum value of a purchase transaction (the total of all increments).	4

Table 38 - Data For Each Public Key that the Scheme Supports for CEP Card Authentication

Field	Contents	Length
$VKP_{CA,ISS}$	The version number of the CA public key for CEP card authentication	1
$LPKM_{CA,ISS}$	Length of the CA public key modulus for CEP card authentication	1
$PKM_{CA,ISS}$	The CA public key modulus for CEP card authentication - **must be in the PSAM**	$LPKM_{CA,ISS}$
$ALGP_{CA,ISS}$	Algorithm to be used with this key	1

Table 39 - Data For Each Public Key that the Scheme Supports for PSAM Authentication

Field	Contents	Length
$VKP_{CA,ACQ}$	The version number of the CA public key for PSAM authentication	1
$PKC_{REG,ACQ}$ or PKC_{ACQ}	A certificate created using the scheme private key identified by $VKP_{CA,ACQ}$. This may be a regional certificate or an acquirer certificate	$LPKM_{CA,ACQ}$
$PKR_{REG,ACQ}$ or PKR_{ACQ}	If required, the public key remainder, which is the portion of the regional or acquirer public key that is not contained in the public key certificate	var
$CSN_{REG,ACQ}$ or CSN_{ACQ}	Regional or acquirer certificate serial number	3

Table 40 - Data For Each Entry in the Blocking List for the Scheme - Optional

Field	Contents	Length
$ID_{ISS,CEP}$	Issuer Identification on the CEP card range to be blocked	4
ID_{CEP}	Identifier of the first card of the range to be blocked	6
ID_{CEP}	Identifier of the last card of the range to be blocked	6

Table 41 - Data For Each Entry in the Certificate Revocation List

Field	Contents	Length
ID_{ISS}	Issuer identification - zeros if the certificate revoked is a regional certificate	4
$ID_{REG,ISS}$	Identifier of the region - zeros if regional certificate is not used	4
$CSN_{REG,ISS}$ or CSN_{ISS}	Regional or Issuer Certificate Serial Number	3
$VKP_{CA,ISS}$	CA Public Key version number	1
$VKP_{REG,ISS}$	Regional public key version number - only required if both the identifier of the region and the id of the issuer are present	1

Table 42 - Data For Each Scheme that Allows Aggregation at the POS Device

Field	Contents	Length
NT_{PCT}	Detail Transaction Percentage. The percentage of detail transaction that a scheme requires from a POS device certified to perform aggregation. For example, if this parameter is set to 10, 90% of transactions may be aggregated.	1

9.2.8.4 In addition to scheme data and logged transactions, each POS device must also contain the data elements listed in Table 44 and Table 45. If the merchant acquirer is in a region that requires a regional certificate, the data in Table 43 must also be in the POS device.

Table 43- Optional Data to Support Acquirer Regional Certificates

Field	Contents	Length
$ID_{REG,ACQ}$	The identifier of the region, if there is a regional certificate. Must match the region identifier in the regional certificate	4
PKC_{ACQ}	An optional acquirer certificate for the PSAM created using the regional private key, (this field only exists if there is a $PKC_{REG,ACQ}$), otherwise the PKC_{ACQ} is in the scheme specific data (see Table 39)	$LPKM_{REG,ACQ}$
PKR_{ACQ}	If required, the public key remainder, which is the portion of the acquirer public key that is not contained in the public key certificate, (this field only exists if there is a $PKC_{REG,ACQ}$), otherwise the PKR_{ACQ} is in the scheme specific data (see Table 39)	var
CSN_{ACQ}	An optional acquirer certificate serial number, (this field only exists if there is a $PKC_{REG,ACQ}$), otherwise the CSN_{ACQ} is in the scheme specific data (see Table 39)	3

Table 44 - Data in the POS Device that may be unsecured

Field	Contents	Length
LOC_{PDA}	Location description	6
PKC_{PSAM}	The PSAM certificate signed by the private key of the merchant acquirer key pair associated with the public key in the acquirer certificates	$LPKM_{ACQ}$
PKR_{PSAM}	The rightmost bytes of the PSAM public key modulus. Only required if the entire PSAM public key modulus will not fit in the PSAM certificate	var
$DTHR_{PDA}$	Date and time transaction is initiated. If the POS device does not have a clock, the portions of this field which cannot be stated definitively should be set to zeros	5
$CNTRY_{PDA}$	The country of the POS device	2
DOM_{PDA}	The domain of the POS device – if not applicable, must be set to '00'	1

9.2.8.5 Some of the scheme data listed in Table 36 must be stored in the PSAM. This data and any other data that is stored in the PSAM must be protected by a MAC when being updated. Some data elements that must be in the PSAM must not be updated after the PSAM is personalized. These data elements are listed in Table 45.

Table 45 - Data in the PSAM that must not be externally updated

Field	Contents	Length
RID_{PSAM}	The RID used by the creator of the PSAM	5
$ID_{PSAMCREATOR}$	The ID assigned by the owner of the RID_{PSAM} to the creator of the PSAM	4
ID_{PSAM}	PSAM identifier	4
NT_{PSAM}	PSAM transaction number	4
SK_{PSAM}	PSAM private key	var

9.2.8.6 The NT_{PSAM} must start at one and must not roll-over. The NT_{PSAM} is incremented by the PSAM by one for each transaction the PSAM processes. Once the NT_{PSAM} has reached its maximum value, the PSAM must become inoperable.

9.2.8.7 The SK_{PSAM} is secret data and must not be readable except by the PSAM.

9.2.9 Batch Management

9.2.9.1 The POS device must maintain POS transactions within collection batches. A collection batch is a set of POS transactions, and their associated batch summary totals, that have been secured by a single PSAM and represent a range of PSAM transaction numbers (NT_{PSAM}). A single physical PSAM may be treated by the POS device as one or more logical PSAMs. This will allow multiple active batches (for example, with different currencies) to be in the POS device at one time.

9.2.9.2 A PSAM may process multiple transactions at one time. However, each transaction processed by a PSAM must have a unique combination of RID_{PSAM}, $ID_{PSAMCREATOR}$, ID_{PSAM} and NT_{PSAM}. The PSAM can request that a batch of transactions be closed at any time. When the batch is closed, it can include or exclude any transactions in progress. However, if a transaction in progress is a cancel last purchase, it must be in the same batch as the purchase transaction. If the transactions in

progress are not added to the current batch, the PSAM will add them to the next batch. The POS device must not allow collection of a batch until the PSAM has closed it.

9.2.9.3 A logical PSAM may contain both an active batch and closed batches. A closed batch is a batch that transactions are no longer being added to.

9.2.9.4 A logical PSAM must maintain no more than one active batch at a time. New transactions must not be added to a closed batch. When a transaction is added to the active batch, the associated batch summary totals must also be updated.

9.2.9.5 The active batch must be closed by the POS device before the batch is collected for transmission to the merchant acquirer. The POS device may also close the active batch based on external events such as operator request or time of day.

9.2.9.6 A closed batch must not be re-opened, and new transactions must not be added to a closed batch.

9.2.9.7 The POS device should not delete closed batches until an acknowledgment has been received from the collecting device or merchant acquirer.

9.2.9.8 A batch may contain detail transaction records. It must contain a batch summary and, if the POS device has been certified to perform aggregation, the batch may also contain aggregation records.

9.2.10 PSAM Hardware and Software Requirements

The PSAM must be a security module as defined below. In addition, the PSAM must perform the cryptographic processing and transaction control as specified in this document. A software evaluation must be performed to guarantee the PSAM functions as described in this document.

Because of the variety of possible POS environments and devices, the requirements do not specify where the PSAM must reside. Also, while a PSAM may be an ICC, the requirements allow for other implementations.

9.2.10.1 A PSAM must be a physically and logically protected hardware device that provides a secure set of cryptographic services.

9.2.10.2 All cryptographic functions for POS transaction processing must be performed in a PSAM.

9.2.10.3 All clear text keys must be physically protected against disclosure and unauthorized modification within a PSAM.

9.2.10.4 A PSAM must be tamper resistant. The intent of the tamper resistance is to protect designated information from unauthorized disclosure, use or modification by employing passive barriers. The PSAM must have a negligible probability of being successfully penetrated in such a way as to disclose all or part of any cryptographic material, keys, or other data. It must be protected by being tamper resistant to such a degree that its passive resistance is sufficient to make penetration infeasible both in its intended environment and when taken to a specialized facility with specialized equipment.

9.2.10.5 Controls must be in place to ensure that equipment is not re-installed after a suspicious alteration of a key in a PSAM has been detected until the PSAM has been inspected and a reasonable degree of assurance has been reached that the PSAM has not been subject to unauthorized physical or functional modification.

9.2.10.6 PSAMs must be designed in such a way to prevent state of the art monitoring attacks, such as radiation tapping, covered channel analysis, etc. known at the time of certification.

9.2.10.7 Each PSAM must have a unique internal identifier composed of the combination of RID_{PSAM}, $ID_{PSAMCREATOR}$ and ID_{PSAM}. This internal identifier must not be changed after personalization.

9.2.10.8 Based on a combination of adequate control procedures during the production process and special features available through design, it must be ensured at initial key loading that a PSAM is authentic, corresponds to a

certified construction and is loaded with a certified program.

9.2.10.9 After a PSAM is created, subsequent down-loading of program updates must only take place after origin authentication.

10. POS Device Transaction Processing

10.1 Purchase Transaction

Purchase is an off-line transaction initiated by a POS device. The amount debited may be verified by the cardholder using a monitoring device or a POS or load device.

The POS device determines the currency to be used prior to the start of the transaction. This information is passed to the CEP card to allow the CEP card to select the slot to be used. If there is no slot in the CEP card for the specified currency, the transaction cannot be made and the CEP card must reject the command.

Purchase transactions require at least two commands: Initialize for Purchase and Debit for Purchase. The CEP card must reject any Debit for Purchase command that is not preceded by a successful Initialize for Purchase command.

In the case of an incremental purchase, a purchase transaction may have one or more Subsequent Debit commands. A purchase transaction may also have one Purchase Reversal command. The CEP card must reject any Subsequent Debit or Purchase Reversal command that is not preceded by a successful Debit for Purchase command or a successful Subsequent Debit command.

Both symmetric and asymmetric cryptography is used in performing a purchase transaction.

- The PSAM initially authenticates itself to the CEP card using the RSA asymmetric algorithm and certificate versions specified by the CEP card.

- The CEP card authenticates itself to the PSAM using a DES key provided by the PSAM. This DES key is sent to the CEP card signed by the private key of the PSAM and encrypted by the public key of the CEP card.

- For subsequent steps of the purchase, the PSAM uses the DES key that it sent to the CEP card to authenticate itself to the CEP

card.

- The CEP card also signs the transaction using a MAC based on a key provided by the card issuer. This MAC allows the card issuer to validate the data and CEP card used in the transaction. The contents of this symmetric MAC are determined by the card issuer. Its purpose is to validate all information seen by the CEP card and forwarded to the card issuer.

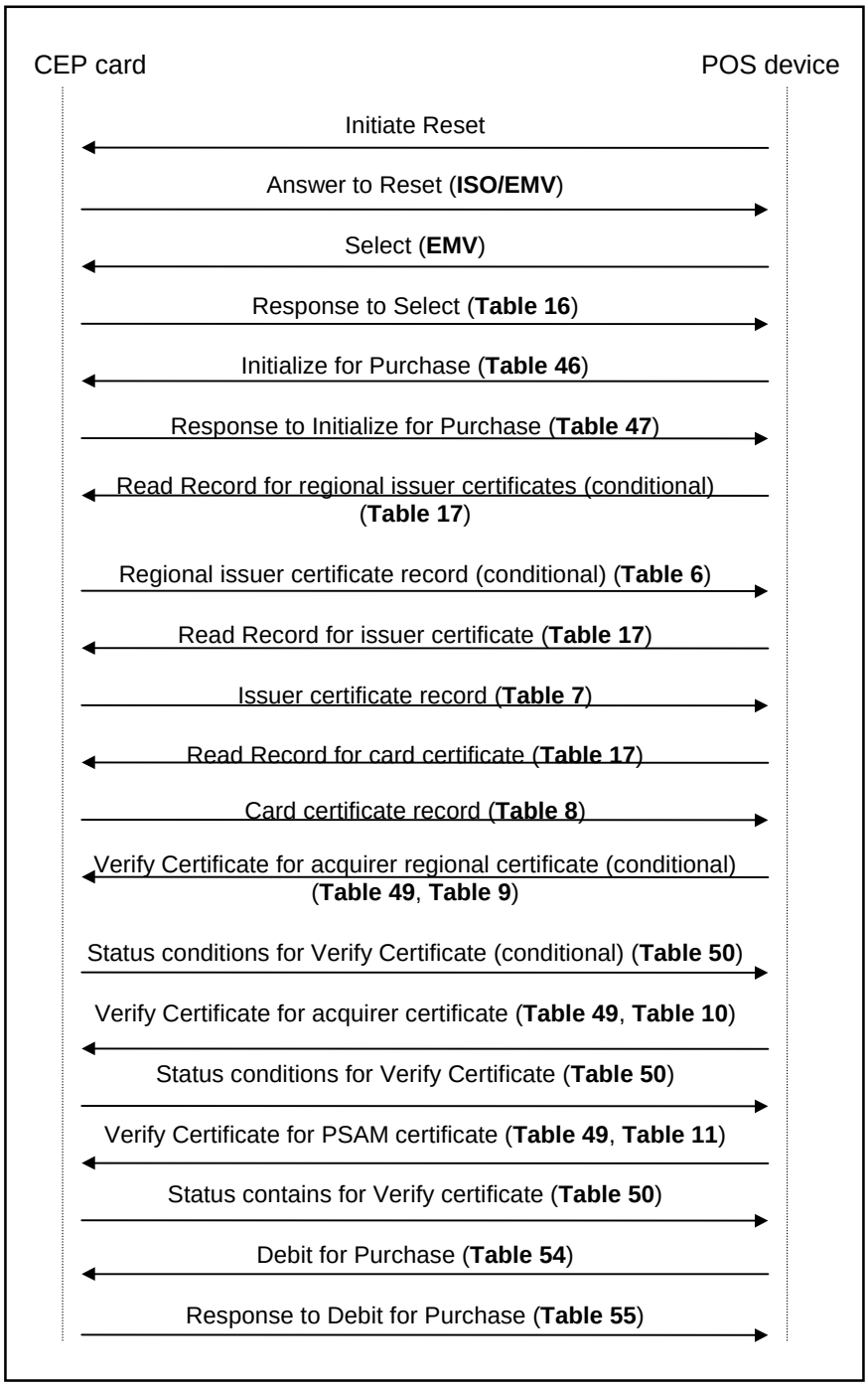
- The PSAM also signs the transaction using a symmetric key to allow the merchant acquirer to validate the data and the PSAM.

- Additional MACs may be created by the CEP depending on the options selected by the card issuer and the merchant acquirer.

At the completion of each successful Debit for Purchase, Subsequent Debit and Purchase Reversal command, the CEP card must update its internal transaction log. A single entry in the log should be made for each value of NT_{CEP}.

The flow in Figure 7 shows an interaction between the POS device and the CEP card for purchase processing. Other flows are possible as long as they meet the requirements in these specifications.

Figure 7 - Purchase Processing



10.1.1 Initiate Transaction

The initiate transaction process consists of:

- Application selection.
- Determination of the currency of the transaction.
- The Initialize for Purchase command.
- Checking the expiration date and, optionally, the card blocking list.

10.1.1.1 If the CEP card has not been reset after being inserted in the POS device or if the CEP application has not been selected, the processing described in section 8.5 must occur. The RID in the AID_{CEP} of the selected application identifies the scheme provider for this transaction.

10.1.1.2 The POS device must contain the data elements in *Table 36 - CEPS Operating Data for a Scheme*, *Table 44 - Data in the POS Device* and *Table 45 - Data in the PSAM* to support the purchase transaction. Additionally, the data in *Table 16 - Response to Select Command* is obtained during application selection.

10.1.1.3 The POS device must begin the purchase transaction with an Initialize for Purchase command. The format of this command is in Table 46. The format of the response is in Table 47. The status conditions are in Table 48.

The POS device must not send any proprietary data to the CEP card unless it has been determined that the CEP card and the POS device support the same proprietary implementation (see section 8.6.1).

Table 46- Initialize for Purchase Command Format

Field	Content	Length
CLA	'90'	1
INS	'50'	1
P1	'01'	1
P2	'00'	1
L_C	Command data length	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$DTHR_{PDA}$	Transaction date and time - if the POS device does not have a clock, any portion of this field which is not definitively known should be zeros	5
$CURR_{PDA}$	Currency	3
LOC_{PDA}	The location of the POS device	6
$CNTRY_{PDA}$	The country of the POS device	2
DOM_{PDA}	The domain of the POS device	1
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 47 - Initialize for Purchase Command Response

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
$ID_{ISS,CEP}$	Issuer identifier	4
ID_{CEP}	Card identifier	6
$DEXP_{CEP}$	Expiration date for transaction	3
$VKP_{CA,ISS,CEP}$	Version of the CA Public Key the PSAM must use for card authentication	1
$ID_{REG,ISS}$	Identifier of the issuer region - zeros if no region	4
$VKP_{REG,ISS}$	Version number of the region public key used to create the issuer certificate - zero if no regional certificate	1
$CSN_{ISS,CEP}$	Identifier of the Issuer's certificate contained in the card	3
$VKP_{CA,ACQ,CEP}$	Version of the CA Public Key the card must use for PSAM authentication	1
$ID_{REG,ACQ}$	Identifier of the acquirer region - zeros if no region	4
$CSN_{ACQ,CEP}$	Identifier of the Acquirer's certificate contained in the card (zero's if not present)	3
AM_{CEP}	Authentication method of the card	1
NT_{CEP}	Transaction Number of the card	2
BAL_{CEP}	Balance before purchase	4
L_{DD}	Length of discretionary data	1
DD_{CEP}	Discretionary data. The contents of this field are established by the card issuer. It is recommended that DD_{CEP} for purchase transactions includes $NT_{LASTLOAD}$ and $NT_{LASTCANCEL}$	0-16
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 48 - Status Conditions for Initialize for Purchase Command

SW1	SW2	Condition
'91'	'02'	CEP Transaction Number has reached its limit
'91'	'10'	CEP application has been locked
'94'	'01'	Currency error
'95'	'08'	Invalid balance (Balance greater than Max Balance)

10.1.1.4 If the response from the CEP card does not indicate a successful completion of the command, normal processing of the transaction must be stopped and exception processing followed.

10.1.1.5 The POS device should be able to provide the cardholder with the balance in the response from the CEP card. If the application profile (AP_{CEP}) indicates that no spontaneous display is permitted, the POS device must suppress providing the balance unless a balance is requested by the cardholder.

10.1.1.6 If the $DEXP_{CEP}$ indicates that the CEP application is no longer valid for purchase transactions, normal processing is stopped and exception processing is performed.

10.1.1.7 The POS device may verify that the card number ($ID_{ISS,CEP}$ and ID_{CEP}) is not in the blocking list for the scheme. If the card number has been blocked, normal processing of the transaction must be stopped and exception processing followed. The blocking list is described in *Table 40 - Data For Each Entry in the Blocking List for the Scheme.*

10.1.2 Recovery of the CEP Card Public Key

The recovery of the CEP card public key process consists of:

- Determination that the public key hierarchy in the CEP card can be processed by the PSAM.
- Use of the Read Record command to retrieve certificates from the CEP card.

- Verification of the certificates, including checking the certificate revocation list.

10.1.2.1 After receiving and validating the response to the Initialize for Purchase command, the POS device must verify that the version of the CA public key used to create the issuer or regional certificate ($VKP_{CA,ISS}$) in the response to the Initialize for Purchase command matches a version number of a $PK_{CA,ISS}$ in the PSAM for the scheme. If there is no match, the transaction is terminated.

10.1.2.2 If the data returned by the CEP card identifies an issuer public key for the scheme that is stored in the PSAM, it is not necessary to read the issuer certificate from the CEP card.

If the required issuer public key is not available[8], a Read Record command is issued to read the certificate record(s). The POS device must use the Application Data Locator (ADL) to find the SFI of the files on the CEP card containing the certificates to determine the number of certificates records to read. The format of the ADL is in the Data Dictionary, section 17. The format of the Read Record command and the response to the command are in section 8.6.2. The first certificate on a card may be an issuer certificate or a regional certificate may precede the issuer certificate. The format of the certificate records are described in section 6.

The PSAM must use the $ALGP_{CA,ISS}$ and the $PKM_{CA,ISS}$ specified by the $VKP_{CA,ISS}$ to verify the retrieved certificate and recover the highest level public key. If the format code of the recovered certificate is '02' the issuer public key has been recovered. If the format code of the recovered certificate is not '02', the POS device must use the Read Record command to read the next certificate record. If all records have been read and no certificate with a format code of '02' is recovered, normal processing of the transaction must be stopped

[8] The issuer public key may be stored in the PSAM, or the issuer certificate may be stored in the POS device and the issuer public key recovered from the issuer certificate using a key stored in the PSAM.

and exception processing followed.

10.1.2.3 After the issuer certificate has been recovered, the next certificate record, the card certificate record, must be obtained using the Read Record command. The format of the card certificate record is described in section 6. The PSAM uses the issuer public key (PK_{ISS}), and its algorithm code ($ALGP_{ISS}$) to verify the card certificate and recover the card public key.

10.1.2.4 The verification that is done to the certificates is described in section 6. If any certificate fails this verification, normal processing of the transaction must be stopped and exception processing followed.

10.1.3 Recovery of the PSAM Public Key

The recovery of the PSAM public key process consists of:

- Determination that a public key hierarchy in the PSAM can be processed by the CEP card.
- The Verify Certificate command for each certificate in the PSAM certificate hierarchy.

10.1.3.1 The following steps must be performed to allow the CEP card to recover the PSAM public key.

1. If the data in the response to the Initialize for Purchase command identifies an acquirer certificate for the scheme that is stored in the POS device or PSAM, the P2 value in the Verify Certificate command must be set to ‘02’ (verify using the cached public key) and processing must continue with step 4.

2. The highest level regional or acquirer certificate in the certificate hierarchy identified by the AID_{CEP} and the $VKP_{CA,ACQ}$ received in the response to the Initialize for Purchase command must be selected.

3. The P2 value in the Verify Certificate command must be set to ‘01’ (verify using the CA public key). The ID_{REG} must be set for regional certificates or the

$ID_{PSAMCREATOR}$ must be set for acquirer certificates. A Verify Certificate command with the certificate selected in step 2 must be sent to the CEP card. The format of the Verify Certificate command is in Table 49. The response to the command is only SW1 and SW2. The status conditions are in Table 50. If the Verify Certificate command is successful, the P2 value in the Verify Certificate command must be set to '03' (verify using the key recovered from the previous Verify Certificate command). If there is an unverified acquirer certificate in the hierarchy selected in step 2, send another Verify Certificate command to the card containing the next certificate in the hierarchy. The identifier in this Verify command will be the $ID_{PSAMCREATOR}$.

4. Send a Verify Certificate command containing the PSAM certificate to the CEP card. The identifier in this Verify Certificate command will be the ID_{PSAM}. If the command is successful, the CEP card has successfully recovered the PSAM public key. Note that P2 for the command was set in step 1 or step 3.

10.1.3.2 The verification that is done by the CEP card to the certificates is described in section 6. If any certificate fails this verification, normal processing of the transaction must be stopped and exception processing followed.

Table 49 - Verify Certificate Command Coding

Field	Content	Length
CLA	'90'	1
INS	'82'	1
P1	'01'	1
P2	Indicates which public key to use to verify the certificate being sent in the command '01' use the public key personalized in the card (i.e., the CA public key) '02' use the cached acquirer key '03' use the public key retrieved by execution of the previous Verify Certificate command.	1
Lc	Length	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
ID_{REG} or $ID_{PSAMCREATOR}$ or ID_{PSAM}	Identifier of the Region, PSAM creator or PSAM	4
PKC	Certificate	LPKM
PKR	Remainder	var
PDATA	Proprietary implementation data	var

Table 50 - Status Conditions for Verify Certificate Command

SW1	SW2	Condition
'63'	'00'	Authentication failed
'63'	'01'	Required key not present
'67'	'00'	Wrong length

10.1.4 Debit CEP Card

The Debit CEP card process consists of:

- Determination of the amount of the first (or only) increment of the transaction.
- Creation of a session key for the transaction and the PS_2 signature.
- The Debit for Purchase command, including verification of the PS_2 signature and creation and verification of the S_3 MAC.

10.1.4.1 TI must be constructed as a single step purchase.

10.1.4.2 The amount of the purchase (M_{PDA}) must be determined and must be confirmed by the cardholder. Inserting a card, pushing an accept button or selecting a product are examples of ways for the cardholder to confirm the amount. The amount of the purchase must not exceed the CEP card balance for the currency (BAL_{CEP}). The total amount of the purchase field ($MTOT_{PDA}$) must be set equal to zero. M_{PDA} for the initial increment of a purchase may be equal to zero. M_{PDA} must not be greater than $MTOTmax_{CURR}$. If the value is too large, normal processing of the transaction must be stopped and exception processing followed.

10.1.4.3 A 16 byte DES key must be created by the PSAM ($SESSKey_{PSAM}$). This key must be a derived key and the two halves of the key must not be equal. The algorithm used to generate $SESSKey_{PSAM}$ must be triple DES or at least as strong as triple DES. The minimum derivation data is NT_{PSAM}. NT_{PSAM} must be updated by the PSAM before the session key is generated. The $SESSKey_{PSAM}$ must be derived from a PSAM specific key.

10.1.4.4 If the POS device and the PSAM support intermediate POS device validation of the CEP card, the PSAM must generate an authentication token (AT), a 16 byte DES key. The fields L_{AT} and AT must be included in the digital signature (DS). The PSAM must send the AT to the POS device. The AT sent to the POS device may be

in the clear.

The method of generating ATs must comply with the requirement that knowledge of any number of ATs must not help compute any secret values stored in the PSAM.

10.1.4.5 If the POS device or the PSAM does not support intermediate POS device validation of the CEP card, the PSAM must set the L_{AT} in the digital signature (DS) to zero.

10.1.4.6 If the PSAM supports aggregation, the aggregated total ($MTOT_{AGG}$) for the card issuer and currency of this transaction must be incremented by the amount of the transaction (M_{PDA}). The number of aggregated transaction (NT_{AGG}) must be incremented by one. The fields $MTOT_{AGG}$, NT_{AGG} and ID_{BATCH} must be included in the digital signature (DS).

10.1.4.7 The PSAM must create a digital signature (DS) by signing the data in Table 52 with the PSAM private key.

10.1.4.8 The PS_2 signature must be created by the PSAM by encrypting the data elements in Table 51 with the CEP card public key.

Table 51 - Format of the Data Recovered from the PS_2

Field	Content/Source	Length
Pad field	'00' - not verified by the CEP card	1
DS	Digital signature contained in PS_2 - see Table 52	$LPKM_{PSAM}$
Padding	Random number generated by the PSAM, not checked by the CEP	$LPKM_{CEP}$ - $LPKM_{PSAM}$-1

Table 52 - Format of the Data Recovered from DS

Field	Content/Source	Length
Header	'6A'	1
Format code	'89'	1
ALGH	Code for the algorithm used to produce the hash ('01' for SHA-1)	1
Length	Length of the fields after this length field and prior to the Pad Pattern	1
M_{PDA}	Amount to be debited	4
$SESSKey_{PSAM}$	Session Key produced by PSAM for authentication purpose	16
L_{AT}	Length of Authentication Token (AT) - zero if no AT present	1
AT	Authentication Token	0 or 16
L_{AGGTOT}	Length of data related to Aggregated Total per Issuer ($AGGTOT_{ISS}$) - zero if $AGGTOT_{ISS}$ not present	1
$AGGTOT_{ISS}$	Aggregated total for the issuer - if present, consists of: $MTOT_{AGG}$ Aggregated total 4 bytes NT_{AGG} Number transactions aggregated 2 bytes ID_{BATCH} ID of POS batch 2 bytes	0 or 8
Pad Pattern	Successive bytes containing 'BB'	Length of $PKM_{PSAM} - 47 - L_{AT} - L_{AGGTOT}$
Hash Result	Hash of signed data, see Table 53	20
Trailer	'BC'	1

Table 53 - Contents of the DS Hash

			Origin of data for POS device generation of DS	Origin of data for CEP card verification of DS
Format code	'89'	1	known	Debit for Purchase
ALGH	Code for the algorithm used to produce the hash ('01' for SHA-1)	1	known	Debit for Purchase

			Origin of data for POS device generation of DS	Origin of data for CEP card verification of DS
Length	Length of the fields after this length field and prior to the Pad Pattern	1	known	Debit for Purchase
M_{PDA}	Amount to be debited	4	known	Debit for Purchase
$SESSKey_{PSAM}$	Session Key	16	known	Debit for Purchase
L_{AT}	Length of Authentication Token (AT) – zero if no AT present	1	known	Debit for Purchase
AT	Authentication Token	0 or 16	known	Debit for Purchase
L_{AGGTOT}	Length of data related to Aggregated Total per Issuer ($AGGTOT_{ISS}$) – zero if $AGGTOT_{ISS}$ not present	1	known	Debit for Purchase
$AGGTOT_{ISS}$	Aggregated Total per Issuer - if present, consists of:	0 or 8	known	Debit for Purchase
	$MTOT_{AGG}$ Aggregated total 4 bytes NT_{AGG} Number transactions aggregated 2 bytes ID_{BATCH} ID of POS batch 2 bytes			
Pad Pattern	Successive bytes containing 'BB'	Length of $PKM_{PSAM} – 47 – L_{AT} – L_{AGGTOT}$	known	Debit for Purchase
$ID_{ISS,CEP}$	Identifies the card issuer	4	Initialize for Purchase response	known
ID_{CEP}	Identifies the card	6	Initialize for Purchase response	known
TI	Transaction Type	1	by construction	by construction
$DTHR_{PDA}$	Transaction date and time	5	known	Initialize for Purchase
$CURR_{PDA}$	Currency	3	known	Initialize for Purchase
AM_{CEP}	Authentication method	1	Initialize for Purchase response	known
NT_{CEP}	Transaction number	2	Initialize for Purchase response	known
RID_{PSAM}	RID used by the creator of the PSAM	5	known	recovered from the PSAM certificate

			Origin of data for POS device generation of DS	Origin of data for CEP card verification of DS
$ID_{PSAMCREATOR}$	Identifier of the PSAM creator	4	known	Verify Certificate
ID_{PSAM}	Identifier of the PSAM	4	known	Verify Certificate
ID_{ACQ}	Acquirer ID	4	known	Debit for Purchase
NT_{PSAM}	Transaction number from PSAM	4	known	Debit for Purchase

10.1.4.9 The Debit for Purchase command is sent to the CEP card. The format of the Debit for Purchase command is in Table 54. The response is in Table 55. The status conditions are in Table 56. This command contains the PS_2 signature.

10.1.4.10 The CEP card must use its private key to recover the data in the PS_2 signature. The CEP card must then use the PSAM public key to recover the data in the digital signature (DS) and validate the signature. If the validation is successful, the CEP card must debit the slot. The CEP card must create an S_3 MAC by signing the data in Table 57 with the DES key ($SESSKey_{PSAM}$) recovered from the digital signature (DS). The CEP card must also create an S_6 MAC using a key established by the card issuer for this purpose. The S_6 MAC must be encrypted (E_6).

10.1.4.11 If the CEP card allows aggregation, it must set b1 of the CPO = 1. If the PSAM indicates that it supports MACed aggregation records ($L_{AGGTOT} \neq 0$), and the CEP card set the CPO to indicate aggregation is allowed, the CEP must create an S_6' using a key established by the card issuer for this purpose. The S_6' must be encrypted to create E_6' and the E_6' delivered in the response to the Debit for Purchase command.

10.1.4.12 During a transaction, the CEP card may change from CPO b1 =1 (aggregation allowed) to CPO b1 = 0 (aggregation not allowed). During a transaction, the CEP card must not change from CPO b1 = 0

(aggregation not allowed) to CPO b1 = 1 (aggregation is allowed).

10.1.4.13 If the AM_{CEP} indicates dual authentication with an S_3' is supported and the PSAM makes use of this option ($L_{AT} \neq 0$), then the CEP card must deliver an S_3'.

Table 54 - Debit for Purchase Command Format

Command data	Content	Length
CLA	'90'	1
INS	'54'	1
P1	'00'	1
P2	'00'	1
L_C	Length of command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
ID_{ACQ}	Acquirer id	4
NT_{PSAM}	PSAM transaction number	4
PS_2	Encrypted digital signature of the PSAM	$LPKM_{CEP}$
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 55 - Debit for Purchase and Subsequent Debit Response Format

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
BAL_{CEP}	Updated balance	4
E_6	Encrypted Issuer S_6 MAC	8
CPO_{CEP}	Card purchase options	1
E_6'	Encrypted Issuer MAC on aggregation totals	0 or 8
S_3	Card authentication MAC	8
S_3'	MAC created using AT	0 or 4
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 56 - Status Conditions for Debit for Purchase and Subsequent Debit Command

SW1	SW2	Condition
'67'	'00'	Wrong length
'93'	'02'	Invalid signature
'65'	'81'	Memory failure
'94'	'04'	Value out of range (zero amount not allowed for subsequent debit)
'94'	'03'	Amount is too high for debit
'95'	'80'	Command out of sequence

10.1.4.14 If the CEP card indicates that aggregation is allowed by setting b1 of the CPO = 1 but does not supply an E_6', normal processing must be stopped and exception processing followed.

10.1.4.15 If the CEP card changes from indicating that

aggregation is not allowed (b1 of the CPO = 0) to indicating that aggregation is allowed (b1 of the CPO = 1), normal processing must be stopped and exception processing followed. The PSAM must not aggregate this transaction.

10.1.4.16 The POS device must add M_{PDA} to $MTOT_{PDA}$.

10.1.4.17 The PSAM may validate the S_3 MAC from the CEP card for all steps of a purchase transaction. The PSAM must validate the S_3 MAC from the CEP card for the last step of a purchase transaction. The MAC is validated using the DES key generated by the PSAM for this transaction ($SESSKey_{PSAM}$). The data elements in the S_3 are listed in Table 57. If the S_3 MAC is invalid, normal processing must be stopped and exception processing followed.

10.1.4.18 If the PSAM does not validate the S_3 MAC from the CEP card for a step of a purchase transaction, the POS device should validate the S_3' MAC from the CEP card for that step. The S_3' MAC is validated using the authentication token (AT) received from the PSAM. The data elements in the S_3' are listed in Table 58. If the S_3' is invalid, normal processing must be stopped and exception processing followed. All steps of the purchase transaction not validated by the PSAM must be considered invalid not just the step with the invalid S_3'.

Table 57 - Contents of S_3

			Origin of data for CEP card – generation of S3	Origin of data for POS device – verification of S3
TI	Transaction Type	1	by construction	by construction
$MTOT_{CEP}$	Transaction amount including M_{PDA}	4	by construction	by construction
M_{PDA}	Amount of the last step	4	Debit for Purchase	known
BAL_{CEP}	Updated balance	4	known	Debit for Purchase response
E_6	Encrypted Issuer MAC	8	by construction	Debit for Purchase – response
CPO_{CEP}	Card purchase options	1	known	Debit for Purchase – response
E_6'	Encrypted MAC on aggregation totals	0 or 8	by construction	Debit for Purchase - response

Table 58 - Contents of S_3'

			Origin of data for CEP card – generation of S_3'	Origin of data for POS device – verification of S_3'
TI	Transaction Type	1	by construction	by construction
$MTOT_{CEP}$	Transaction amount including M_{PDA}	4	by construction	by construction
M_{PDA}	Amount of the last step	4	Debit for Purchase	known
BAL_{CEP}	Updated balance	4	known	Debit for Purchase response
E_6	Encrypted Issuer MAC	8	by construction	Debit for Purchase – response
CPO_{CEP}	Card purchase options	1	known	Debit for Purchase – response
E_6'	Encrypted MAC on aggregation totals	0 or 8	by construction	Debit for Purchase - response
S_3	Card authentication MAC for PSAM	8	by construction	Debit for Purchase - response

10.1.4.19 If the first step of the purchase transaction is the only step and the transaction is to be completed, required processing is described in section 10.1.7.

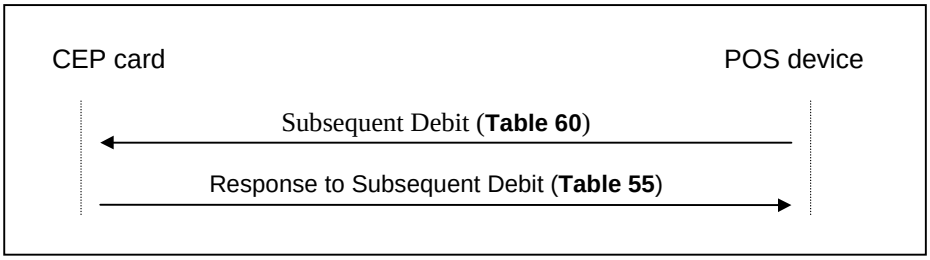
10.1.4.20 If a subsequent debit is to be made after this first step of the purchase transaction, the E_6 and E_6', if there was one, returned by the CEP card, the CPO_{CEP}, the BAL_{CEP}, the $MTOT_{PDA}$ and the amount of this step of the purchase (M_{PDA}) must be retained by the POS device. Additional required processing is described in section 10.1.5.

10.1.4.21 If the first step of the purchase transaction is to be reversed, required processing is described in section 10.1.6.

10.1.5 Incremental Purchase Processing

The flow in Figure 8 shows the continuation of the interaction between the POS device and the CEP card for incremental purchase processing.

Figure 8 - Incremental Purchase Processing



The incremental purchase process consists of:

- Determination of the amount of the next increment of the transaction.
- Creation of the S_2 MAC.
- The Subsequent Debit command, including verification of the S_2 MAC and creation and verification of the S_3 MAC.

10.1.5.1 TI must be reconstructed to indicate an incremental purchase.

10.1.5.2 The amount of the next increment (M_{PDA}) must be determined. M_{PDA} for a subsequent increment of a purchase must be greater than zero. The value of M_{PDA} plus the current value of $MTOT_{PDA}$ must not be greater than $MTOTmax_{CURR}$. If the value is too large, normal processing of the transaction must be stopped and exception processing followed.

10.1.5.3 The AM_{CEP} must be examined. If the card issuer requires mutual authentication for subsequent steps of an incremental purchase, the S_2 MAC must be created

by the PSAM by signing the data elements in Table 59 with the PSAM generated DES key($SESSKey_{PSAM}$). If the card issuer does not require mutual authentication, the S_2 MAC must not be created.

Table 59 - Contents of S_2 MAC for Subsequent Debit and Purchase Reversal

			Origin of data for POS device – generation of S2	Origin of data for CEP card – verification of S2
TI	Transaction Type	1	by construction	by construction
$MTOT_{PDA}$	Cumulative purchase amount already debited	4	by construction	by construction
M_{PDA}	Amount to be debited or reversed	4	known	Subsequent Debit

10.1.5.4 The Subsequent Debit command is sent to the CEP card. The format of the command is in Table 60. The response is in *Table 55 - Debit for Purchase and Subsequent Debit Response Format*.

Table 60 - Subsequent Debit Command Format

Field	Content	Length
CLA	'90'	1
INS	'54'	1
P1	'01'	1
P2	'00'	1
Lc	Command data length	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
M_{PDA}	Next Amount to be debited	4
S_2	MAC of the PSAM (present only if mutual authentication, AM_{CEP} = '02')	0 or 8
PDATA	Proprietary implementation data	var
Le	'00'	1

10.1.5.5 The CEP must create an S_6 using a key established by the card issuer for this purpose. The S_6 MAC must be encrypted (E_6).

10.1.5.6 If the CEP card allows aggregation, it must set b1 of the CPO = 1. If the PSAM indicated that it supports MACed aggregation records ($L_{AGGTOT} \neq 0$) in the Debit for Purchase command, and the CEP card set the CPO to indicate aggregation is allowed, the CEP must create an S_6' using a key established by the card issuer for this purpose. The S_6' must be encrypted to create E_6' and the E_6' delivered in the response to the Subsequent Debit command.

10.1.5.7 If the AM_{CEP} indicates dual authentication with an S_3' is supported and the PSAM indicated in the Debit for Purchase command that it makes use of this option ($L_{AT} \neq 0$), then the CEP card must deliver an S_3'.

10.1.5.8 If the CEP card indicates that aggregation is allowed by setting b1 of the CPO = 1 but does not supply an E_6',

normal processing must be stopped and exception processing followed.

10.1.5.9 If the CEP card changes from indicating that aggregation is not allowed (b1 of the CPO = 0) to indicating that aggregation is allowed (b1 of the CPO = 1), normal processing must be stopped and exception processing followed. The PSAM must not aggregate this transaction.

10.1.5.10 The POS device must add M_{PDA} to $MTOT_{PDA}$.

10.1.5.11 The PSAM may validate the S_3 MAC from the CEP card. The PSAM must validate the S_3 MAC from the CEP card for the last step of a purchase transaction. The MAC is verified using the DES key generated for this transaction ($SESSKey_{PSAM}$). The data elements in the S_3 are listed in Table 57. If the S_3 MAC is invalid, the data from this increment must not be logged. The last successful increment must be logged and normal processing of the transaction must be stopped and exception processing followed.

10.1.5.12 If the PSAM does not validate the S_3 MAC from the CEP card for a step of a purchase transaction, the POS device should validate the S_3' MAC from the CEP card for that step. The S_3' MAC is validated using the authentication token (AT) received from the PSAM. The data elements in the S_3' are listed in Table 58. If the S_3' is invalid, normal processing must be stopped and exception processing followed. All steps of the purchase transaction not validated by the PSAM must be considered invalid not just the step with the invalid S_3'.

10.1.5.13 The E_6 returned by the CEP card, the CPO_{CEP}, the BAL_{CEP} and the M_{PDA} for this increment must be retained as well as the E_6, the CPO_{CEP}, the BAL_{CEP} and the M_{PDA} from the previous increment. If E_6's were provided for this increment or the previous increment, they must be maintained as well. This will allow the correct fields to be logged, even if the current increment is eventually reversed.

10.1.5.14 If the purchase transaction is to be completed, required

processing is described in section 10.1.7.

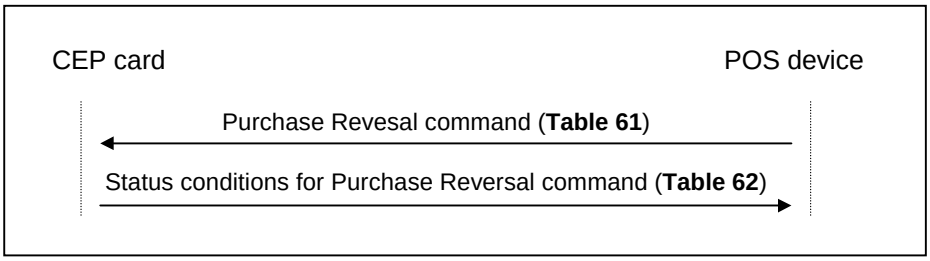
10.1.5.15 If an additional subsequent debit is to be made for this purchase transaction, processing in this section must begin again starting with requirement 10.1.5.1.

10.1.5.16 If the last increment of this purchase transaction is to be reversed, required processing is described in section 10.1.6.

10.1.6 Purchase Reversal Processing

The flow in Figure 9 shows the continuation of the interaction between the POS device and the CEP card for purchase reversal processing.

Figure 9 - Purchase Reversal Processing



The purchase reversal process consists of:

- Computation of the values of a successful reversal transaction.
- Creation of the S_2 MAC.
- The Purchase Reversal command, including verification of the S_2 MAC.

If no response is received from the CEP card for the Purchase Reversal command, the reversal is considered successful.

10.1.6.1 TI must be reconstructed to indicate a reversal.

10.1.6.2 The S_2 MAC must be created by the PSAM by signing the data elements in *Table 59 - Contents of S2 MAC* with the PSAM generated DES key ($SESSKey_{PSAM}$).

10.1.6.3 Before the Purchase Reversal command is sent to the CEP card, the final values of a successfully reversed transaction must be stored in the PSAM.

- The amount of the reversed increment (M_{PDA}) must be subtracted from the previously computed total amount of the purchase ($MTOT_{PDA}$).

- The CPO_{CEP} and the E_6 from the increment prior to the increment to be reversed is retrieved. If an E_6' was received for the increment prior to the increment to be reversed, it must also be retrieved.

- The BAL_{CEP} after a successful Purchase Reversal command must be computed.

This data must be logged by the PSAM as the final transaction detail. The logged data for a reversed single step purchase must not include an S_6 or an S_6' and CPO_{CEP} must be set to '00'.

10.1.6.4 The Purchase Reversal command is sent to the CEP card. The format of the command is in Table 61. The response consists of only SW1 and SW2. The status conditions are in Table 62.

Table 61 - Purchase Reversal Command Format

Field	Content	Length
CLA	'90'	1
INS	'5E'	1
P1	'01'	1
P2	'00'	1
Lc	Command data length	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
S_2	PSAM authentication MAC	8
PDATA	Proprietary implementation data	var

Table 62 - Status Conditions for Purchase Reversal Command

SW1	SW2	Condition
'93'	'02'	Invalid Signature
'95	'80'	Command out of sequence

10.1.6.5 If no response is received from the CEP card, the Purchase Reversal command must be considered successful. No exception processing should be done if the response from the CEP card indicates an error. The data logged in the PSAM must be included in the current batch of transactions.

10.1.6.6 After a reversal, the purchase transaction must be completed. Required processing is described in section 10.1.7.

10.1.7 Complete Transaction

The complete transaction process consists of:

- Determination if this transaction should be aggregated.
- Logging of the transaction data, protected by and an S_5 and updating of the batch summary record, protected by an S_4.

10.1.7.1 The E_6 and E_6', if there was one, returned by the CEP card from the last successful increment of the purchase must be used as the final E_6 and E_6' for this transaction.

If the last increment was reversed, the E_6 and E_6', if there was one, saved by the PSAM from the previous increment must be used.

If there was only one increment for this purchase and it was reversed, there will be no E_6 or E_6'.

10.1.7.2 The CPO_{CEP}, the BAL_{CEP}, the M_{PDA} and the $MTOT_{PDA}$ fields must reflect the transaction status after the last successful increment.

If there was only one increment for this purchase and it was reversed, the CPO_{CEP} and the $MTOT_{PDA}$ must be zero. The BAL_{CEP} must be the BAL_{CEP} returned in the response to the Initialize for Purchase command.

10.1.7.3 The final step in processing a transaction is for the PSAM to determine if the transaction should be

aggregated. The following four conditions must always be met before a transaction can be aggregated:

1. The scheme must allow aggregation.

2. The POS device/PSAM combination must be certified by the scheme to perform aggregation.

3. The card issuer must allow aggregation and the CEP card must allow aggregation for this transaction. This is determined by checking the CPO_{CEP} from the last successful increment of the transaction.

4. The transaction must have completed without an error.

10.1.7.4 The merchant acquirer may also establish additional restrictive parameters that control when a PSAM will aggregate a transaction. If the transaction does not meet the conditions of these merchant acquirer parameters, the detail must be captured. For example, an acquirer restriction may be based on transaction amount (MTOT). In this case, if the $MTOT_{PDA}$ is greater than the MTOT established by the merchant acquirer the transaction must not be aggregated.

10.1.7.5 If aggregation is permitted by the scheme provider, the merchant acquirer and the CEP card, as the card issuer's agent, then the PSAM must determine if the detail must be captured for this particular transaction, based upon the detail transaction percentage for the scheme. The PSAM process of determining the transactions to be aggregated must be based on a random selection rather than selecting transactions in a sequential fashion. The suggested random process is for the PSAM to generate a random number, with at least 2 digits, and divide that random number by 100. If the remainder is less than or equal to the percentage specified by the scheme, the detail must be captured.

10.1.7.6 If the transaction is to be aggregated, the PSAM must determine if it has an aggregation record for the card issuer for the currency of the transaction for this scheme. If the PSAM does not have an aggregation record, a new aggregation record must be created. If the

PSAM has insufficient space to create a new aggregation record, the transaction must not be aggregated. The aggregation record may be stored in the PSAM or in the POS device datastore. However, if the aggregation record is not stored in the PSAM, the PSAM must verify the integrity of the data prior to each update.

10.1.7.7 In addition to the data listed in *Table 65 - Minimum Transaction Data to be Logged in the POS Device*, the fields listed in Table 63 must be updated and logged as part of an aggregation record.

Table 63 - Additional Issuer Aggregation Data

Field	Content	Length
ID_{CEP}	CEP card that created the S_6'	6
$MTOT_{AGG}$	Net value of all aggregated transactions in this aggregation record	4
NT_{CEP}	CEP card transaction number of the last aggregated transaction	2
NT_{AGG}	Number of transactions aggregated in this aggregation record	2
NT_{PSAM}	PSAM transaction number of the last aggregated transaction	4
S_6'	MAC on aggregated total record	8

10.1.7.8 If the count of aggregated transactions in the aggregation record (NT_{AGG}) has reached its maximum value, the transaction must not be aggregated.

10.1.7.9 If the transaction is to be aggregated, the amount of the transaction ($MTOT_{PDA}$) must be added to the aggregation total amount ($MTOT_{AGG}$) for the card issuer. The count of aggregated transactions in the aggregation record (NT_{AGG}) must be increased by 1.

10.1.7.10 If the transaction is to be aggregated and an E_6' was sent by the CEP card, the E_6' must be decrypted to obtain the S_6'. The E_6 must not be used.

10.1.7.11 If the transaction is not to be aggregated, the E_6 must be decrypted to obtain the S_6. If an E_6' was obtained from

the CEP card, it must not be used.

10.1.7.12 The aggregation records must be transmitted to the merchant acquirer at the same time as the non-aggregated detail transaction records in the batch.

10.1.7.13 The PSAM must maintain a batch summary record for each batch. The minimum data in that summary record is listed in Table 64. The summary record may be stored in the PSAM or in the POS device datastore. However, if the summary record is not stored in the PSAM, the PSAM must verify the integrity of the data prior to each update. The data that is in common across all transactions in a batch, for example, the batch number, may be stored once in the summary record rather than with each individual transaction.

10.1.7.14 An S_4 generated by the PSAM must protect all of the CEPS data in the batch summary record sent to the merchant acquirer. The generation of the S_4 must be done in a manner that ensures that no transactions can be deleted from the batch without the merchant acquirer detecting the deletion. Three examples of different methods that may be used are:

1. The PSAM only generates an S_4 for a batch when the batch is closed.

2. The first and last NT_{PSAM} is kept in the batch summary record. If the POS device aggregates transactions, first and last NT_{PSAM} must also be kept with each aggregation record.

3. Some variable data from the previous batch must be stored in the batch summary record. NT_{BATCH} could be used for this purpose. If this method is used, the merchant acquirer will need to keep the information about a collected batch until the batch with the next sequential batch number has been collected.

Table 64 - Minimum Data for a Batch Summary Record

Field	Value	Length (bytes)
RID_{PSAM}	Identifier of the RID owner that assigned the PSAM creator Identifier	5
$ID_{PSAMCREATOR}$	Identifier of the PSAM creator	4
ID_{PSAM}	PSAM Identifier assigned by the merchant acquirer	4
ID_{BATCH}	Batch Number	2
$MTOT_{BATCH}$	Net amount of all transactions (purchases less cancel last purchases) in batch - this includes both aggregated and non aggregated transactions	4
NT_{BATCH}	Total number of transactions in the batch. This includes a count of all detail transactions plus the NT_{AGG} from each aggregation record.	2
S_4	MAC - created using the PSAM MAC key - the minimum contents of the S_4 are the data listed in this table (excluding the S_4 MAC)	8

10.1.7.15 The PSAM must increase the total count of transactions in its active batch (NT_{BATCH}) by 1 and the amount of the active batch ($MTOT_{BATCH}$) by the amount of the transaction ($MTOT_{PDA}$).

10.1.7.16 The data in Table 65 must be updated for each transaction. An S_5 must be created by the PSAM for each record. The minimum data to be used to create the S_5 is the data in Table 65 excluding the S_5. In particular, the S_5 must protect the CEP card generated MACs and the data needed to validate those MACs. For aggregated records, the data in Table 63, must also be included in the MAC. The detailed transaction records do not need to be stored in the PSAM. The aggregation record may be stored in the PSAM or in the POS device datastore. However, if the aggregation record is not stored in the PSAM, the PSAM must verify the integrity of the data prior to each update.

10.1.7.17 A PSAM must maintain a sequential counter of all non-zero amount transactions processed. This counter must be sent to the merchant acquirer with each transaction logged.

Table 65 - Minimum Transaction Data to be Logged in the POS Device

Field	Contents	Length (bytes)	Origin of data	Subset logged for aggregation
ID_{SCHEME}	Usually the AID from the CEP card but may be a reference number	var	known	✔
$ID_{ISS,CEP}$	Issuer Identifier	4	Initialize for Purchase response or Initialize for Cancellation response	✔
ID_{CEP}	Card serial number	6	Initialize for Purchase response or Initialize for Cancellation response	
TI_{PDA}	Transaction Indicator - set by POS device	1	by construction	
$DTHR_{PDA}$	Date & Time stamp from transaction initiation	5	Known	
$CNTRY_{PDA}$	Country of the POS device	2	Known	✔
DOM_{PDA}	Domain of the POS device	1	Known	✔
$CURR_{PDA}$	Currency	3	Known for purchase or from Initialize for Cancellation response	✔
AM_{CEP}	Authentication method supported by the CEP card	1	Initialize for Purchase response, zero for Cancel last Purchase	
NT_{CEP}	Card transaction number	2	Initialize for Purchase response or Initialize for Cancellation response	
RID_{PSAM}	Owner of the RID that assigned the PSAM creator id	5	known	✔
$ID_{PSAMCREATOR}$	Identification of the PSAM creator	4	known	✔
ID_{PSAM}	PSAM Identifier assigned by the merchant acquirer	4	known	✔
ID_{ACQ}	Acquirer ID; usually the actual ID_{ACQ} but may be a reference number	4 or var	known	✔
NT_{PSAM}	PSAM transaction Number	4	known	
$MTOT_{PDA}$	Net value of transaction	4	by construction	

Field	**Contents**	**Length (bytes)**	Origin of data	Subset logged for aggregation
M_{PDA}	Value of last increment (either debit or recredit, depending on TI)	4	Known for purchases or in Initialize for Cancellation response	
S_6	MAC over Issuer-defined data	8	In Debit for Purchase response - will not be present for reversed single step purchases or for cancellations. If not present must be filled with zeros	
BAL_{CEP}	New Card Balance	4	Debit for Purchase response or by construction for cancellation	
DD_{CEP}	Issuer discretionary data	0-16	Initialize for Purchase response or Initialize for Cancellation response	
$DEXP_{CEP}$	Expiration date for transaction	3	Initialize for Purchase response or Initialize for Cancellation response	
ID_{BATCH}	Batch Number	2	By construction	✔
$VKP_{CA,ISS,CEP}$	Version of the CA Public Key the PSAM must use for card authentication	1	Initialize for Purchase response Fill with zeros for cancellation	
$ID_{REG,ISS}$	Identifier of the issuer region - zeros if no region	4	Initialize for Purchase response Fill with zeros for cancellation	
$VKP_{REG,ISS}$	Version number of the region public key used to create the issuer certificate	1	Initialize for Purchase response Fill with zeros for cancellation	
$CSN_{ISS,CEP}$	Identifier of the Issuer's certificate contained in the card	3	Initialize for Purchase response Fill with zeros for cancellation	
CC_{PDA}	Transaction status	2	Known	
S_5	MAC – created by PSAM MAC key	8	By construction	✔

10.1.8 Exception Processing

10.1.8.1 The CEP card must not permit the purchase transaction to take place if any of the following conditions exist:

- The application is blocked, see reference 8, EMV for a definition of application blocking.
- The application is locked.
- The application has been deactivated.
- The application has not been activated.
- The transaction counter (NT_{CEP}) has reached the maximum.
- The slot balance (BAL_{CEP}) exceeds the maximum ($BALmax_{CEP}$).
- The PS_2 signature or S_2 MAC does not authenticate correctly.
- The currency of the POS device ($CURR_{PDA}$)is not supported, that is, there is no slot with a matching currency ($CURR_{CEP}$).
- The slot balance is insufficient ($BAL_{CEP} < M_{PDA}$).

10.1.8.2 If no response is received by the POS device from the CEP card for a command, the POS device may resend the command. If no response is received for a Purchase Reversal command and the CEP card is still available, the POS device must resend the command. If an SW1SW2 of ‘9580’ (command out of sequence) is received from the CEP card when a Debit for Purchase, or Subsequent Debit command is resent, the POS device should send a Get Previous Signature command to the card to obtain the MACs for transaction. If the Get Previous Signature command is successful, normal

processing should resume.

10.1.8.3 If a purchase transaction is terminated before the Debit for Purchase command is sent to the CEP card, the cardholder or POS device operator must be notified that that transaction has been terminated. No further processing is required by the POS device. The conditions that would cause this situation are:

- M_{PDA} exceeds $MTOTmax_{CURR}$.
- The $DEXP_{CEP}$ indicates that the application is no longer valid for purchase transactions.
- The ID_{CEP} is in the scheme blocking list.
- A certificate on the CEP card is invalid.

10.1.8.4 If a purchase transaction is terminated by an error after the Debit for Purchase command is sent to the CEP card, the data elements in Table 64 and Table 65 must be updated and stored in the PSAM and POS device. The completion code field (CC_{PDA}) indicates that the transaction did not complete normally. The values of CC_{PDA} are listed in Table 66.

Table 66 - Transaction Condition Codes Determined by the POS Device

CC_{PDA}	Condition
'00 01'	Invalid or missing MAC from CEP card
'00 02'	No response received from the CEP card.
'00 11'	Cancel Last Purchase invalid, wrong PSAM
'00 12'	Cancel Last Purchase invalid, purchase not in active batch
'6x xx' or '9x xx'	CC_{PDA} contains the Status Words returned by the CEP card.
'00 xx'	RFU
all other values	For proprietary implementations

10.1.8.5 In the event that goods or services cannot be provided, and the CEP card has not been removed, the POS device should attempt to reverse the purchase or the last increment of the purchase.

10.1.8.6 If goods or services have been dispensed but the final MAC does not reach the PSAM due to an interruption such as card removal or power interruption and the CEP card is still available the Get Previous Signature command must be issued for recovery purposes. The processing of this command is in section 8.7.4.

If the CEP card has been removed from the POS device, the Initialize for Purchase command should be sent by the POS device to the CEP card before the Get Previous Signature command is sent. It is during the processing of the Initialize for Purchase transaction, that the PSAM recognizes that it is dealing with a CEP card that participated in an interrupted transaction.

10.1.8.7 If the PSAM cannot complete the process of sending the final transaction log data to the POS device datastore, the PSAM must retain the transaction data and send that data to the POS device when communication with the POS device is restored.

10.2 Cancel Last Purchase Transaction

Cancel last purchase is an off-line transaction that may be optionally initiated by a POS device to cancel the last purchase transaction conducted by the CEP card. The transaction to be canceled must be the last transaction completed by the CEP card. The amount credited may be verified by the cardholder using a monitoring device or a POS or load device.

In the case of an incremental purchase, the cancellation is limited to the amount of the final step.

The same PSAM and CEP card used in the original transaction must be used in performing the cancellation. The transaction to be canceled must still be in the active batch in the POS device.

The cancel last purchase transaction uses two commands: Initialize for Cancellation and Recredit for Cancellation.

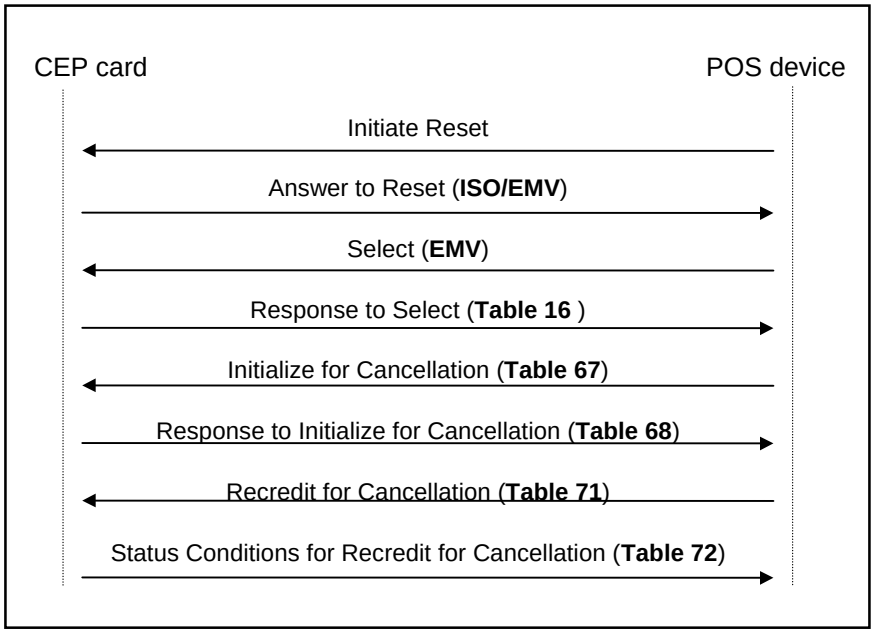
Symmetric cryptography is used in executing a cancel last purchase transaction. The CEP card creates a DES MAC using the DES key supplied by the PSAM in the original purchase transaction. The PSAM uses this MAC to authenticate the CEP card. The PSAM authenticates itself to the CEP card by creating a MAC created using the same DES key. Data for a cancellation is supplied by the CEP card using data from the original purchase transaction. The PSAM also creates a MAC for the transaction using a symmetric key to allow the merchant acquirer to validate the data and the PSAM.

At the completion of each successful Recredit for Cancellation command, the CEP card must update its internal transaction log.

A cancel last purchase transaction may be performed at a POS device that supports aggregation. However, the cancel last purchase transaction must not be aggregated.

The flow in Figure 10 shows the interaction between the POS device and the CEP card for cancel last purchase processing.

Figure 10 - Cancel Last Purchase Processing



10.2.1 Initiate Transaction

The initiate transaction process consists of:

- Application Selection.
- The Initialize for Cancellation command.
- Creation of the S_1 MAC.

10.2.1.1 If the CEP card has not been reset after being inserted in the POS device or if the CEP application has not been selected, the processing described in section 8.5 must occur.

10.2.1.2 If the application profile (AP_{CEP}) on the CEP card indicates that cancel last purchase is not supported, normal processing of the transaction must be stopped and exception processing followed.

10.2.1.3 TI must be constructed as a cancellation.

10.2.1.4 The POS device must begin the cancel last purchase transaction with a Initialize for Cancellation command. The format of this command is in Table 67. The format of the response is in Table 68. The status conditions are in Table 69.

Table 67 - Initialize for Cancellation Command Format

Field	Content	Length
CLA	'90'	1
INS	'50'	1
P1	'02'	1
P2	'00'	1
L_C	Length of the command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$DTHR_{PDA}$	Transaction date and time. If the POS device does not have a clock, any portion of this field that cannot be definitively known is set to zeros.	5
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 68 - Initialize for Cancellation Response Data

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
$ID_{ISS,CEP}$	Issuer ID	4
ID_{CEP}	CEP card identifier	6
$DEXP_{CEP}$	Expiration date for transaction	3
BAL_{CEP}	Slot balance (current)	4
$CURR_{CEP,LOG}$	Currency	3
NT_{CEP}	Transaction Number of the current cancellation transaction	2
$NT_{CEP,LOG}$	CEP Transaction number of the purchase transaction to be canceled	2
$RID_{PSAM,LOG}$	RID used by the PSAM creator	5
$ID_{PSAMCREATOR,LOG}$	Identification of the PSAM creator	4
$ID_{PSAM,LOG}$	Identification of the PSAM	4
$ID_{ACQ,LOG}$	Acquirer Id	4
$NT_{PSAM,LOG}$	PSAM Transaction number of the purchase transaction to be canceled	4
$MTOT_{CEP,LOG}$	Total value of purchase transaction	4
$M_{PDA,LOG}$	Value of last increment	4
S_1	Card authentication MAC	8
L_{DD}	Length of discretionary data	1
DD_{CEP}	Discretionary data	0-16
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 69 - Status Conditions for Initialize for Cancellation Command

SW1	SW2	Condition
'91'	'02'	CEP Transaction Number has reached its limit
'91'	'10'	CEP application has been locked
'94'	'09'	Last transaction was not a Purchase
'95'	'04'	Last Purchase was not successful
'95'	'05'	Last Purchase has been canceled or reversed

10.2.2 Credit CEP Card

The credit CEP card process consists of:

- Validation of the S_1 MAC.
- Creation of the S_2 MAC.
- Logging of the transaction data protected by an S_5 and updating the batch summary record protected by an S_4.
- The Recredit for Cancellation command.

10.2.2.1 The PSAM must validate the S_1 MAC from the CEP card. The MAC is validated using the DES key established with the card during the original purchase transaction ($SESSKey_{PSAM}$). The content of the S_1 MAC is shown in Table 70. If the S_1 MAC is invalid, normal processing of the transaction must be stopped and exception processing followed.

Table 70 - Content of the S_1 MAC

			Origin of data for CEP card – generation of S_1	Origin of data for POS device – verification of S_1
$ID_{ISS,CEP}$	Issuer identifier	4	known	Initialize for Cancellation response

ID_{CEP}	Card identifier	6	known	Initialize for Cancellation response
$DEXP_{CEP}$	Expiration date for transaction	3	known	Initialize for Cancellation response
BAL_{CEP}	Slot balance	4	known	Initialize for Cancellation response
TI	Transaction type (cancel)	1	By construction	By construction
$DTHR_{PDA}$	Transaction date and time	5	Initialize for Cancellation	known
$CURR_{CEP,LOG}$	Currency	3	Log card	Initialize for Cancellation response
NT_{CEP}	Transaction Number of the current cancellation transaction	2	known	Initialize for Cancellation response
$NT_{CEP,LOG}$	CEP Transaction number of the purchase transaction to be canceled	2	Log card	Initialize for Cancellation response
$RID_{PSAM,LOG}$	RID used by the PSAM creator	5	Log card	Known
$ID_{PSAMCREATOR,LOG}$	Identification of the PSAM creator	4	Log card	Known
$ID_{PSAM,LOG}$	Identification of the PSAM	4	Log card	Known
$ID_{ACQ,LOG}$	Acquirer Id	4	Log card	Initialize for Cancellation response
$NT_{PSAM,LOG}$	PSAM Transaction number of the purchase transaction to be canceled	4	Log card	Initialize for Cancellation response
$MTOT_{CEP,LOG}$	Net value of transaction	4	Log card	Initialize for Cancellation response
$M_{PDA,LOG}$	Value of last increment	4	Log card	Initialize for Cancellation response
DD_{CEP}	Discretionary data	0-16	By construction	Initialize for Cancellation response

10.2.2.2 The PSAM must verify that the RID_{PSAM}, the $ID_{PSAMCREATOR}$, and the ID_{PSAM} in the response are the

same as its identifier. Additionally, the PSAM must verify that the transaction is in its active batch. If either of these checks fail, normal processing of the transaction must be stopped and exception processing followed.

10.2.2.3 NT_{PSAM} must be incremented by 1 by the PSAM before the generation of the S_2 MAC.

10.2.2.4 The S_2 MAC must be created by the PSAM by signing the data elements in *Table 73 - Data in S2 MAC for Cancel Last Purchase* with the DES key that the PSAM generated for the original transaction ($SESSKey_{PSAM}$).

10.2.2.5 The PSAM must increase the total count of transactions in its active batch (NT_{BATCH}) by 1 and decrease the amount of the active batch ($MTOT_{BATCH}$) by the amount of the transaction (M_{PDA}).

10.2.2.6 The PSAM must maintain a summary record for each batch. The minimum data in that summary record is listed in Table 64. The summary record may be stored in the PSAM or in the POS device datastore. However, if the summary record is not stored in the PSAM, the PSAM must verify the integrity of the data prior to each update. The data that is in common across all transactions in a batch, for example, the batch number, may be stored once in the batch summary rather than with each individual transaction.

10.2.2.7 An S_4 generated by the PSAM must protect all of the CEPS data in the batch summary record sent to the merchant acquirer. The generation of the S_4 must be done in a manner that ensures that no transactions can be deleted from the batch without the merchant acquirer detecting the deletion. Some examples of methods that may be used are:

- The PSAM only generates an S_4 for a batch when the batch is closed.

- The first and last NT_{PSAM} is kept in the batch summary record. If the POS device aggregates transactions, first and last NT_{PSAM} must also be kept

with each aggregation record.

- Some variable data from the previous batch must be stored in the batch summary record. NT_{BATCH} could be used for this purpose. If this method is used, the merchant acquirer will need to keep the information about a collected batch until the batch with the next sequential batch number has been collected.

10.2.2.8 The data in *Table 65 - Minimum Transaction Data to be Logged in the POS Device* must be updated for each transaction. There is no S_6 or AM_{CEP} for the cancel last purchase transaction.

Fields in Table 65 that are not available for cancel last purchase transactions must be zero filled.

The data must be updated assuming the Recredit for Cancellation command is successful. The logged CC_{PDA} must be '0000', the logged NT_{CEP} must be the NT_{CEP} received in the response to the Initialize for Cancellation command, the logged BAL_{CEP} must be the BAL_{CEP} received in the response to the Initialize for Cancellation command incremented by $M_{PDA,LOG}$.

An S_5 must be created by the PSAM for each record. The minimum data to be used to create the S_5 is in *Table 65 - Minimum Transaction Data to be Logged in the POS Device*. The detailed transaction records do not need to be stored in the PSAM.

10.2.2.9 The Recredit for Cancellation command is sent to the CEP card. The content of the S_2 is in Table 73. The format of the command is in Table 71. The response is only SW1 and SW2.

Table 71 - Format of the Recredit for Cancellation Command

Field	Content	Length
CLA	'90'	1
INS	'52'	1
P1	'01'	1
P2	'00'	1
L_C	Length of the command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
NT_{PSAM}	PSAM transaction number	4
S_2	PSAM authentication MAC	8
PDATA	Proprietary implementation data	var

Table 72 - Status Conditions for Recredit for Cancellation Command

SW1	SW2	Condition
'93'	'02'	Invalid MAC.
'95'	'80'	Command out of sequence (recredit not allowed).

Table 73 - Data in S2 MAC for Cancel Last Purchase

			Origin of data for POS device – generation of S2	Origin of data for CEP card – verification of S2
TI	Transaction type	1	By construction	By construction
NT_{PSAM}	PSAM transaction number	4	known	Recredit for Cancellation
M_{PDA}	Amount to be recredited	4	Initialize for Cancellation response	known

10.2.3 Exception Processing

10.2.3.1 The CEP card must not permit the cancel last purchase transaction to take place if any of the following conditions exist:

- The application is locked.
- The application has been deactivated
- The transaction counter (NT_{CEP}) has reached the maximum.
- The application profile (AP_{CEP}) indicates that cancel last purchase is not supported.
- The S_2 MAC does not authenticate correctly.
- The purchase transaction being canceled was not successful or has already been canceled.
- The last transaction completed by the CEP card was not a purchase.

10.2.3.2 If an error occurs during a cancel last purchase transaction or if the cancel last purchase transaction is not supported by the POS device or by the CEP card, the cardholder or POS device operator must be informed that the transaction is terminated and no additional processing is required by the POS device.

10.2.3.3 If no response is received by the POS device from the CEP card for a Credit for Cancellation command, the POS device must resend the command at least once. If no response is received then from the CEP card, the transaction is assumed to be successful.

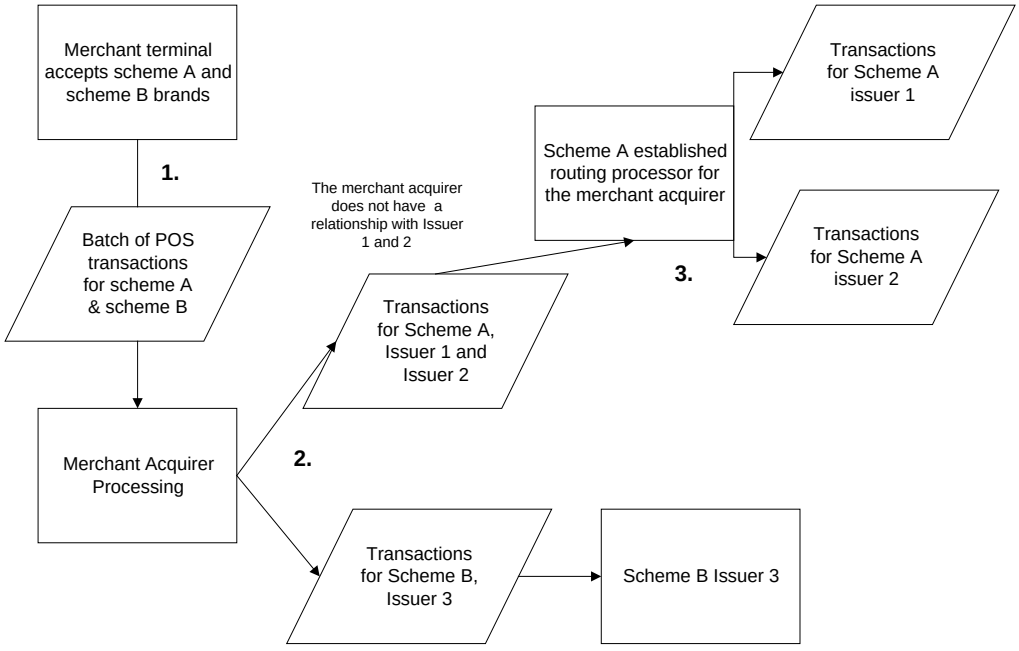
11. Merchant Acquirer Processing

This section describes CEP processing after the transaction batches are collected from the POS devices. How the batches are collected is outside the scope of this document. The minimum validations that must be done are described along with the data that must be sent to the card issuer.

11.1 Transaction Processing

Figure 11 provides an overview of the merchant acquirer processing from the POS device to the card issuer. In this example, the POS device accepts CEP cards from two schemes. The POS transaction processing for both schemes must be the same at the merchant acquirer to maintain interoperability, however, file and record formats to the card issuer will vary by implementation.

Figure 11 - POS Batch Processing Flow



1. The merchant acquirer collects batches of transactions from its merchants. A batch can contain transactions for multiple

schemes.

2. Each batch is validated and sorted by card issuer destination. The merchant acquirer participates in settlement with the card issuer or the entity that receives the batch.

3. When a merchant acquirer becomes a member of a scheme the scheme provider and the merchant acquirer must establish at least one processor to be the destination for all POS transactions intended for a card issuer without a direct connection to the merchant acquirer. In the diagram, card issuer 1 and 2 do not have a direct connection to the merchant acquirer. The data for those card issuers is sent to the processor established by the scheme and the merchant acquirer.

11.1.1 Validating Collected Batches

The merchant acquirer must collect transactions from the POS device, in a manner that ensures integrity of the data, according to a schedule dictated by the scheme providers.

The merchant acquirer must acknowledge receipt of the batch to the merchant or the POS device This acknowledgment can be used by the merchant to trigger the deletion of the batch from the POS device. The timing of the acknowledgment and the deletion process will vary by merchant and merchant acquirer.

The minimum data in a collection batch is defined in *Table 64 - Minimum Data for a Batch Summary Record*, *Table 65 - Minimum Transaction Data to be Logged in the POS Device* and *Table 63 - Additional Issuer Aggregation Data*.

A merchant acquirer processes all batches from its merchants and forwards the transactions to each card issuer or processor. The merchant acquirer participates in settlement with the merchants and each transaction recipient.

11.1.1.1 The merchant acquirer must validate that the collection batch can be read and that all data is formatted correctly to ensure that it has been transmitted correctly. If there was an error in transmission and the batch is still available, it should be re-transmitted. If the batch cannot be properly transmitted, the batch must be rejected, and the transactions in the batch must not be forwarded to the card issuers.

11.1.1.2 The merchant acquirer must perform the batch-level validations described in Table 74. If any of these validations fail, the merchant acquirer must reject the batch, and the transactions in the batch must not be forwarded to the card issuers.

Table 74 - Batch Edit Criteria

Batch Edit	**Validation Criteria**
Duplicate Batch	Validate PSAM identifier and Batch number against previously collected batches.
S_4 MAC	Validate the S_4 MAC.
NT_{BATCH}	Ensure that NT_{BATCH} equals the number of all detail transactions in the batch plus the sum of the NT_{AGG} counter(s) in each aggregation record.
$MTOT_{BATCH}$	Ensure that $MTOT_{BATCH}$ equals the sum of the $MTOT_{PDA}$ from each detail purchase transaction and $MTOT_{AGG}$ from each aggregation record less the $MTOT_{PDA}$ from each detail cancel last purchase transaction.
NT_{PSAM} range	Validate the NT_{PSAM} in each transaction to ensure that there are no missing transactions. If the values of NT_{PSAM} are not always consecutive a method of detecting missing data is required.

11.1.1.3 The merchant acquirer must ensure that no duplicated transactions (as identified by RID_{PSAM}, $ID_{PSAMCREATOR}$, ID_{PSAM} and NT_{PSAM}) are forwarded to the card issuer.

11.1.1.4 The merchant acquirer must validate the ID_{SCHEME} in each transaction to ensure that it is a scheme provider with which the merchant acquirer has a relationship. If the ID_{SCHEME} is not valid, the transaction must be rejected and must not be forwarded to the card issuer.

11.1.1.5 The merchant acquirer must validate each aggregation record using the ID_{SCHEME} to ensure that the scheme provider permits aggregation for its CEP cards. If the scheme provider does not permit aggregation, the aggregation record must be rejected and must not be forwarded to the card issuer.

11.1.1.6 Each record forwarded to the card issuer must contain the results of the acquirer validation (CC_{ACQ}) and an indicator marking the transaction for settlement or for reporting only (SI).

11.1.1.7 The merchant acquirer must perform the transaction-level validations specified in Table 75 for all purchase transactions. If any of these validations fail, the transaction must be forwarded to the card issuer for reporting only. A transaction forwarded for reporting only has the SI field in the transaction set to '01'. The CC_{ACQ} must be set to the value indicated in Table 75 for all transactions that fail a validation. If the transaction passes the validations, the SI and CC_{ACQ} fields in the transactions forwarded to the card issuer must be set to '00'.

11.1.1.8 The merchant acquirer must perform the transaction-level validations specified in Table 75 for all cancel last purchase transactions. If the transaction passes the validations, the SI and CC_{ACQ} fields in the transactions must be set to '00'. If any of these validations fail, the CC_{ACQ} must be set to the indicated value, and the SI field must be set as follows:

- If the POS Completion Code validation fails, the transaction must be forwarded to the card issuer for reporting only and the SI field in the transaction must be set to '01'.

- If any of the other validations fail, the merchant acquirer must ensure that the settlement disposition of the cancel last purchase is the same as the settlement disposition of the corresponding purchase transaction[9].

  – If the purchase transaction is being forwarded for settlement (with SI = '00'), then the cancel last purchase must also be forwarded for settlement.

  – If the purchase transaction is being forwarded for reporting only (with SI = '01'), then the cancel last purchase must also be forwarded for reporting only.

[9] The POS device is required to ensure that a cancel last purchase transaction must be in the same collection batch as the purchase transaction being canceled.

– If no corresponding purchase transaction is present in the batch, then the cancel last purchase must be forwarded for settlement (with SI = ‘00’).

Table 75 - Purchase Transaction Edit Criteria

Transaction Edit	Validation Criteria	CC_{ACQ} if error
S_5 MAC	Validate the S_5 MAC	‘0004’
POS Completion Code	Validate that CC_{PDA} = ‘0000’ (which indicates that the transaction completed normally).	‘0001’
Card Blocking List	Ensure that the card identifier ($ID_{ISS,CEP}$ and ID_{CEP}) is not listed in the scheme provider’s card blocking list (this may be an optional validation for a scheme).	‘0002’
Certificate Revocation	Ensure that the issuer certificate or the optional regional certificate ($VKP_{CA,ISS}$ and CSN_{ISS} and, optionally, $VKP_{REG,ISS}$ and ID_{REG}) is not included in the scheme provider’s certificate revocation list	‘0003’
$VKP_{CA,ISS,CEP}$	Ensure that the $VKP_{CA,ISS,CEP}$ matches a valid PK version for the scheme.	‘0005’

11.1.1.9 The merchant acquirer must perform the transaction-level validations specified in Table 76 for all aggregation records. If any of these validations fail, the transaction must be forwarded to the card issuer for reporting only, the SI field in the transaction must be set to ‘01’, and the CC_{ACQ} must be set to the indicated value.

Table 76 - Aggregate Record Edit Criteria

Transaction Edit	Validation Criteria	CC_{ACQ} if error
S_5 MAC	Validate the S_5 MAC	‘0004’

11.1.2 Creating Issuer Batches

Issuer batches are created by the merchant acquirer and contain all POS transactions for each recipient (which may be either an individual card issuer or a processor). Any sorting or batching

requirements (for instance by currency, scheme, or card issuer) are determined by the processing agreement with the recipient and are outside the scope of this document.

The issuer batch must contain all transactions that passed validations and are being forwarded to the card issuer for either settlement or reporting. Transactions that failed validation, and are being forwarded for reporting purposes only, may be included in the same batch, or may be batched separately, depending on the merchant acquirer's processing agreement with the recipient.

The batch contains each detail and aggregation record being forwarded for settlement, and also includes a batch summary record. The data in the batch must be protected by one or more MACs created by a symmetric key shared between the merchant acquirer and the recipient, using a MAC algorithm shared by the two parties. The MAC or MACs do not need to protect all data in the batch, but must be constructed in such a way that no data in the batch can be changed without detection.

The merchant acquirer must participate in settlement with the card issuer or processor receiving the issuer batch. If the issuer batch or an individual transaction does not pass minimum validation by the recipient, then no settlement for that batch of transaction will occur. See section 16.4.1.1 through 16.4.1.3 for the minimum validations performed by the recipient of an issuer batch.

11.1.2.1 The merchant acquirer must create one or more issuer batches for each recipient. The set of batches must include all detail and aggregate transactions destined to the recipient, including both those transactions to be settled, and those being forwarded for reporting purposes only.

11.1.2.2 Each issuer batch must contain a batch summary record with the minimum data defined in Table 77.

11.1.2.3 The minimum data the merchant acquirer must send to the card issuer for detail transaction records and aggregation records is the data in *Table 63 - Additional Issuer Aggregation Data* and *Table 65 - Minimum Transaction Data to be Logged in the POS Device*. This data must be modified as specified in Table 78

11.1.2.4 The merchant acquirer must protect the data in each

issuer batch with, at a minimum, a MAC over the entire batch. This MAC must be generated using an algorithm and key agreed to with the recipient.

11.1.2.5 The merchant acquirer must participate in settlement with the recipients of the issuer batches. The recipient will be required to settle for each transaction that passes the minimum validations defined in sections 16.4.1.1 through 16.4.1.3.

11.1.2.6 The merchant acquirer must archive each transaction for a period of time specified by the scheme provider.

Table 77 - Issuer Batch Summary Data

Field	Content	Length (bytes)
	Recipient Identifier	var
$DTHR_{BATCH}$	Date and Time batch created.	5
	Source Identifier - may be the merchant acquirer or may be an intermediate processor	var
$ID_{BATCH,SOURCE}$	Batch number assigned by the entity sending this batch (the source of the batch)	2
$MTOT_{BATCH,SOURCE}$	Net amount of settlement transactions in the batch ($MTOT_{PDA}$ of each purchase plus $MTOT_{AGG}$ from each aggregation record less $MTOT_{PDA}$ of each cancel last purchase). The MTOT amount from transactions that are being forwarded for reporting only (where SI = '01') are not included in this total. This field may be the sum of multiple fields within the data.	4
$NT_{BATCH,SOURCE}$	Total number of transactions in the batch. This includes a count of all detail transactions plus the NT_{AGG} from each aggregation record. This field may be the sum of multiple fields within the data.	2
MAC	The MAC generated to protect the entire batch	var

Table 78 - Issuer Transaction Modifications

Field	Content	Length (bytes)
AID_{CEP}	**Modify**: If the ID_{SCHEME} in the collection transaction contains a reference number assigned by the merchant acquirer, the merchant acquirer must replace this reference number with the $AID_{CEP.}$	5-16
ID_{ACQ}	**Modify**: If the ID_{ACQ} field in the collection transaction contains a reference number assigned by the merchant acquirer, the merchant acquirer must replace this reference number with the $ID_{ACQ.}$	4
S_5	**Delete:** This field was included in the collection detail for verification by the merchant acquirer. It must not be sent to the card issuer.	8
CC_{ACQ}	**Append:** The CC_{ACQ} field determined during transaction validation must be appended.	3
DD_{SCHEME}	**Append:** Any additional data required by the scheme provider must be appended.	0-20
SI	**Append:** The SI field determined during transaction validation must be appended.	1

11.2 Truncation

Some scheme providers may permit transactions to be truncated and archived by the merchant acquirer, rather than being forwarded to the card issuer. Some card issuers participating in such schemes may enter into business agreements with merchant acquirers, requiring the merchant acquirers to truncate and store CEP transactions on behalf of the card issuer.

If the merchant acquirer is truncating transactions on behalf of the card issuer, then the merchant acquirer must send only a settlement summary record to the card issuer, in a format agreed between the card issuer and the merchant acquirer.

11.3 POS Device Management

The merchant acquirer is responsible for creating, maintaining and distributing the PSAMs and for maintaining necessary cryptographic keys and other operating data at the point-of-sale. The creation of a PSAM must be under the control of a certified PSAM creator.

11.3.1.1 Each PSAM must be personalized with a unique identifier (RID_{PSAM} + $ID_{PSAMCREATOR}$ + ID_{PSAM}). It must not be possible to alter this identifier after the PSAM has been personalized. The RID_{PSAM} must be a valid RID that the PSAM creator is authorized to use. The $ID_{PSAMCREATOR}$ must be assigned by the owner of the RID_{PSAM}. The ID_{PSAM} must be assigned by a certified PSAM creator.

11.3.1.2 An RSA key pair must be generated for use as the acquirer key. The key must have a minimum modulus length of 896 bits and a public key exponent of either 2, 3 or $2^{16}+1$. The private key portion must never appear in unencrypted form outside of a secure module.

11.3.1.3 If a regional certifying authority is in use, a certificate must be obtained for the acquirer public key signed by the regional certifying authority private key.

11.3.1.4 If no regional certifying authority is in use, a certificate must be obtained for the acquirer public key signed by each of the certifying authority private keys designated by the schemes with which the merchant acquirer has a relationship.

11.3.1.5 An RSA key pair must be generated for each PSAM. The key must have a modulus length of 736 bits and a public exponent of either 2, 3 or $2^{16}+1$.

The PSAM private key must never appear in unencrypted form outside of a secure module.

11.3.1.6 Each PSAM must be personalized with the PSAM private key in a secure manner. It must not be possible to retrieve this key from the PSAM, nor to alter this key after the PSAM has been personalized.

11.3.1.7 A PSAM public key certificate must be generated signed by the acquirer private key.

11.3.1.8 One or more symmetric keys for each PSAM must be generated for use in generating and verifying the S_5 and the S_4 MACs. These keys must never appear in unencrypted form outside of a secure module.

The PSAM must be personalized with the symmetric MAC keys. It must not be possible to retrieve these keys from the PSAM. These keys may be updated only if the updates can be sent to the PSAM encrypted and MACed.

11.3.1.9 A secret key must never appear in unencrypted form outside of the PSAM or other secure module.

11.3.1.10 The merchant acquirer must be able to receive from the scheme providers, and send to the POS device, all scheme operating data. It must be possible to update this data as required by the participating schemes. The required operating data is described in section *Table 36 - CEPS Operating Data for a Scheme*.

The CA public keys for a scheme must be stored in the PSAM and must be updated using a MAC to ensure the integrity of the data.

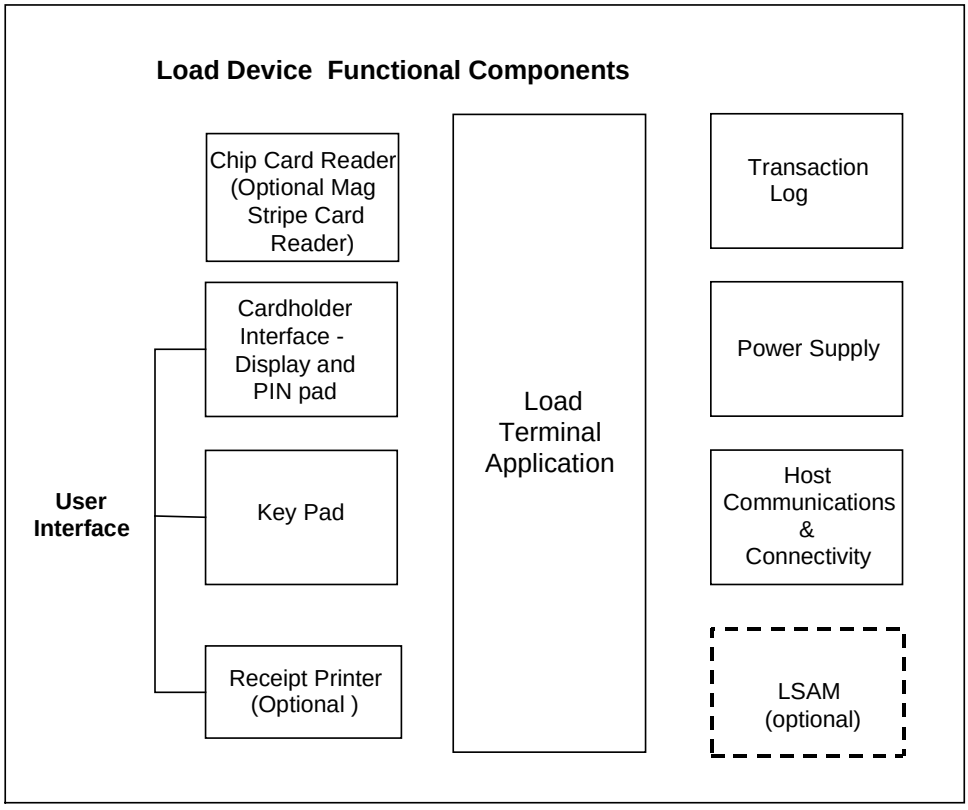
11.3.1.11 The merchant acquirer must be able to update the operating data in the POS device and PSAM as required by the schemes with which it has a relationship.

12. Load Device Characteristics

12.1 Overview of a Load Device

Figure 12 illustrates the functional components of a CEP load device.

Figure 12 - The Load Device



Load devices may operate in both attended and unattended environments. In an attended environment, for example, a load device at a bank branch teller station, a third party will enter data for the CEP transaction.

In an unattended environment, (for example, a kiosk at a public transit station, or a home computer), the CEP transaction is automated for the cardholder.

The load device will interface with a load acquirer's host software using proprietary message formats and communication protocols.

12.2 Requirements

Load devices that are not interoperable are outside the scope of these requirements.

12.2.1 Support for Multiple Schemes and Currencies

12.2.1.1 Load devices that follow these specifications are able to support the acceptance of cards from multiple CEP schemes. However, business relationships between the load acquirer and the particular scheme provider must determine whether a particular load device accepts a scheme's CEP cards.

12.2.1.2 Each load device must maintain a list of the AIDs that it supports.

A load device that supports multiple AIDs must have the ability to select an application by comparing the set of AIDs supported in the device, and the set of AIDs present on the CEP card. In some cases, interaction with the cardholder may be required in making the final decision on which application to select. The application selection process is described in reference 8, EMV.

12.2.1.3 The load device must contain a list of currencies that it supports. A currency cannot be loaded at a load device unless the load device supports that currency. For a currency exchange transaction, only currencies that the load device supports can be target currencies.

12.2.2 Compliance with Standards

12.2.2.1 The load device must comply with the requirements stated in these specifications. Additionally, the standards in reference 8, EMV and any country or local governing standards apply. If a country or local standard is more stringent than, or conflicts with, requirements in these specifications, then the country or local standard overrides any of these requirements. Additional standards include:

- Applicable key and PIN management standards.
- Electromagnetic standards.
- Country-specific electrical and modem standards.
- Procedures for cardholder interface screens, buttons, and keyboards.

12.2.3 Card Acceptance

12.2.3.1 Device hardware and software must be capable of interacting with the CEP applications as described in this document.

12.2.3.2 Devices must not assume that a funding application on a CEP card is the funding account to be used for a load. If the load device supports unlinked loads, cardholders must be prompted to indicate their selected funding source. The load device may offer the cardholder the option of selecting the type of account to use.

12.2.4 Card Reader

12.2.4.1 The load device must have an integrated circuit card (ICC) reader that is compatible with reference 8, *EMV* Part 1. The card reader must support both T=1 and T=0 protocols. When T=1 is used, the NAD sent to the CEP card must be zero.

12.2.4.2 The reader must let cardholders retrieve their cards either manually or automatically at the completion or termination of a load transaction.

12.2.4.3 In environments where the card is accessible to the consumer during a transaction, the load device must be capable of determining that a card has been removed before the completion of the transaction and must be able to perform the necessary exception processing.

12.2.4.4 The load device must secure the CEP card in the reader in unattended devices to reduce the likelihood of the card being accidentally removed or moved around while the load or currency exchange transaction takes place.

12.2.4.5 A magnetic stripe card reader should also exist to support the reading of magnetic stripe cards for unlinked loads.

12.2.5 Display and Cardholder Interface Design

The cardholder interface should be easy to use. The cardholder interface includes the screen dialog, function keys, brand signage, PIN pads and printed receipts (where applicable).

12.2.5.1 The following information must be provided to the cardholder:

- CEP card slot balance before the transaction and the currency of the slot.

  For currency exchange transactions, the load acquirer may not support all of the source currencies loaded onto the CEP card. An alphabetic currency code will have been established by the card issuer for all slots on the card that have a currency assigned. This field ($CALPHA_{CEP}$) must be used to display the currency of the slot to the cardholder. The currency exponent is the last byte of the currency and that field ($CURRE_{CEP}$) must be used to correctly display the minor units of currency.

- The maximum amount that can be loaded. The source of this information is either:

  – information in a slot when a currency has been assigned to a slot in the CEP card (BALmax),

  – or a CEP card reference maximum balance (REFBALmax). When both the card issuer and the load acquirer support it, the reference maximum balance on the CEP card will be converted to an amount in the currency to be loaded.

  – or a load device default.

- Amount to be loaded or source amount to be exchanged, allowing the cardholder to choose or

confirm the amount.

- Card slot balance after a load or currency exchange transaction.

- Visual or audible status confirmation of the transaction, for example, completed or terminated.

- Exception messages such as request declined by issuer, communications failure, insufficient funds.

12.2.5.2 For vendors that want to manufacture personal use load devices driven by voice recognition rather than by key entry and screen display, the information stated above must be available as part of the cardholder interface. The criteria for secure PIN pads defined in this standard are also mandatory for this type of device.

12.2.5.3 The load device must permit termination of the current transaction, allowing removal of the card, up until the time the cardholder chooses the load or exchange amount to be used for the load or currency exchange transaction.

12.2.6 Financial PIN Security

This section describes security issues that pertain only to load devices designed to accept a financial PIN in a shared network environment.

A load device that utilizes a financial PIN is also categorized as a PIN Entry Device (PED). A PIN Entry Device is a physically and logically protected hardware device that provides a secure set of cryptographic services.

12.2.6.1 A PIN Entry Device must perform cryptographic functions.

12.2.6.2 All clear text keys and PINs must be physically protected against disclosure and unauthorized modification within a PIN Entry Device. Disclosure does not apply to public keys.

12.2.6.3 A PIN Entry Device must be tamper responsive. This

means that physical penetration of a PIN Entry Device, when it is being operated in its intended manner and environment, must cause the automatic and immediate erasure of all PINs, cryptographic keys and all useful residue of PINs and keys contained within the device. Attempts must leave evidence such that the device cannot be put back in service without a high probability of the tampering being noticed.

12.2.6.4 The unauthorized determination of the secret data (PINs and keys) stored within the PIN Entry Device, or the placing of a "tap" within the device to record secret data, must result in physical damage to the device to the extent that the damage has a high probability of detection should the device be placed back in service. Furthermore, determining the data stored within the device must require specialised equipment and skills that are not generally available.

12.2.6.5 Controls must be in place to ensure that equipment is not re-installed when a suspicious alteration of a key in a PIN Entry Device is detected until it has been inspected and a reasonable degree of assurance has been reached that the equipment has not been subject to unauthorized physical or functional modification.

12.2.6.6 PIN Entry Devices must be designed in such a way to prevent state of the art monitoring attacks, such as radiation tapping, covered channel analysis etc. known at the time of certification.

12.2.6.7 Each PIN Entry Device must be uniquely identifiable within the Card-Accepting Scheme. The internal ID must not be changed after initialisation.

12.2.6.8 Based on a combination of adequate control procedures during the production process and special features available through design, it must be ensured at initial key loading that a PIN Entry Device is authentic, corresponds to a certified construction and is loaded with a certified program.

12.2.6.9 Subsequent down-line loading of program updates must

only take place after origin authentication. This requirement applies only to security related services in PIN Entry Devices.

12.2.6.10 Transmission of the clear text PIN from the PIN Entry Device keyboard to the circuitry where it will be enciphered must take place within the boundaries of the PIN Entry Device. The transmission medium (cable, wire) between the PIN Entry Device keyboard and the encipherment circuitry must be highly physically protected and prohibit installation of tapping devices.

12.2.6.11 The PIN must be enciphered within the device using an approved ISO (see next) algorithm and PIN block format.

12.2.6.12 In order to obtain secure transfer of the transaction PIN, PIN block encipherment must use one of the following:

- a "unique key per transaction" scheme as specified in ISO 9564-1,
- a double length key as specified in ISO 11568-2,
- a technique guaranteeing at least the same cryptographic strength.

12.2.6.13 Data and keys must only be used in the PIN Entry Device for which they were originally intended.

12.2.6.14 A PIN Entry Device must only be placed in service if there is an assurance that the equipment has not been subject to unauthorized modifications or tampering.

12.2.6.15 A PIN Entry Device should be recognised as a genuine certified device.

12.2.6.16 Successful penetration of the device must not permit disclosure of any previously entered Transaction PIN (i.e. prevent backtracking).

12.2.6.17 There must be no feasible way to determine any past key given the knowledge of any data which had been transmitted to or from the device while in operational

service.

12.2.7 Date and Time Processing

12.2.7.1 Support of a real-time clock with battery backup is required. The load device must synchronize its clock to ensure that it contains a date and time that is within 4 hours for the actual date and time.

12.2.8 Power Failure

12.2.8.1 In case of a power loss during a transaction, the load device must notify the load acquirer host about the status of the transaction either immediately or on resumption of power. If all load acquirer processing is in a single device this notification will not occur.

12.2.8.2 If the card is fully contained within the load device, the device must eject the card in case of a power failure.

13. Load Acquirer Processing - Load Transactions

Load is an on-line transaction initiated by a load device and sent to the card issuer host system. The amount actually loaded may be verified by the cardholder using a monitoring device or the load device.

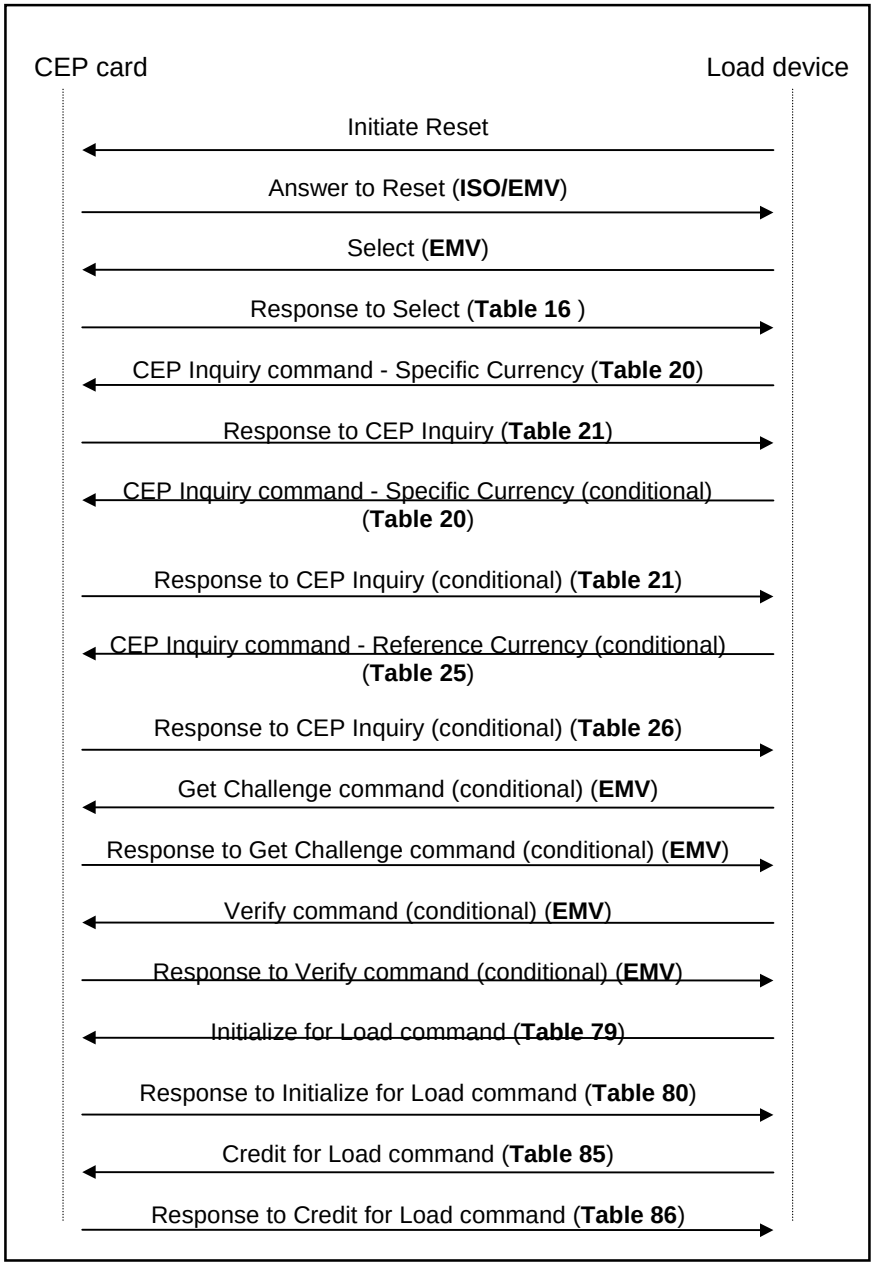
The load device determines the currency to be used prior to the start of the transaction. If the load device supports multiple load currencies the cardholder selects the currency to be loaded. The load device uses the CEP Inquiry command to determine the current and maximum balances in the slots in the CEP card for the currency or currencies it supports. The balance information is used to display the current balance and the maximum amount that can be added to the slot. If there is no slot in the CEP card for the specified currency, the CEP card responds to the CEP Inquiry with a status code that identifies this condition to the load device. This status code also reflects whether there is an empty slot available for loading a new currency. If the currency does not exist in the CEP card and there is no empty slot available, the load device may prompt the cardholder to initiate a currency exchange transaction, otherwise, normal processing of the transaction must be stopped and exception processing followed.

Load transactions use two commands: Initialize for Load and Credit for Load. The Credit for Load command must be preceded by a successful Initialize for Load command.

At the completion of each successful Credit for Load command, the CEP card must update its internal transaction log.

The flow in Figure 13 shows an interaction between the load device and the CEP card for load processing. Other flows are possible as long as they meet the requirements in this specification.

Figure 13- Load Processing



13.1 Normal Processing

13.1.1 Initiate Transaction

The initiate transaction process consists of:

- Application Selection.
- Determination of the currency and the maximum balance.
- Determination of the source of funds.
- Verification of off-line PINs (if off-line PIN processing selected for linked loads).
- The Initialize for Load command.
- Creation of the S_1 MAC.
- Generation and use of R_1 for unlinked loads.

13.1.1.1 At attended load devices, cardholder decisions may be entered by the device operator. PINs must be entered by the cardholder.

13.1.1.2 If the CEP card has not been reset after being inserted in the load device or if the CEP application has not been selected, the processing described in section 8.5 must occur.

13.1.1.3 If the load device supports multiple currencies, the cardholder must be allowed to select the currency to be loaded.

13.1.1.4 The load device must use the CEP Inquiry command described in section 8.7.1 to determine the current and maximum balances for the currency to be used for this transaction. Retrieval of this information from the CEP card may occur before the cardholder chooses the currency of the transaction, and in that case, the current and maximum balances for all currencies supported by both the load device and the CEP card must be obtained.

13.1.1.5 If a maximum balance has been established in the card for the currency to be loaded, the cardholder must not be able to enter a load amount greater than the maximum balance minus the current balance.

If the currency to be loaded is not a currency already assigned to a slot in the CEP card, no maximum balance is available for display. The load device may issue a CEP Inquiry command (see Table 25) to obtain an reference maximum balance (REFBALmax) in a reference currency selected by the card issuer. The reference currency should be a widely used currency to maximize the likelihood that the it will be recognized by load devices worldwide. The load device may use this estimated maximum balance in the display to the cardholder. If the reference currency is not the load currency, it must be converted before being used. The load acquirer must establish the currency conversion rate to be used. The load device must indicate to the cardholder that this is an estimated maximum balance and should not limit the cardholder to values based on this maximum.

13.1.1.6 If the application profile (AP_{CEP}) indicates that the CEP card supports both linked and unlinked loads, the load device must prompt the cardholder to determine which is requested. If the load device only supports linked load or only supports unlinked load, the load device must ensure that the card supports that type of load by looking at the CEP card application profile.

13.1.1.7 The load device must determine the source of funds for a load transaction through an interaction with the cardholder.

For a linked load, a load device that supports account selection must check the application profile (AP_{CEP}) in the CEP card to see if account selection is supported by the CEP card. If account selection is supported, the load device should prompt the cardholder to indicate whether the source of funds is a debit, credit, or deposit account.

For an unlinked load, the source of funds must be one of the following:

- a funding application on the CEP card; the load device may prompt the cardholder to indicate whether the source of funds is a debit, credit, or deposit account.

- a funding application on another card; the load device may prompt the cardholder to indicate whether the source of funds is a debit, credit, or deposit account.

- cash.

The funding application must not be a CEP application.

If the source of funds is a funding application, the load device reads information from the funding application. The processing of cardholder identification for a funds request for an unlinked load is outside of the scope of this document. This processing is addressed in documents describing the funding application.

The physical handling of cash is outside of the scope of this document.

13.1.1.8 Cards supporting linked loads must allow on-line PINs, and must support off-line PINs in either cleartext or encrypted form or both. The application profile (AP_{CEP}) indicates the type(s) of off-line PIN supported by the CEP card.

For a linked load, the load device must obtain a PIN from the cardholder and determine if on-line or off-line PINs are to be used.

From the AP_{CEP}, the load device determines the type(s) of PIN supported by both the card and the load device, and selects one of the mutually supported types.

If the selected PIN type is on-line, the PIN must be encrypted and sent to the card issuer for validation.

If off-line PIN processing is selected, the load device must authenticate the cardholder by sending the PIN in unencrypted or encrypted form to the CEP card using the Verify command. If the PIN is encrypted, the

Verify command must be preceded by a Get Challenge command. The result of the Verify command is retained by the CEP card and should be sent to the card issuer in the DD_{CEP} field. The Get Challenge and Verify commands are coded as described in reference 8, EMV.

If encrypted PINs are used, verification of the highest level certificate uses the CA public key identified by the version number ($VKP_{CA,ISS}$) recovered from the FCI returned in the response to the Select command (see *Table 16 - Response to Select Command*). The CA public key must be in the SAM of a secure PIN pad used for encryption of PINs,

If the off-line PIN is blocked or if the off-line PIN is entered incorrectly and there are no more attempts allowed, the load acquirer must continue normal processing of the transaction[10].

13.1.1.9 The load device sends an Initialize for Load command to the CEP card to begin the load process. The format of the Initialize for Load command is shown in Table 79. The format of the response to the Initialize for Load command is shown in Table 80. The status conditions are in Table 81.

[10] The off-line PIN must not be sent in the message to the card issuer. The reason that the transaction is sent to the card issuer with an error is that this processing allows the card issuer to respond to the message with a PIN unblock command.

Table 79 - Initialize for Load Command

Field	Content	Length
CLA	'90'	1
INS	'50'	1
P1	'00'	1
P2	'00'	1
L_C	Length of command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$DTHR_{LDA}$	Transaction date and time	5
$CURR_{LDA}$	Currency	3
ID_{LACQ}	Identifies the load acquirer	4
ID_{LDA}	Load device ID	6
M_{LDA}	Amount to be loaded	4
PDATA	Proprietary implementation data	var
L_e	'00'	1

Table 80 - Initialize for Load Response data

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
$ID_{ISS,CEP}$	Issuer ID	4
ID_{CEP}	Card identifier	6
$DEXP_{CEP}$	Expiration Date	3
NT_{CEP}	Transaction Number	2
S_1	Card MAC	8
H_{CEP}	10 most significant bytes of the SHA-1 hash of transaction data (including an R_{CEP} generated by the CEP card that is unique for this transaction).	10
L_{DD}	Length of discretionary data	1
DD_{CEP}	Discretionary data -It is strongly recommended that DD_{CEP} include $NT_{LASTLOAD}$, $NT_{LASTCANCEL}$, and the Pin verification results for all loads.	0-32
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 81 - Status Conditions for Initialize for Load

SW1	SW2	Meaning
'91'	'01'	Application is not active
'91'	'02'	Transaction Number (NT_{CEP}) has reached its limit
'91'	'06'	Application has been deactivated
'91'	'10'	CEP application is locked
'94'	'01'	Currency specified cannot be loaded. The requested currency is not established in a slot and there are no available slots.
'94'	'02'	Load amount is too high ($BAL_{CEP}+M_{LDA}>BALMAX_{CEP}$).

13.1.1.10 The load device must not allow a transaction from a CEP card that is has expired for load transactions. The

$DEXP_{CEP}$ field must be equal to or later than the current date in the load device. If the CEP card has expired for load transactions, normal processing of the transaction must be stopped and exception processing followed.

13.1.1.11 The load device may warn the cardholder if the CEP application is about to expire.

13.1.1.12 If an unlinked load has been requested the LSAM must perform the following steps:

- Generate a random number (R_1).

  R_1 will be used as a DES key and must be odd parity.

- Encrypt R_1 under a secret key known to next processing node. R_1 may be transmitted in the PIN block of transactions.

- Generate 2 16 byte random numbers (R_{LSAM} and $R2_{LSAM}$) for this transaction. Create two SHA-1 hashes of transaction data and each random number (H_{LSAM}) and ($H2_{LSAM}$). Only the 8 most significant bytes of the hashes will be used. See section 6.5.1.7 for the contents of H_{LSAM} and $H2_{LSAM}$.

- Create a MAC (MAC_{LSAM}) of the data elements in Table 82 using R_1 as the MAC key. The MAC must be created as described in reference 8, EMV. Only the 4 most significant bytes of the generated MAC will be used.

- Set the ALG_{LSAM} to ‘01’, indicating these specifications for unlinked load security.

Table 82 - Data Elements in the MAC of an Unlinked Load

Field	Content	Length
$ID_{ISS,CEP}$	Issuer ID	4
ID_{CEP}	Card identifier	6
NT_{CEP}	Transaction Number	2
$CURR_{LDA}$	Currency	3
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
M_{LDA}	Amount to be loaded	4
S_1	MAC from the CEP card	8
H_{CEP}	The 10 most significant bytes of the SHA-1 hash of transaction data (including an R_{CEP} generated by the CEP card that is unique for this transaction)	10
H_{LSAM}	The 8 most significant bytes of the SHA-1 hash of transaction data (including an R_{LSAM} uniquely generated by the LSAM for this transaction)	8
$H2_{LSAM}$	The 8 most significant bytes of the SHA-1 hash of transaction data (including an $R2_{LSAM}$ uniquely generated by the LSAM for this transaction)	8
DD_{CEP}	Discretionary data	0-32

13.1.1.13 The load acquirer must assign a unique acquirer generated identification number (REFNO) for this transaction. For a non cash unlinked load, the messages going to the card issuer and the funds issuer may have different identification numbers.

13.1.1.14 The load acquirer must communicate with the card issuer and, for non cash unlinked loads, communicate with the funds issuer. The communication with the funds issuer may precede, follow or be done in parallel with the communication with the card issuer. The load request must be logged. If parallel processing is used and communications with the funds issuer is required, the load acquirer must wait for both responses to determine the subsequent processing.

13.1.2 Communicate with Card Issuer

The communicate with card issuer process consists of:

- Sending the load request to the card issuer.
- Receiving a response from the card issuer.

13.1.2.1 The minimum information to be sent to the card issuer is listed in Table 83.

Table 83 - Minimum Data Elements Sent to the Card Issuer for a Load Transaction

Field	Content	Length
	Indicator - linked or unlinked load request	var
AID_{CEP}	Scheme identifier	5-16
BAL_{CEP}	Balance prior to Load	4
$BALmax_{CEP}$	Maximum slot balance (0 if new currency)	4
$CNTRY_{LDA}$	Country of the load device	2
$CURR_{LDA}$	Currency	3
DD_{CEP}	Discretionary data	0-32
DD_{SCHEME}	Discretionary data required by the scheme	0-20
$DEXP_{CEP}$	Expiration date	3
DOM_{LDA}	Domain of the load device	1
$DTHR_{LDA}$	Transaction date and time	5
ID_{CEP}	Card identifier	6
$ID_{ISS,CEP}$	Issuer ID	4
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
M_{LDA}	Amount to be loaded	4
NT_{CEP}	Transaction Number	2
$REFNO_{ACQ,ISS}$	Acquirer identifier for the transaction	3

S_1	Signature from the CEP card	8
The following are sent for unlinked loads		
ALG_{LSAM}	Algorithm defining cryptographic approach between LSAM and card issuer SAM. Set to '01'	1
$DES(R_1)$	Encrypted random number generated by LSAM using key known by issuer or the next processing node	8
MAC_{LSAM}	MAC of transaction data using R_1 as key	4
H_{LSAM}	The 8 most signification bytes of a SHA-1 hash of transaction data (including an R_{LSAM} uniquely generated by the LSAM for this transaction)	8
$H2_{LSAM}$	The 8 most significant bytes of a SHA-1 hash transaction data (including an $R2_{LSAM}$ uniquely generated by the LSAM for this transaction)	8
The following may be sent for linked loads		
ACCTTYPE	Type of funding account - for linked loads	1
encrypt(PIN block)	Encrypted PIN block	8

13.1.2.2 The minimum information to be received from the card issuer for approved transactions (CC_{ISS} = '0000') is listed in Table 84. If the transaction is not approved, the items marked as "optional for declines" may not be present. If a transaction is not approved by the card issuer, exception processing (see section 13.2) must be followed.

Table 84 - Minimum Data Elements Sent by the Card Issuer to the Load Acquirer on a Load Transaction

Field	Content	Length
$BALmax_{ISS}$	An optional maximum balance sent as an advice to the load acquirer by the card issuer, if the amount to be loaded plus the current balance (if there is one) is greater than the maximum balance the card issuer will allow	4
CC_{ISS}	Completion code	2
DD_{ISS}	Discretionary data from issuer - optional for declines. If a new currency is being established, BALmax, and CALPHA must be included.	0-64
ID_{CEP}	Card identifier	6
$ID_{ISS,CEP}$	Issuer ID	4
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
$REFNO_{ACQ,ISS}$	Acquirer transaction identifier	3
S_2	MAC from issuer. Optional for declines For unlinked loads must contain H_{LSAM} for approvals. For declines, if present, must not contain H_{LSAM}.	8

13.1.3 Communicate with Funds Issuer

The communicate with funds issuer process consists of:

- Sending the authorization request to the funds issuer.
- Receiving a response from the funds issuer.

13.1.3.1 The load acquirer will only communicate with the funds issuer if

- this is an unlinked load, and
- the source of funds is an account at the funds issuer.

13.1.3.2 The message to the funds issuer must contain an indication that this is a funds authorization for a CEP

load. The other information to be sent to the funds issuer is defined by the funding application.

13.1.3.3 The information to be received from the funds issuer is defined by the funding application.

13.1.3.4 If a transaction is declined by the funds issuer, exception processing (see section 13.2) must be followed.

13.1.4 Credit CEP Card

The credit CEP card process consists of:

- Processing of script messages from the card issuer.
- The Credit for Load command.
- Notification of the cardholder of the results of the load transaction.
- Participation in settlement for unlinked loads.

This section will only be performed for approved transactions. If either the card issuer or the funds issuer declines a transaction, exception processing must be followed. Transactions approved by the card issuer will have CC_{ISS} = '0000'.

13.1.4.1 For unlinked loads, the LSAM must release R_{LSAM} for inclusion in the Credit for Load command.

If a funds request is sent to a funds issuer, this process must not be performed before an approval is received from the funds issuer. See section 13.2.2.9.

13.1.4.2 The load device must examine the response received from the card issuer to see if it contains any script messages. Any script message beginning with tag '71' must be sent immediately to the CEP card. The format and processing of the script messages is in reference 8, EMV.

13.1.4.3 The Credit for Load command is sent to the CEP card with P2 set to '00'. The format of the Credit for Load

command is shown in Table 85. The format of the response to the Credit for Load command is shown in Table 86. The status conditions are in Table 87.

If the status condition from a Credit for Load command is not '9000' the response to the command consists only of SW1 SW2 and no signatures are generated.

13.1.4.4 If the status condition from a Credit for Load command is '9000' the CEP card must respond with an S_3 MAC. If the CEP application rejects the Credit for Load command (the first byte of CC_{TRX} b8 = 1), the CEP card must also send R_{CEP} in the response. For unlinked loads, the LSAM must verify R_{CEP} in the response by comparing, in a secure manner, a SHA-1 hash of the R_{CEP} in the CEP card response and other transaction data (see section 6.5.1.7) with the H_{CEP} sent by the CEP card in the response to the Initialize for Load command. If the CEP card rejects the Credit for Load command exception processing (see section 13.2) must be followed.

13.1.4.5 For linked loads, if there is no response to the Credit for Load command, exception processing (see section 13.2) must be followed.

13.1.4.6 For unlinked load, if there is no response to the Credit for Load command, or if any other interruption in processing occurs after the R_{LSAM} has been released from the LSAM, exception processing (see section 13.2) must be followed.

Table 85 - Credit for Load Command Format

Field	Content	Length
CLA	'90'	1
INS	'52'	1
P1	'00' – R_{LSAM} not in command, don't return R_{CEP} '10' – R_{LSAM} in command, return R_{CEP}	1
P2	'00' - if the slot balance and, optionally, other data are to be updated (S_2 must be present) '80' - if nothing is to be updated (S_2 must not be present, P1 must be '00') '81' - if the slot balance is not to be updated, but other data is to be updated (S_2 must be present, P1 must be '00')	1
Lc	Length of command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
CC_{ISS}	Completion code (fill with 'FFFF' if response not received from card issuer)	2
S_2	Card Issuer MAC - optional for declines - must be present if DD_{ISS} is present and must include CC_{ISS}. Data used to create MAC must include H_{LSAM} for approved unlinked loads. Data used to create MAC for declines and approved linked loads must not include H_{LSAM}.	0 or 8
R_{LSAM}	Random number from LSAM - only present for approvals of unlinked loads.	0 or 16
L_{DD}	Length of discretionary data	1
DD_{ISS}	Discretionary data from issuer - optional for declines	0-64
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 86 - Credit for Load Response Format

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
BAL_{CEP}	Slot balance after load - unchanged if P2 is not equal to '00'	4
CC_{TRX}	Transaction completion code	2
S_3	Final MAC from CEP card	8
R_{CEP}	Proof of no transaction (included only if load failed and a P1 = '01', a P2 = '00' and R_{LSAM} were sent in the Credit for Load command)	0 or 16
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 87 - Status Conditions for Credit for Load

SW1	SW2	Meaning
'95'	'80'	Command out of sequence (load not allowed).

13.1.4.7 Any script commands received from the card issuer beginning with a tag '72' must be sent to the CEP application after the Credit for Load command is completed. The format and processing of script messages is in reference 8, EMV.

13.1.4.8 If the transaction was successful (first byte of CC_{TRX} = '00'), a transaction completion message may be sent to the card issuer. The format of the transaction completion message is in *Table 90 - Minimum Data to be Included in a Transaction Completion Message to the Card Issuer*.

13.1.4.9 The information in the completion message is combined with the information already logged to create the final log for the transaction. A log of all load transactions must be maintained by the load acquirer regardless of completion status for the period of time defined by the scheme provider.

13.1.4.10 If the transaction was a successful unlinked load, the load acquirer must participate in the settlement process with the card issuer. If the transaction was a successful non cash unlinked load, the load acquirer must participate in the settlement process with the funds issuer. The load acquirer is due funds from the funds issuer for successful non cash unlinked loads and owes funds to the card issuer for all successful unlinked loads.

13.1.4.11 If the transaction was not successful the exception processing in section 13.2 must be performed.

13.1.5 Notification to Cardholder

13.1.5.1 The load device must notify the cardholder of the results of the transaction.

13.1.5.2 If CC_{ISS} is not equal to zero, this must be treated as an error situation and the cardholder notified of the error. In certain situations the card cardholder must be notified of the specific error. These error conditions are listed in *Table 102 - Issuer Validations for Load*.

13.1.5.3 If the load device is capable of producing a printed receipt, the information in Table 88, at a minimum must be provided to the cardholder

Table 88 - Cardholder Receipt Information

Field	Content
	Transaction type - Load
	Source of funds
$AUTHCODE_{FUNDS}$	Authorization code - for unlinked loads with a funding application
BAL_{CEP}	Slot balance after load
$ID_{ISS,CEP}$ & ID_{CEP}	CEP card number
$DTHR_{LDA}$	Transaction date and time
ID_{LACQ} & ID_{LDA}	Load Acquirer and load device identification
M_{LDA} & $CURR_{LDA}$	Transaction amount and currency

13.2 Exception Processing

If an error occurs during a load transaction, all participants in the transaction must be notified of the error. The financial liability must be adjusted to reflect the final results of the transaction.

The exception handling for linked loads and unlinked loads is different and is discussed in separate sections.

All script messages received from the card issuer must be sent to the CEP card even if exception processing is performed.

13.2.1 Linked Load

The load acquirer must notify the card issuer if an error occurs to allow card issuer processing to complete correctly. However, there is no financial liability between the load acquirer and the card issuer to be adjusted. The card issuer is responsible for all financial activity related to a linked load transaction.

13.2.1.1 If an error occurs prior to sending the S_1 to the card issuer:

- Normal processing of the transaction must be stopped.
- The cardholder must be informed that the transaction has been terminated.

13.2.1.2 If there is no response to the message sent to the card issuer containing the S_1:

- Normal processing of the transaction must be stopped.
- An attempt must be made to obtain a proof of transaction/no transaction from the CEP card. The following sequence of commands must be sent to the CEP card to get an S_3:

    1. Send a Credit for Load command with P2 = ‘80’

(no updates to be performed) to the CEP card.

2. If the response to the Credit for Load command is not SW1SW2 = ‘9000’, send another Credit for Load command with P2 = ‘80’ (no updates to be performed) to the CEP card.

3. If the response to the second Credit for Load command is not SW1SW2 = ‘9000’, send a Get Previous Signature command to the CEP card.

The Credit for Load command is described in section 13.1.4. The Get Previous Signature command is described in section 8.7.4.

If the response to a Credit for Load or Get Previous Signature command is SW1SW2 equal to ‘9000’, the response will contain an S_3 MAC. Otherwise, no S_3 will be available.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it is included in the message. The CC_{LACQ} in the message must be set to ‘0001’ (no valid response received from the card issuer).

- The cardholder must be informed that the transaction has been terminated.

13.2.1.3 If the card issuer declines a load request and the S_2 is not included in the response:

- Normal processing of the transaction must be stopped.

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing. If the card issuer included an advisory maximum balance ($BALmax_{ISS}$) that value may be used to restart the transaction with a lower amount.

13.2.1.4 If the card issuer declines a load request and the S_2 is include in the response:

- Normal processing of the transaction must be stopped.

- A Credit for Load command must be sent to the CEP card. P2 in the command is set to '81'. The format of the Credit for Load command is shown in Table 85. The format of the response to the Credit for Load command is shown in Table 86. The status conditions are in Table 87.

  If an error occurs during processing of this Credit for Load command, a transaction completion message without an S_3 must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. The CC_{LACQ} in the message must be set to '0002' (data update failed).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

13.2.1.5 If the card issuer approves an linked load request, then two error situations can occur:

1. A command unsuccessful response (SW1SW2 not equal to '9000' or SW1SW2 equal to '9000' and the first byte of CC_{TRX} b8 = 1) is received from the CEP card. In this case,

   - Normal processing of the transaction must be stopped.

   - A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it must be included in the message. The CC_{LACQ} in the message must be '0003' (error response from CEP card).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

2. If no response is received from the CEP card:

   - Normal processing of the transaction must be stopped.

   - An attempt must be made to get a proof of no transaction (S_3) from the CEP card. The following sequence of commands must be sent to the CEP card to get an S_3:

     – Resend the Credit for Load command without changes to the CEP card.

     – If the response to the Credit for Load command is SW1SW2 = '9580' (out of sequence), send a Get Previous Signature command to the CEP card.

     The Credit for Load command is described in section 13.1.4. The Get Previous Signature command is described in section 8.7.5.

     The response to a successful Credit for Load or Get Previous Signature command will contain an S_3 MAC. If the command was not successful or if the CEP card is no longer present, no S_3 will be available.

   - A transaction completion message (containing the S_3, if received from the CEP card) must be sent to the card issuer. See section 13.2.3 for a description of this processing. The CC_{LACQ} in the message must be set to '0003' (error response from CEP card) or '0004' (no response from the CEP card).

   - The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.2 for a

description of this processing.

13.2.2 Unlinked Load

In the case of unlinked loads, financial obligations occur between the load acquirer and the card issuer and, for non cash unlinked loads, between the load acquirer and the funds issuer. The final financial liability must reflect the final results of the transaction. The generation of R_1, R_{LSAM} and $R2_{LSAM}$ by the LSAM begins the process of controlling financial liability as the shared R_1 and shared SHA-1 hashes of R_{LSAM} and $R2_{LSAM}$ are used to establish the proof of a valid communication between the card issuer and the load acquirer and between the load acquirer and the CEP card. The load acquirer must ensure that once generated, R_1, R_{LSAM} and $R2_{LSAM}$ are used for only one transaction even if the transaction does not complete successfully.

13.2.2.1 If an error occurs prior to sending the S_1 to the card issuer:

- Normal processing of the transaction must be stopped.
- If the LSAM has generated R_1, R_{LSAM} and $R2_{LSAM}$, the load acquirer must ensure that these random numbers cannot be used for another transaction.
- The cardholder must be informed that the transaction has been terminated.

13.2.2.2 If there is no response to the message sent to the card issuer containing the S_1:

- Normal processing of the transaction must be stopped.
- An attempt must be made to obtain a proof of transaction/no transaction (S_3) from the CEP card. The $R2_{LSAM}$ must be obtained from the LSAM. After the LSAM has released $R2_{LSAM}$, all of the LSAM random numbers for the transaction (R_1, R_{LSAM} and $R2_{LSAM}$) must no longer be usable. The following sequence of commands must be sent to the CEP card to get an S_3:

1. Send a Credit for Load command with P2 = ‘80’ (no updates to be performed) to the CEP card.

2. If no response is received from the CEP card, send another Credit for Load command with P2 = ‘80’ (no updates to be performed) to the CEP card.

3. If the response to the second Credit for Load command is not SW1SW2 = ‘9000’, send a Get Previous Signature command to the CEP card.

The Credit for Load command is described in section 13.1.4. The Get Previous Signature command is described in section 8.7.4.

If the response to a Credit for Load or Get Previous Signature command is SW1SW2 equal to ‘9000’, the response will contain an S_3 MAC. Otherwise, no S_3 will be available.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it is included in the message. The $R2_{LSAM}$ generated by the LSAM for this error must be included in the message. The CC_{LACQ} in the message must be set to ‘0001’ (no valid response received from card issuer).

- No funds are due to the card issuer.

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

13.2.2.3 If the card issuer declines a load request and the S_2 is not included in the response:

- Normal processing of the transaction must be stopped.

- The load acquirer must ensure that the R_1, R_{LSAM}

and $R2_{LSAM}$, generated for the transaction, are not used for another transaction.

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing. If the card issuer included an advisory maximum balance ($BALmax_{ISS}$) that value may be used to restart the transaction with a lower amount.

- No funds are due the card issuer.

13.2.2.4 If the card issuer declines a load request and the S_2 is included in the response:

- Normal processing of the transaction must be stopped.

- The load acquirer must ensure that the R_1, R_{LSAM} and $R2_{LSAM}$, generated for the transaction, are not used for another transaction.

- A Credit for Load command must be sent to the CEP card. P2 in the command is set to '81'. The R_{LSAM} must not be released by the LSAM. The format of the Credit for Load command is shown in Table 85. The format of the response to the Credit for Load command is shown in Table 86. The status conditions are in Table 87.

  If an error occurs during processing of this Credit for Load command, a transaction completion message without an S_3 and without an $R2_{LSAM}$ must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. The CC_{LACQ} in the message must be set to '0002' (data update failed).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

- No funds are due the card issuer.

13.2.2.5 If the card issuer approves a load request but the application rejects it (SW1 SW2 equal to '9000' and the first byte of CC_{TRX} not equal to '00') and the R_{CEP} received in the response from the card validates correctly:

- Normal processing of the transaction must be stopped.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. The S_3 obtained from the CEP card in the response to the Credit for Load command must be included in the message. The CC_{LACQ} in the message must be set to '0003' (error response from CEP card).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

- No funds are due the card issuer.

13.2.2.6 If the card issuer approves a load request and

- a command unsuccessful response (SW1SW2 not equal to '9000' or SW1SW2 equal to '9000' and the first byte of CC_{TRX} not equal to '00') is received from the CEP card, and

- the 10 most significant bytes of the SHA-1 hash of the R_{CEP} received in the response from the card and other transaction data (see section 6.5.1.7) does not match the H_{CEP} received from the CEP card in the Initialize for Load response (if SW1 SW2 equal to '9000') or no R_{CEP} is returned by the CEP card (if SW1 SW2 not equal to '9000'), or if it is not possible to verify the R_{CEP},

the transaction must be considered successful. Funds are not returned to the cardholder and the card issuer is

due funds from the load acquirer.

A transaction completion message must be sent to the card issuer as notification of a suspect transaction. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it must be included in the message to the card issuer. The CC_{LACQ} in the message must be set to '0000' (transaction successful). The suspect transaction indicator in the message must be set on.

13.2.2.7 If the card issuer approves a load request and there is an interruption in processing[11] after the R_{LSAM} leaves the device containing the LSAM, the Credit for Load command must be resent, without changes, to the CEP card. Three situations can then occur:

1. If the response to the Credit for Load command received from the CEP card has an SW1SW2 = '9000', normal processing is resumed.

2. If no response is received from the CEP card or the response from the CEP card is not '9580' (Out of sequence), the transaction must be considered successful. Funds are not returned to the cardholder and the card issuer is due funds from the load acquirer.

   A transaction completion message must be sent to the card issuer as notification of a suspect transaction. Transaction completion messages are described in section 13.2.3. No S_3 will be obtained from the CEP card, to be included in the message. The CC_{LACQ} in the message must be set to '0000' (transaction successful). The suspect transaction indicator in the message must be set on.

3. If an SW1SW2 = '9580' (Out of sequence) is received from the CEP card, a Get Previous Signature command is sent to the CEP card.

[11] If the LSAM is at the load device, this interruption would be no response from the CEP card. If the LSAM is at the load acquirer host, this interruption would be no response from either the CEP card or the load device.

a) If a valid R_{CEP} is received from the Get Previous Signature command:

- Normal processing of the transaction must be stopped.
- A transaction completion message must be sent to the card issuer. The S_3 obtained from the CEP card must be included in the message. The CC_{LACQ} is set to '0003' (error response from the card).
- The cardholder must be informed that the transaction has been terminated.
- The card issuer is not due funds.

b) If a valid R_{CEP} is not received from the Get Previous Signature command, the transactions must be considered successful. Funds are not returned to the cardholder and the card issuer is due funds from the load acquirer.

A transaction completion message must be sent to the card issuer as notification of a suspect transaction. Transaction completion messages are described in section 13.2.3. If an S_3 is obtained from the CEP card, it must be included in the message. The CC_{LACQ} in the message must be set to '0000' (transaction successful). The suspect transaction indicator in the message must be set on.

13.2.2.8 If no response is received from the funds issuer and either (1) a load request message was not sent to the card issuer or (2) the card issuer declined the load request:

- Normal processing of the transaction must be stopped. Any exception processing specified in the funding application specifications must be followed.
- The cardholder must be informed that the transaction has been terminated and the reason for

the termination. See section 13.1.5 for a description of this processing.

13.2.2.9 If no response is received from the funds issuer and a load request message was sent to the card issuer and the card issuer did not decline the load request:

- Normal processing of the transaction must be stopped. Any exception processing specified in the funding application specifications must be followed.

- An attempt must be made to obtain a proof of transaction/no transaction (S_3) from the CEP card. The $R2_{LSAM}$ must be obtained from the LSAM. After $R2_{LSAM}$ is obtained from the LSAM, R_1, R_{LSAM} and $R2_{LSAM}$ must no longer be usable. The R_{LSAM} must not have been released by the LSAM before this point in the processing as $R2_{LSAM}$ must not be released if R_{LSAM} has been released. The following sequence of commands must be sent to the CEP card to get an S_3:

  1. Send a Credit for Load command with P2 = ‘80’ (no updates to be performed) to the CEP card.

  2. If no response is received from the CEP card, send another Credit for Load command with P2 = ‘80’ (no updates to be performed) to the CEP card.

  3. If the response to the second Credit for Load command is not SW1SW2 = ‘9000’, send a Get Previous Signature command to the CEP card.

  The Credit for Load command is described in section 13.1.4. The Get Previous Signature command is described in section 8.7.4.

  If the response to a Credit for Load or Get Previous Signature command is SW1SW2 equal to ‘9000’, the response will contain an S_3 MAC. Otherwise, no S_3 will be available.

- A reversal message must be sent to the funds issuer.

The minimum data to be sent in this message is listed in Table 89.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it must be included in the message. The $R2_{LSAM}$ generated by the LSAM for this error must be included in the message. The CC_{LACQ} in the message must be set to '0006' (no funds available for load).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

- The card issuer is not due any funds.

Table 89 - Minimum data to be Included in the Reversal Message to the Funds Issuer

Field	Contents	Length
	Indicator that this is a reversal of a CEP card load and the reason for the reversal	var
	Reversal data defined by the funding application	var

13.2.2.10 If the funds issuer declines a transaction and a load request message was not sent to the card issuer:

- Normal processing of the transaction must be stopped.

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

13.2.2.11 If the funds issuer declines a transaction and a load request message was sent to the card issuer:

- Normal processing of the transaction must be stopped.

- An attempt must be made to obtain a proof of transaction/no transaction (S_3) from the CEP card. The $R2_{LSAM}$ must be obtained from the LSAM. After $R2_{LSAM}$ is obtained from the LSAM, R_1, R_{LSAM} and $R2_{LSAM}$ must no longer be usable. The R_{LSAM} must not have been released by the LSAM before this point in the processing as $R2_{LSAM}$ must not be released if R_{LSAM} has been released. The following sequence of commands must be sent to the CEP card to get an S_3:

  1. Send a Credit for Load command with P2 = '80' (no updates to be performed) to the CEP card.

  2. If no response is received from the CEP card, send another Credit for Load command with P2 = '80' (no updates to be performed) to the CEP card.

  3. If the response to the second Credit for Load command is not SW1SW2 = '9000', send a Get Previous Signature command to the CEP card.

  The Credit for Load command is described in section 13.1.4. The Get Previous Signature command is described in section 8.7.4.

  If the response to a Credit for Load or Get Previous Signature command is SW1SW2 equal to '9000', the response will contain an S_3 MAC. Otherwise, no S_3 will be available.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 13.2.3. If an S_3 was obtained from the CEP card, it must be included in the message. The $R2_{LSAM}$ generated by the LSAM for this error must be included in the message. The CC_{LACQ} in the message must be set to '0006' (no funds available for load).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 13.1.5 for a description of this processing.

- The card issuer is not due any funds.

13.2.2.12 If an error occurs after an authorization request has been sent to a funds issuer and the card issuer is not due any funds, a reversal message must be sent to the funds issuer. The minimum data to be sent in this message is listed in Table 89**.**

13.2.2.13 If a load transaction does not complete successfully and the card issuer is not due any funds, any cash collected from the cardholder must be returned.

13.2.3 Transaction Completion Messages

Transaction completion messages are optional if a transaction completes normal processing. Transaction completion messages must be sent to the card issuer if any exception processing is performed after the S_1 is sent to the card issuer.

Transaction completion messages may be informational or they may have financial impact. All transaction completion messages for linked loads are informational. Transaction completion messages for unlinked load with a CC_{LACQ} of '0000' indicate that the card issuer is due funds for this transaction. The minimum data in a transaction completion message for a load transaction is shown in Table 90.

Table 90 - Minimum Data to be Included in a Transaction Completion Message to the Card Issuer for a Load Transaction

Field	Contents	Length
	Indicator that this is a transaction completion message	var
	Indicator - linked or unlinked load	var
AID_{CEP}	Identifier of the scheme	5-16
CC_{LACQ}	Status code from the load acquirer	2
CC_{TRX}	Status code from the CEP card	2
$CURR_{LDA}$	Currency	3
ID_{CEP}	CEP card identifier	6
$ID_{ISS,CEP}$	Identifier of the card issuer	4
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
M_{LDA}	Amount	4
NT_{CEP}	Transaction number	2
$R2_{LSAM}$	Random number generated by the LSAM - only present for unlinked loads where the LSAM did not release R_{LSAM} for inclusion in the Credit for Load command.	16
$REFNO_{ACQ,ISS}$	Acquirer identifier for the load request message	3
S_3	MAC from the CEP card (if available)	8
STI	Indicator of a suspect transaction	1

13.3 Additional Requirements for Unlinked Loads

13.3.1 Processing Requirements

13.3.1.1 The load acquirer must be able to be identified uniquely by the card issuer. Two possible methods to accomplish this are:

(1) The entity that first receives the load request uses the load acquirer identifier (ID_{LACQ}) in the load

request to retrieve the decryption key for R_1, and the decryption key retrieved is unique for the entity with financial responsibility and there is node to node identification of all entities between the load acquirer and the card issuer.

(2) Maintain the identifier for the load acquirer (ID_{LACQ}) in the LSAM for inclusion in the MAC computation.

13.3.1.2 The load acquirer must ensure that only one of the following events occur:

- The S_2 and R_{LSAM} are sent to the CEP card.
- An $R2_{LSAM}$ is sent to the card issuer.

13.3.1.3 R_1 must never leave the LSAM in the clear.

13.3.1.4 The load acquirer must ensure that the H_{CEP} used by the LSAM to verify the R_{CEP} from the CEP card are for the same transaction. The load acquirer must also ensure that each H_{CEP} is only used once.

13.3.2 LSAM Hardware and Software Requirements

The LSAM must be a security module as defined below. In addition, the LSAM must perform the cryptographic processing and transaction control as specified in this document. A software evaluation must be performed to guarantee the LSAM functions as described in this document.

Because of the variety of possible load environments and devices, the requirements do not specify where the LSAM must reside. Also, while a LSAM may be an ICC, the requirements allow for other implementations.

13.3.2.1 A LSAM must be a physically and logically protected hardware device that provides a secure set of cryptographic services.

13.3.2.2 All clear text keys must be physically protected against disclosure and unauthorized modification within a LSAM.

13.3.2.3 A LSAM must be tamper resistant. The intent of the tamper resistance is to protect designated information from unauthorized disclosure, use or modification by employing passive barriers. The LSAM must have a negligible probability of being successfully penetrated in such a was as to disclose all or part of any cryptographic material, keys, or other data. It must be protected by being tamper resistant to such a degree that its passive resistance is sufficient to make penetration infeasible both in its intended environment and when taken to a specialized facility with specialized equipment.

13.3.2.4 Controls must be in place to ensure that equipment is not re-installed after a suspicious alteration of a key in a LSAM has been detected until the LSAM has been inspected and a reasonable degree of assurance has been reached that the LSAM has not been subject to unauthorized physical or functional modification.

13.3.2.5 LSAMs must be designed in such a way to prevent state of the art monitoring attacks, such as radiation tapping, covered channel analysis, etc. known at the time of certification.

13.3.2.6 Each LSAM must be uniquely identifiable within a scheme.

13.3.2.7 Based on a combination of adequate control procedures during the production process and special features available through design , it must be ensured at initial key loading that a LSAM is authentic, corresponds to a certified construction and is loaded with a certified program.

13.3.2.8 Subsequent down-loading of program updates must only take place after origin authentication.

14. Load Acquirer Processing - Currency Exchange Transaction

Currency exchange changes value from one currency of the CEP card into value in another currency. All or part of the value in a slot may be changed to another currency. If the new (target) currency already occupies a slot in the CEP card, the new value will be added to that slot. If the new currency does not already exist in the CEP card, a slot will be assigned. If the entire value in the former (source) currency is exchanged, the source slot may be assigned for the new currency.

If the amount in the source slot is not being exchanged in its entirety, and the new (target) currency does not already exist in the purse, and there is no empty slot available to be assigned, then the currency exchange cannot be performed.

If a slot contains a zero balance ($BAL_{CEP} = 0$), the slot can be available for assigning to a new currency.

Currency exchange is performed at a load device, and is always on-line to the card issuer.

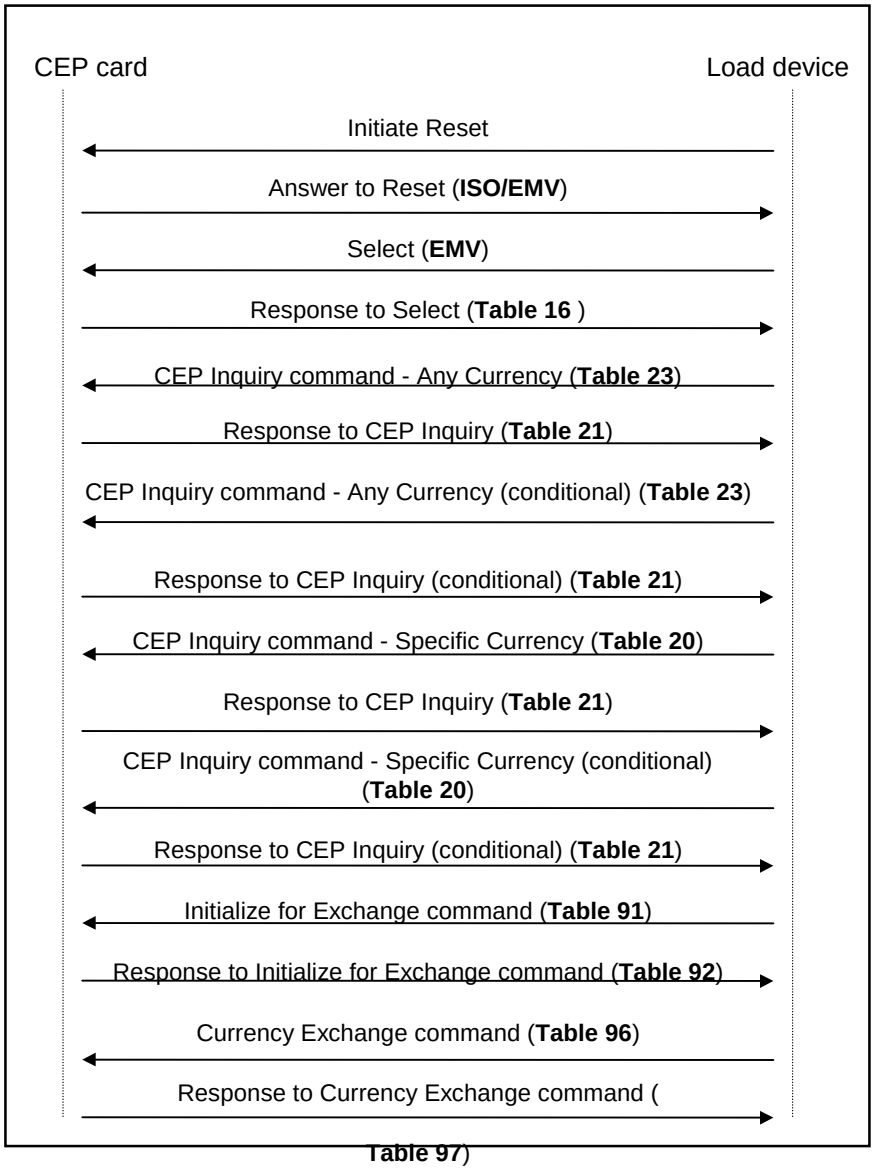
The currency exchange of a small amount of one currency may result in a zero amount in the new currency because of processing fees.

Currency exchange transactions use two commands: Initialize for Exchange and Currency Exchange. The Currency Exchange command must be preceded by a successful Initialize for Exchange command.

At the completion of each successful Currency Exchange command, the CEP card must update its internal transaction log.

The flow in Figure 14 shows an interaction between the load device and the CEP card for currency exchange processing. Other flows are possible as long as the requirements in this specifications are met.

Figure 14 - Currency Exchange Processing



14.1 Normal Processing

14.1.1 Initiate Transaction

The initiate transaction processing consists of:

- Application selection.

- Determination of the currencies to be used for the transaction.

- The Initialize for Exchange command.

14.1.1.1 If the CEP card has not been reset after being inserted in the load device or if the CEP application has not been selected, the processing described in section 8.5 must occur.

14.1.1.2 If the application profile (AP_{CEP}) on the CEP card indicates that currency exchange is not supported, normal processing of the transaction must be stopped and exception processing followed.

14.1.1.3 The load device must use the CEP Inquiry command described in section 8.7.1 to determine the balances and maximum balances for the currencies applicable to this transaction. For source currencies, the CEP Inquiry - Any Currency command must be used. For target currencies, the CEP Inquiry - Specific Currency command must be used.

14.1.1.4 If the load device supports multiple currencies, the cardholder must be allowed to select the target currency. If the CEP card contains slots with multiple currencies having a balance greater than zero, the card holder must be allowed to select the source currency.

14.1.1.5 The cardholder must be allowed to select the amount of the source currency to be exchanged.

14.1.1.6 The load device must send an Initialize for Exchange command to the CEP card to begin the currency exchange process. The format of this command is in Table 91. The format of the response is in Table 92. The error status conditions for the command are in Table 93.

Table 91 - Format of the Initialize for Exchange Command

Field	Content	Length
CLA	'90'	1
INS	'50'	1
P1	'03'	1
P2	'00'	1
Lc	Length of command data	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
$DTHR_{LDA}$	Transaction date and time	5
$CURR_{SOURCE}$	Currency of the source slot	3
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
M_{LDA}	Amount to be converted, in source currency	4
$CURR_{TARGET}$	Currency of the target slot	3
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 92 - Response to Initialize for Exchange

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
$ID_{ISS,CEP}$	Issuer ID	4
ID_{CEP}	Card identifier	6
$DEXP_{CEP}$	Expiration Date	3
NT_{CEP}	Transaction Number	2
L_{DD}	Length of discretionary data	1
DD_{CEP}	Discretionary data - it is strongly recommended that DD_{CEP} include $NT_{LASTLOAD}$, $NT_{LASTCANCEL}$, S_1	0-32
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 93 - Status Conditions for Initialize for Exchange

SW1	SW2	Meaning
'91'	'02'	Transaction counter has reached its limit
'94'	'03'	Exchange amount too high
'94'	'06'	No slot available
'94'	'20'	Source currency does not exist

14.1.1.7 The load acquirer must not terminate the transaction based on the expiration date($DEXP_{CEP}$) returned in the response to the Initialize for Exchange command.

14.1.1.8 The load acquirer must log the minimum required data received from the load device and a unique acquirer generated identification number (REFNO) for this transaction.

14.1.2 Communicate with Card Issuer

The communicate with card issuer process consists of:

- Sending the currency exchange request to the card issuer.
- Receiving a response from the card issuer.

14.1.2.1 After the currency exchange request has been logged, the load acquirer will communicate with the card issuer. The minimum information to be sent to the card issuer is listed in Table 94.

Table 94 - Minimum Data Elements Sent to the Card Issuer by the Load Acquirer for a Currency Exchange Transaction

Field	Content	Length
	Indicator that this is a currency exchange request	var
AID_{CEP}	Scheme identifier	5 - 16
$BALmax_{TARGET}$	Maximum balance of the target slot prior to the exchange (0 if new currency).	4
BAL_{SOURCE}	Balance of the source slot prior to the exchange	4
BAL_{TARGET}	Balance of the target slot prior to the exchange (0 if new currency)	4
$CNTRY_{LDA}$	Country of the load device	2
$CURR_{SOURCE}$	Currency of the source slot	3
$CURR_{TARGET}$	Target currency	3
DD_{CEP}	Discretionary data from the CEP card	0-32
DD_{SCHEME}	Discretionary data for the scheme	0-20
$DEXP_{CEP}$	Expiration date	3
DOM_{LDA}	Domain of the load device	1
$DTHR_{LDA}$	Transaction date and time	5
ID_{CEP}	Card identifier	6
$ID_{ISS,CEP}$	Issuer ID	4
ID_{LACQ}	Identifier of the load acquirer	4

ID_{LDA}	Identifier of the load device	6
M_{SOURCE}	Amount to be converted from the source slot	4
NT_{CEP}	Transaction Number	2
$REFNO_{ACQ,ISS}$	Acquirer id for this transaction	3

14.1.2.2 The minimum information received from the card issuer for approved transactions is listed in Table 95. If the transaction is not approved, the items marked as "optional for declines" may not be present. If a transaction is not approved by the issuer, exception processing (see section 14.2) is followed.

Table 95 - Minimum Data Elements Received from the Card Issuer on a Currency Exchange Transaction

Field	Content	Length
CC_{ISS}	Response code	2
DD_{ISS}	Discretionary data from issuer - optional for declines - it is strongly recommended that DD_{ISS} include BAL_{SOURCE}, BAL_{TARGET}, S_2. If a new currency is being established, $BALmax_{TARGET}$, and $CALPHA_{TARGET}$ must be included.	0-64
ID_{CEP}	Card number	4
$ID_{ISS,CEP}$	Issuer ID	4
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
$Mmax_{ISS}$	An optional exchange amount sent as an advice to the load acquirer by the card issuer, if the amount to be exchanged (in the source currency) plus the current balance of the target slot (if there is one) is greater than the maximum balance the card issuer will allow for the target currency. This field is only present for declines.	4
$REFNO_{ACQ,ISS}$	Acquirer id for this transaction	3

14.1.3 Exchange Currencies on CEP card

The exchange currencies process consists of:

- Processing of script messages from the card issuer.
- The Currency Exchange command.
- Notification of the cardholder of the results of the currency exchange transaction.

This section will only be performed for approved transactions. If the card issuer declines a request, exception processing must be followed.

14.1.3.1 The load device must examine the response received from the card issuer to see if it contains any script messages. Any script message beginning with tag '71' must be sent immediately to the CEP card. The format and processing of script messages is in reference 8, EMV.

14.1.3.2 The load device sends a Currency Exchange command to the card. The format of the Currency Exchange command is shown in Table 96. The format of the response to the Currency Exchange command is shown in Table 97. Status conditions are in Table 98.

Table 96 - Format of the Currency Exchange Command

Field	Content	Length
CLA	'90'	1
INS	'56'	1
P1	'00'	1
P2	'00'	1
Lc	Command data length	1
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, L_{DD}.	1
CC_{ISS}	Status from the card issuer - (fill with 'FFFF' if no response from the card issuer)	2
L_{DD}	Length of discretionary data	1
DD_{ISS}	Discretionary data from issuer - optional for declines	0-64
PDATA	Proprietary implementation data	var
Le	'00'	1

Table 97 - Currency Exchange Response Format

Field	Content	Length
L_{CEPS}	The length of the CEPS data that follows. From the byte immediately following this length field to, but not including, PDATA.	1
CC_{TRX}	Completion code	2
S_3	Signature of the CEP	8
$BAL_{CEP,SOURCE}$	Slot balance after currency exchange	4
$BAL_{CEP,TARGET}$	Slot balance after currency exchange	4
PDATA	Proprietary implementation data	var
SW1 SW2	Status bytes	2

Table 98 - Status Conditions for Currency Exchange Command

SW1	SW2	Meaning
'94'	'04'	Value out of range
'95'	'80'	Command out of sequence (currency exchange not allowed)

14.1.3.3 Any script commands received from the card issuer beginning with tag '72' must be sent to the CEP application after the Currency Exchange command is completed. The format and processing of script messages is in reference 8, EMV.

14.1.3.4 If the transaction was successful, a transaction completion message may be sent to the card issuer. The format of the transaction completion message is in *Table 100 - Minimum Data to be Included in an Transaction Completion Message to the Card Issuer for a Currency Exchange Transaction*.

14.1.3.5 The information in the completion message is combined with the information already logged to create the final log for the transaction. A log of all currency exchange transactions must be maintained by the load acquirer, regardless of completion status, for the period of time defined by the scheme provider.

14.1.3.6 If the transaction was not successful, the exception processing in section 14.2 must be performed.

14.1.4 Notification to Cardholder

14.1.4.1 The load device must notify the cardholder of the results of the transaction.

14.1.4.2 If CC_{ISS} is not equal to zero, this must be treated as an error situation and the cardholder notified of the specific error. These error conditions are listed in *Table 104 - Issuer Validations for Currency Exchange.*

14.1.4.3 If the load device is capable of producing a printed receipt, the information in Table 99, at a minimum must

be provided to the cardholder.

Table 99 - Cardholder Receipt Information

Field	Content
	Transaction type - Currency Exchange
$BAL_{CEP,SOURCE}$	New slot balance for source currency
$BAL_{CEP,TARGET}$	New slot balance for target currency
$ID_{ISS,CEP}$ & ID_{CEP}	CEP card number
$DTHR_{LDA}$	Transaction date and time
ID_{LACQ} & ID_{LDA}	Load acquirer and load device Identification
M_{LDA} & $CURR_{LDA}$	Source transaction amount and currency

14.2 Exception Processing

14.2.1 Exception Conditions

The load acquirer must notify the card issuer if an error occurs to allow card issuer processing to complete correctly. However, there is no financial liability between the load acquirer and the card issuer to be adjusted. The card issuer is responsible for all financial activity related to a currency exchange transaction.

All script messages received from the card issuer must be sent to the CEP card even if exception processing is performed.

14.2.1.1 If an error occurs prior to sending the request to the card issuer:

- Normal processing of the transaction must be stopped.
- The cardholder must be informed that the transaction has been terminated.

14.2.1.2 If there is no response to the message sent to the card issuer:

- Normal processing of the transaction must be stopped.

- An attempt must be made to get a proof of no transaction (S_3) from the CEP card. The following sequence of commands must be sent to the CEP card to get an S_3:

  1. Send a Currency Exchange command to the CEP card. CC_{ISS} must be equal to 'FFFF'.

  2. If there is no response from the CEP card, send another Currency Exchange command to the CEP card. CC_{ISS} must be equal to 'FFFF'.

  3. If the response to the second Currency Exchange command is not SW1SW2 = '9000', send a Get Previous Signature command to the CEP card.

  The Currency Exchange command is described in section 14.1.3. The Get Previous Signature command is described in section 8.7.5.

  The response to a successful command will contain an S_3 MAC. If the command was not successful or if the CEP card is no longer present, no S_3 will be available.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 14.2.2. If an S_3 was obtained from the CEP card, it must be included in the message. The CC_{LACQ} must be set to '0001' (no valid response received from the card issuer).

- The cardholder must be informed that the transaction has been terminated.

14.2.1.3 If the card issuer declines a currency exchange request and there is no DD_{ISS} field included in the response :

- Normal processing of the transaction must be stopped.

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 14.1.4 for a description of this processing. If the card issuer included an advisory maximum exchange limit ($Mmax_{ISS}$) that value may be used to restart the transaction with a lower amount.

14.2.1.4 If the card issuer declines a currency exchange request and there is a DD_{ISS} field included in the response:

- Normal processing of the transaction must be stopped.

- A Currency Exchange command must be sent to the CEP card. The format of the Currency Exchange command is shown in Table 96. The format of the response to the Currency Exchange command is shown in

- Table 97. The status conditions are in Table 98.

  If an error occurs during processing of this Currency Exchange command, a transaction completion message without an S_3 must be sent to the card issuer. Transaction completion messages are described in section 14.2.2. The CC_{LACQ} in the message must be set to '0002' (data update failed).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 14.1.4 for a description of this processing.

14.2.1.5 If the card issuer approves a currency exchange request, then two error situations can occur:

1. A command unsuccessful response (SW1SW2 not equal to '9000' or SW1SW2 equal to '9000' and the first byte of CC_{TRX} not equal to '00') is received from the CEP card. In this case,

   - Normal processing of the transaction must be stopped.

- A transaction completion message must be sent to the card issuer. Transaction completion messages are described in section 14.2.2. If an S_3 was obtained from the CEP card, it must be included in the message. The CC_{LACQ} in the message must be '0003' (error response from CEP card).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 14.1.4 for a description of this processing.

3. If no response is received from the CEP card:

   - Normal processing of the transaction must be stopped.

   - An attempt must be made to get a proof of no transaction (S_3) from the CEP card. The following sequence of commands must be sent to the CEP card to get an S_3:

     – Resend the Currency Exchange command without changes to the CEP card.

     – If the response to the Currency Exchange command is SW1SW2 = '9580' (out of sequence), send a Get Previous Signature command to the CEP card.

     The Currency Exchange command is described in section 14.1.3. The Get Previous Signature command is described in section 8.7.5.

     The response to a successful Currency Exchange or Get Previous Signature command will contain an S_3 MAC. If the command was not successful or if the CEP card is no longer present, no S_3 will be available.

   - A transaction completion message (containing the S_3, if received from the CEP card) must be sent to the card issuer. See section 14.2.2 for a

description of this processing. The CC_{LACQ} in the message must be set to '0004' (no response from the CEP card).

- The cardholder must be informed that the transaction has been terminated and the reason for the termination. See section 14.1.4 for a description of this processing.

14.2.2 Transaction Completion Messages

Transaction completion messages are optional if a transaction completes normal processing. Transaction completion messages must be sent to the card issuer if any exception processing is performed after the S_1 is sent to the card issuer.

All transaction completion messages for currency exchanges transactions are informational. The minimum information to be included in a transaction completion message for a currency exchange transaction is shown in Table 100.

Table 100 - Minimum Data to be Included in an Transaction Completion Message to the Card Issuer for a Currency Exchange Transaction

Field	Content	Length
	Indicator that this is a transaction completion message	var
	Indicator - currency exchange	var
AID_{CEP}	Identifier of the scheme	5-16
CC_{TRX}	Status code from the CEP card	2
CC_{LACQ}	Status code from the load acquirer	2
$CURR_{SOURCE}$	Source currency	3
$CURR_{TARGET}$	Target currency	3
ID_{CEP}	CEP card identifier	6
$ID_{ISS,CEP}$	Identifier of the card issuer	4
ID_{LACQ}	Identifier of the load acquirer	4
ID_{LDA}	Identifier of the load device	6
M_{LDA}	Amount - in source currency	4
NT_{CEP}	Transaction number	2
$REFNO_{ACQ,ISS}$	Acquirer identifier for the currency exchange request message	3
S_3	MAC from the CEP card (if available)	8

15. Funds Issuer Processing

15.1 Unlinked Load Transactions

15.1.1 Normal Processing

15.1.1.1 A funds issuer will receive funds authorization request messages from the load acquirer. The information received from the load acquirer will contain an indication that this is a CEP load request. The other information received from the load acquirer is defined by the funding application.

15.1.1.2 The funds issuer will log the funds authorization request.

15.1.1.3 The funds issuer will perform its normal processing for a funds authorization request and respond to the load acquirer. The information to be sent to the load acquirer is defined by the funding application.

15.1.1.4 The funds issuer will participate in settlement with the load acquirer.

15.1.2 Exception Processing

15.1.2.1 A funds issuer may receive funds authorization reversal messages from the load acquirer host. The minimum data contained in that reversal is listed in *Table 89 - Minimum data to be Included in the Reversal Message to the* Funds Issuer.

15.1.2.2 The funds issuer will log the funds authorization reversal.

15.1.2.3 The funds issuer will perform its normal processing for a funds authorization reversal.

16. Card Issuer Processing

16.1 Administrative Processing

16.1.1 Card Management

Table 101 identifies the principle CEP card application options that are available to card issuers.

Table 101 - CEP Card Application Options

Option	Card Issuer
Number of slots supported	Card issuer option
Currencies supported	Card issuer option
Maximum balance per currency	Card issuer option
Expiration date for transactions	Card issuer option
Number of certificates used/ use of regional public key	Required to follow scheme rules
CEP application lock/ unlock	Card issuer option
Aggregation of POS transactions	If the scheme supports aggregation, the card issuer must ensure that the CEP card sets the CPO appropriately.
Cancel Last Purchase	Card issuer option
Currency Exchange support	Card issuer option, but if multiple currencies are supported, either currency exchange or unload must be supported.
Unload supported	Card issuer option, but if multiple currencies are supported, either currency exchange or unload must be available.
Inclusion of funding account number in CEP card	Card issuer option
Types of load supported: unlinked, linked or both	Card issuer option
Authentication method supported	Card issuer option
Discretionary data processing	Card issuer option, following scheme guidelines

16.1.2 Key Management

During the card personalization process, the data elements containing card private keys and CA public keys are created and stored in the non-volatile memory of the ICC. The card issuer must adhere to the following requirements for managing these keys and certificates.

16.1.2.1 An RSA key pair must be generated for use as the issuer key. The key must have a minimum modulus length of 896 bits and a public key exponent of either 2, 3 or $2^{16}+1$. The private key portion must never appear in unencrypted form outside of a secure module.

16.1.2.2 If a regional certifying authority is in use, a certificate must be obtained for the issuer public key signed by the regional certifying authority private key.

16.1.2.3 If no regional certifying authority is in use, a certificate must be obtained for the issuer public key signed by each of the certifying authority private keys designated by the schemes with which the card issuer has a relationship.

16.1.2.4 An RSA key pair must be generated for each CEP card. The key must have a modulus length greater than or equal to 768 bits and a public exponent of either 3 or $2^{16}+1$.

The CEP card private key must never appear in unencrypted form outside of a secure module.

16.1.2.5 Each CEP card must be personalized with the CEP card private key in a secure manner. It must not be possible to retrieve this key from the CEP card, nor to alter this key after the CEP card has been personalized.

16.1.2.6 A CEP card public key certificate must be generated signed by the issuer private key.

16.1.2.7 A symmetric key for each CEP card must be generated for use in generating and verifying the S_6 MAC. This key must never appear in unencrypted form outside of a

secure module.

The CEP card must be personalized with the symmetric MAC key. It must not be possible to retrieve this key from the CEP card. This key may be updated only if the updates can be sent to the CEP card encrypted and MACed.

16.1.2.8 A secret key must never appear in unencrypted form outside of the CEP card or other secure module.

16.1.2.9 The card issuer must ensure that all CEP card keys are placed onto the CEP card in a secure manner.

16.1.2.10 The card issuer must generate keys to be provided to card suppliers and card personalizers to ensure the security of un-personalized CEP cards and CEP card secret data during transport.

16.2 Load Transactions

This section describes the minimum specifications for card issuer processing for load transactions.

16.2.1 Normal Processing

16.2.1.1 The card issuer receives a load request from the load acquirer. The minimum data contained in that request is listed in *Table 83 - Minimum Data Elements Sent to the Card Issuer for a Load Transaction*.

16.2.1.2 The card issuer must log all load requests.

16.2.1.3 The card issuer must perform any required currency conversion for a linked load. The card issuer must follow network rules for currency conversion for an unlinked load.

16.2.1.4 The card issuer must validate the data received from the load acquirer. Table 102 shows the validations that are required and the value that CC_{ISS} must be set to if there is an error.

Table 102 - Issuer Validations for Load

Field	Validation required	CC_{ISS} if error	Cardholder Notification Required
$ID_{ISS,CEP}$ and ID_{CEP}	Must be an identifier of a card issued by the card issuer	'0001	No
$CURR_{LDA}$	Must be a currency supported by the card issuer	'0002'	Yes
$DEXP_{CEP}$	Must not be an expired CEP card	'0003'	Yes
	Must be a valid account and account type for this cardholder	'0004	Yes
	Funding account must have sufficient funds for load request (Linked load only.)	'0005'	Yes
S_1	Card MAC must be valid	'0006'	No
PIN Block	On-line PINs must be valid. (Linked load only.)	'0007'	Yes
AID_{CEP}	Must be a scheme supported by the card issuer	'0008'	Yes
M_{LDA}	Amount to be load exceeds maximum balance - this will usually occur when a new currency is being loaded and no maximum balance has been established	'0009'	Yes
MAC_{LSAM}	Invalid LSAM MAC (unlinked load only)	'000A'	No
	other errors	'00FA'	No

16.2.1.5 For a linked load, the card issuer must verify that the account is a valid account and that funds are available in the account for the amount of the requested load amount.

16.2.1.6 The card issuer must create an R_{CEP} that is the same as the R_{CEP} generated by the CEP card for this transaction. The definition of R_{CEP} is a card issuer responsibility, but R_{CEP} must be unique for each transaction and must be used to verify the MAC_{LSAM}.

16.2.1.7 The card issuer must validate the S_1 MAC and generate an S_2 MAC. Except as noted below, the definition of the contents of these MACs is a card issuer responsibility. Table 103 provides a list of the

recommended data elements for these MACs. The recommended data elements for the S_3 MAC, which the card will generate after a successful load, is also included in this table for completeness.

16.2.1.8 The data elements marked with an M (mandatory) in Table 103 must be included in the S_2 MAC under certain conditions. See section 18.1.100 for a description of these conditions.

Table 103 - Data Elements for Load Signatures

	Contents	Length	S1	S2	S3
BAL_{CEP} - prior to transaction	Balance of the slot prior to completion	4	√		
BAL_{CEP} –after transaction	Balance of the slot after completion	4		√	√
$BALMAX_{CEP}$ - after transaction	Maximum balance of the slot after completion	4		√	√
$BALMAX_{CEP}$ - prior to transaction	Maximum balance of the slot prior to completion	4	√		
CC_{ISS}	Completion code	2		M	
CC_{TRX}	Transaction Completion code	2			√
$CURR_{LDA}$	Currency	3	√		√
DD_{CEP}	Discretionary data (Initialize for Load response)	0-32	√		√
DD_{ISS}	Discretionary Data (Credit for Load command)	0-64		√	
$DEXP_{CEP}$	Transaction Expiration Date	3	√		
$DTHR_{LDA}$	Transaction Date and time	5	√		√
ID_{CEP}	Identifier of the CEP card	6	√	√	√
$ID_{ISS,CEP}$	Identifier of the card issuer	4	√	√	√
ID_{LACQ}	Load Acquirer Identifier	4	√		√
ID_{LDA}	Load device Identifier	6	√		√

M_{LDA}	Transaction amount	4	√		√
NT_{CEP}	Transaction number CEP	2	√	√[12]	√
S_1	Card MAC	8		√	
S_2	Card issuer MAC	8			
S_3	Final card MAC	8			
H_{LSAM}	8 most significant bytes of a SHA-1 hash of transaction data, including a random number (R_{LSAM}) generated by the LSAM	8		M	
TI_{CEP}	Transaction Indicator	1	√	√	√

16.2.1.9 If the off-line PIN verification for a linked load was not successful because the PIN had been blocked, the card issuer must decline the transaction with a CC_{ISS} of '0007'. The PIN verification status in DD_{CEP} must indicate this condition. The card issuer may use the response message to unblock the PIN.

16.2.1.10 The card issuer must determine if a new $BALmax_{CEP}$ is required. If the $BALmax_{CEP}$ is zero, the $BALmax_{CEP}$ must be established. If the $BALmax_{CEP}$ is not zero, the issuer may establish a new $BALmax_{CEP}$. The new $BALmax_{CEP}$ must be greater or equal to the current balance on the card (BAL_{CEP}) plus the amount to be loaded (M_{LDA}).

16.2.1.11 If the amount to be loaded (M_{LDA}) plus the current balance on the card (BAL_{CEP}) is greater than the card issuer determined BALmax, the card issuer may decline the transaction with an CC_{ISS} of '0009' and, optionally, send an advisory $BALmax_{ISS}$ in the response to the load acquirer. No S_2 should be sent in the response. If the card issuer does not decline the transaction, a new $BALmax_{CEP}$ and an S_2 must be include in the response.

[12] If the NT_{CEP} is not included in the S_1 or if the S_1 is not included in the S_2, then NT_{CEP} must be included in the S2 to prevent replay.

16.2.1.12 A new alphabetic currency code (CALPHA) must be established for a new currency. A new alphabetic currency code (CALPHA) may be established for an existing currency.

16.2.1.13 If this is an unlinked load, the card issuer must

- Recover the random number (R_1).
- Validate the MAC_{LSAM} by encrypting the data elements listed in *Table 82 - Data Elements in the MAC of an Unlinked Load* using the random number (R_1) as the MAC key and comparing the results to the value received from the load acquirer. If the MAC_{LSAM} is invalid, the request must be declined with an CC_{ISS} of '000A'

The cryptography for MACs is described in section 6.5.

16.2.1.14 Script messages may be included in the response to the load acquirer. The formatting of the script message is described in reference 8, EMV.

16.2.1.15 The card issuer must format a message to be sent back to the load acquirer and log that message. The minimum data elements to be included in that message are listed in *Table 84 - Minimum Data Elements Sent by the Card Issuer to the Load Acquirer on a Load Transaction.*

16.2.1.16 The card issuer must participate in settlement with the load acquirer for unlinked loads and must update its funds pools and reporting with the additional liability incurred with the completed load.

16.2.1.17 Card history must be updated by the card issuer. All transactions that affect card balance and liability change must be retained by a card issuer for the period defined by the scheme provider.

16.2.2 Exception Processing

16.2.2.1 If the card issuer declines the transaction, the response code in the message to the load acquirer must indicate

that the transaction has been declined by setting the value of CC_{ISS} to the value specified in *Table 102 - Issuer Validations for Load*. The minimum data in the message to the load acquirer is in *Table 84 - Minimum Data Elements Sent by the Card Issuer to the Load Acquirer on a Load Transaction*.

16.2.2.2 The card issuer may decline a transaction and include updates to the CEP in the decline message.

16.2.2.3 The card issuer may receive transaction completion messages (see *Table 90 - Minimum Data to be Included in a Transaction Completion Message to the* Card Issuer) with either an error status code (CC_{LACQ} not equal to '0000') or the suspect transaction indicator set on.

If the transaction is marked as successful (CC_{LACQ} equal to '0000') and the suspect transaction indicator is on, the card issuer is responsible for resolving the matter. If the cardholder is due funds, it is the responsibility of the card issuer to return the funds to the cardholder.

The next transaction for this CEP card should contain the $NT_{LASTLOAD}$ of the last successful load. This will allow the card issuer to resolve any suspect transactions.

16.2.2.4 If a card issuer receives a transaction completion message with a an invalid S_3 for any load transaction or a transaction completion message with a bad $R2_{LSAM}$ for an unlinked load transaction, the error should be resolved through the scheme provider's dispute resolution process. The $R2_{LSAM}$ can be validated by computing an SHA-1 hash of the $R2_{LSAM}$ in the transaction completion message and other transaction data (see section 6.5.1.7) and comparing the 8 most significant bytes of the computed hash to the $H2_{LSAM}$ received in the load request message.

16.3 Currency Exchange Transactions

This section describes the minimum specifications for card issuer processing for currency exchange transactions.

16.3.1 Normal Processing

16.3.1.1 The card issuer receives a currency exchange request from the load acquirer. The minimum data contained in that request is listed in *Table 94 - Minimum Data Elements Sent to the Card Issuer by the Load Acquirer for a Currency Exchange Transaction*

16.3.1.2 The card issuer must log all currency exchange requests.

16.3.1.3 The card issuer must validate the data received from the load acquirer. Table 104 shows the validations that are required.

Table 104 - Issuer Validations for Currency Exchange

Field	Validation required	CC_{ISS} if error	Cardholder Notification Required
$ID_{ISS,CEP}$ and ID_{CEP}	must be an identifier of a card issued by the card issuer	'0051'	No
$CURR_{SOURCE}$	must be a currency supported by the card issuer	'0052'	No
$CURR_{TARGET}$	must be a currency supported by the card issuer	'0053'	Yes
AID_{CEP}	must be a scheme supported by the card issuer	'0054'	No
S_1	Card MAC must be valid	'0056'	No
M_{SOURCE}	Amount to be converted exceeds maximum balance	'0057'	Yes
	other error	'00FA'	No

16.3.1.4 The card issuer must validate the S_1 MAC and generate an S_2 MAC. The definition of the contents of these MACs is a card issuer responsibility. Table 105 provides the recommended contents of the S_1 and S_3 MACs generated by the CEP card and the S_2 MAC generated by the card issuer.

Table 105 - Data Elements for Currency Exchange Signatures

	Contents	Length	S1	S2	S3
$BAL_{CEP,SOURCE}$ - prior to transaction	Balance of the source slot prior to completion	4	√		
$BAL_{CEP,SOURCE}$ -after transaction	Balance of the source slot after completion	4		√	√
$BAL_{CEP,TARGET}$ – after transaction	Balance of the target slot after completion	4		√	√
$BAL_{CEP,TARGET}$ - prior to transaction	Balance of the target slot prior to completion	4	√		
$BALmax_{CEP,TARGET}$ – after transaction	Maximum balance of the target slot after completion	4		√	√
$BALMAX_{CEP,TARGET}$ - prior to transaction	Maximum balance of the target slot prior to completion	4	√		
CC_{ISS}	Completion code	2		√	
CC_{TRX}	Transaction Completion code	2			√
$CURR_{LDA,SOURCE}$	Currency of source slot	3	√		√
$CURR_{LDA,TARGET}$	Currency of target slot	3	√		√
DD_{CEP}	Discretionary data (Initialize for Exchange response)	0-32	√		√
DD_{ISS}	Discretionary Data (Currency Exchange command)	0-64		√	
$DEXP_{CEP}$	Transaction expiration date	1	√		
$DTHR_{LDA}$	Transaction Date and time	5	√		√
ID_{CEP}	Identifier of the CEP card	6	√		√
$ID_{ISS,CEP}$	Identifier of the card issuer	4	√		√
ID_{LACQ}	Load Acquirer Identifier	4	√		√
ID_{LDA}	Load device Identifier	6	√		√
M_{LDA}	Transaction amount	4	√		√
NT_{CEP}	Transaction number CEP	2	√		√
S_1	Card MAC	8		√	

TI_{CEP}	Transaction Indicator		√	√	√

16.3.1.5 The card issuer must perform the currency conversion for a currency exchange.

16.3.1.6 The card issuer must determine if a new $BALmax_{TARGET}$ is required. If the $BALmax_{TARGET}$ is zero, the $BALmax_{TARGET}$ must be established. If the $BALmax_{TARGET}$ is not zero, the issuer may establish a new $BALmax_{TARGET}$. The new $BALmax_{TARGET}$ must be greater to or equal than the current balance on the card (BAL_{TARGET}) plus the amount to be exchanged (M_{SOURCE} converted to target currency).

16.3.1.7 If the amount to be exchanged (M_{SOURCE} converted to target currency) plus the current balance on the card (BAL_{TARGET}) is greater than the card issuer determined BALmax, the card issuer may decline the transaction with an CC_{ISS} of '0057' and, optionally, send an advisory $Mmax_{ISS}$ in the response to the load acquirer. No DD_{ISS} should be sent in the response. If the card issuer does not decline the transaction, a new $BALmax_{TARGET}$ and an DD_{ISS} must be included in the response.

16.3.1.8 A new alphabetic currency code (CALPHA) must be established for a new currency. A new alphabetic currency code (CALPHA) may be established for an existing currency.

16.3.1.9 The card issuer must update the source and target funds pools and update card history with the results of this transaction.

16.3.1.10 Script messages may be included in the response to the load acquirer. The formatting of the script message is described in reference 8, EMV.

16.3.1.11 The card issuer must format a message to be sent back to the load acquirer and log that message. The minimum data elements to be included in that message are listed in *Table 95 - Minimum Data Elements Received from the Card Issuer on a Currency Exchange*

Transaction.

16.3.2 Exception Processing

16.3.2.1 If the card issuer does not approve the transaction, the response code in the message to the load acquirer will indicate that the transaction has been declined by setting the value of CC_{ISS} to the value specified in Table 104. The format of the message to the load acquirer is in *Table 95 - Minimum Data Elements Received from the Card Issuer on a Currency Exchange Transaction.*

16.3.2.2 The card issuer may decline a transaction and include updates to the CEP in the decline message.

16.3.2.3 The card issuer may receive transaction completion messages (see *Table 100 - Minimum Data to be Included in an Transaction Completion Message to the Card Issuer for a Currency Exchange Transaction*) with an error status code (CC_{LACQ} not equal to '0000').

If the transaction completion message does not contain an S_3 it must be treated as a suspect transaction. The next transaction for this CEP card in either the source or target currencies should contain the balance (BAL_{CEP}). This information should allow the card issuer to resolve any suspect transactions.

16.3.2.4 If a card issuer receives a transaction completion message with an invalid S_3 for a currency exchange transaction, the error should be resolved through the scheme provider's dispute resolution process.

16.4 POS Transactions

This section describes the minimum specifications for card issuer processing of purchase and cancel last purchase transactions. Requirements 16.4.1.1 through 16.4.1.3 also apply to intermediate processors forwarding transactions between the merchant acquirer and the card issuer.

16.4.1.1 Each recipient of an issuer batch must validate that the batch can be read and that all data is formatted correctly to ensure that it has been transmitted correctly. If the

batch was transmitted incorrectly and is still available, it should be re-transmitted. If the batch cannot be properly transmitted, the batch must be rejected, and the transactions in the batch must not be forwarded to another recipient. No funds will be due to the sender of the batch.

16.4.1.2 The batch recipient must perform the batch validations specified in Table 106. Any batches that fail these validations must be rejected, and the transactions within the batch must not be forwarded to another recipient.

16.4.1.3 The batch recipient must participate in settlement with the source of the batch for the value of all accepted batches.

Table 106 - Batch Edit Criteria

Batch Edit	**Validation Criteria**
Duplicate Batch	Validate ID_{SOURCE} and Batch Number against previously collected batches.
MAC protecting batch	Validate the MAC protecting the batch using a key and algorithm agreed with the source of the batch
NT_{BATCH}	Ensure that NT_{BATCH} equals the number of all detail transactions in the batch plus the sum of the NT_{AGG} counter in each aggregation record.
$MTOT_{BATCH}$	Ensure that $MTOT_{BATCH}$ equals the sum of the $MTOT_{PDA}$ from each detail purchase transaction and $MTOT_{AGG}$ from each aggregation record less the $MTOT_{PDA}$ for each detail cancel last purchase transaction. Only transaction that have been forwarded for settlement (with SI = '00') are included.

16.4.1.4 The card issuer must perform the transaction validations specified in Table 107 for all transactions that have been forwarded for settlement (with SI = '00'). Any transactions that fail these validations must be forwarded to a data repository designated for this purpose by the scheme provider. Such transactions may also be referred to the dispute process provided by the scheme provider

Table 107 - Purchase Transaction Edit Criteria

Transaction Edit	Validation Criteria
S_6 Validation	Ensure that the S_6 MAC generated by the CEP card is valid
Card Blocking List	Ensure that the card identifier ($ID_{ISS,CEP}$ and ID_{CEP}) is not listed in the scheme provider's account blocking list. This validation is optional by scheme.
Issuer Certificate Revocation	Ensure that the issuer certificate identifier ($VKP_{CA,ISS}$ and CSN_{ISS}, and optionally, $VKP_{REG,ISS}$ and ID_{REG}) is not included in the scheme provider's issuer certificate revocation list

16.4.1.5 The card issuer must validate the S_6 MAC. The definition of this MAC is a card issuer responsibility. Table 108 provides the recommended contents of the S_6 MAC.

Table 108 - Recommended Data Elements for S_6 MAC

Field	Contents	Length
BAL_{CEP}	Balance of the slot after completion	4
$CURR_{PDA}$	Currency	3
$DTHR_{PDA}$	Transaction Date and time	5
ID_{CEP}	Identifier of the CEP card	6
$ID_{ISS,CEP}$	Identifier of the card issuer	4
ID_{PSAM}	PSAM Identifier	4
$ID_{PSAMCREATOR}$	PSAM creator identifier	4
$MTOT_{PDA}$	Transaction amount	4
NT_{CEP}	Transaction number CEP	2
NT_{PSAM}	Transaction number PSAM	4
RID_{PSAM}	RID used by PSAM creator	5

16.4.1.6 The card issuer must validate the S_6‘ MAC on aggregation total records. The definition of this MAC is a card issuer responsibility. Table 109 provides the recommended contents of the S_6‘ MAC.

Table 109 - Recommended Data Elements for S_6‘ MAC

Field	Contents	Length
$CURR_{PDA}$	Currency of the aggregated total record	3
ID_{BATCH}	Identifier for a POS batch	2
ID_{CEP}	Identifier of the CEP card that produced the S_6’	6
$ID_{ISS,CEP}$	Identifier of the card issuer	4
ID_{PSAM}	PSAM Identifier	4
$ID_{PSAMCREATOR}$	PSAM creator identifier	4
$MTOT_{AGG}$	Net value of all aggregated transactions in this aggregation record, updated by the card for each M_{PDA}	4
NT_{CEP}	Transaction number CEP	2
NT_{AGG}	Number of transactions aggregated in this aggregation record, updated by the card at the first Debit command	2
NT_{PSAM}	Transaction number PSAM	4
RID_{PSAM}	RID used by PSAM creator	5

16.4.1.7 If the card issuer identifies other errors in the transaction record which should have been identified during merchant acquirer processing it may dispute the transaction as provided for in the scheme provider’s operating rules.

16.4.1.8 Table 110 shows examples of edits that may indicate fraud or system or card malfunction. If the transaction fails these or similar edits, the card issuer must submit the transaction to the risk management procedures established by itself or the scheme provider.

Table 110 - Risk Management Validation Examples

Transaction Edit	Validation Criteria
Card Serial Number	Validate the $ID_{ISS,CEP}$ and ID_{CEP} to ensure that is an issued card.
Transaction Currency	Ensure that the currency of the transaction is a currency supported by the card issuer.
Duplicate transaction	Validate the ID_{CEP} and NT_{CEP} against previously received transactions.
Card Expiry Date	Validate that the $DEXP_{CEP}$ matches the expiry date in the card.

16.4.1.9 The card issuer is liable for the outstanding balance on all its valid CEP cards. The card issuer must keep a record of its outstanding liability as required by the scheme provider.

16.4.1.10 The card issuer must update its funds pools and reporting with the liability change incurred with the completed POS transactions.

16.4.1.11 Card history must be updated by the card issuer. All POS detail transaction records, whether settled or not-settled, must be available for the period of time specified by the scheme. All transactions that affect card balance and liability change must be retained by a card issuer for the period defined by the scheme provider.

17. Processing Node Transfers

17.1 Transactions Originating at POS Devices

Processing node transfers occur between two processing nodes required to send transactions from the merchant acquirer to the card issuer. These processing nodes include the merchant acquirer, the card issuer, and any entity used by the merchant acquirer or the card issuer as its processing agent.

17.1.1.1 To insure the integrity of the data content and the financial effects of transactions, these processing nodes (or processors) must perform the following tasks for POS transactions:

- Share one or more MAC keys with connecting processors, create a MAC on all transactions sent to another processor and verify the MAC on all transactions received from another processor.
- Send transactions to other processors in the agreed format.
- Participate in a financial transaction with the connecting processors at the time that the transaction is sent or received. Funds move when the transaction moves.

17.1.1.2 When receiving a transmission, the processor must perform the processing described in requirements 16.4.1.1 through 16.4.1.3 in the card issuer section.

17.1.1.3 When sending a transmission, the processor must perform the processing described in section 11.1.2. The actions described in Table 78 are not required.

17.2 Transactions Originating at Load Devices

Processing node transfers occur between two processing nodes required to send transactions from the load acquirer to the card issuer. These processing nodes include the load acquirer, the card issuer, and any entity used by the load acquirer or the card issuer as

its processing agent.

17.2.1.1 To insure the integrity of the data content and the financial effects of transactions, these processing nodes (or processors) must perform the following tasks:

- Share one or more keys with connecting processors.

- Using a shared key, decrypt the PIN block, or other data field, containing the R_1 on all transactions received from another processor and, using a shared key, re-encrypt the PIN block, or other data field, containing the R_1 on all transactions sent to another processor.

  R_1 must never be in the clear outside of a hardware security module.

  If R_1 is being transmitted in a PIN block, processing must not require R_1 to be in PIN format.

- Send transactions to other processors in the agreed format.

- Participate in a financial transaction with the connecting processors at the time that the transaction is sent or received. Funds move when the transaction moves.

18. Data Elements

This section contains the definition of all CEP data elements.

For each data element, the following descriptions are presented where applicable:

- Tag – the tag assigned to the data element in CEPS. This is only present for data elements that are TLV encoded within the card.
- Reference -- if the name, format and definition are further described in another specification.
- Purpose -- a description of the usage of the data element.
- Format -- the data size and data format.
- Content -- the required value for the application.

The subscripts applied in the data element name indicate the source or entity described by the data element, some examples follow:

- LDA - Load Device Application.
- PDA - Purchase Device Application.
- CEP - Common Electronic Purse (the card).
- CH - Cardholder.
- LOG - Log Record.

Bytes or bits specified as Reserved for Future Use (RFU) must be set to the value indicated, or to zero if no value is given. An entity receiving data specified as RFU must not examine or depend upon the coding of these bytes or bits.

18.1 List of data elements

The data elements are presented in alphabetical sequence of abbreviated name.

18.1.1 ACCTYPE (Source Funds Account Type)

Reference: See ISO 8583, field 3. The account type used here corresponds to positions 3 and 4 of that field.

Purpose: Type of account to be the source of funds

Format: BCD, 2 digits (1 byte)

Content: As specified by ISO

Remarks: Required only for linked loads, this element describes the cardholder selection of the type of account.

18.1.2 ADL (Application Data Locator)

Tag 'DF10'

Purpose: Identifies the location of certificate records that may be read using the Read Record command.

Format: See Table 111 for the format of the ADL. See Table 112 for the format of an entry within the ADL.

Table 111 - Format of the ADL

'DF10'	Length	ADL Entry 1	ADL Entry 2	...	ADL Entry *n*

Table 112 - Format of an ADL Entry

Byte	Meaning
1	SFI is in the five most significant bits; remaining bits should be 0b
2	First (or only) record number to be read
3	Last (or only if = byte 2) record to read
4	Type of ADL entry. See Table 113.

Table 113 - Coding of an ADL entry Type

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				Format code of the certificate data in the record				Authentication Public Key Elements
x	x	x	x					RFU

Table 114 - Format Codes for Certificates

Format code	Certificate Types
0001b	Regional Issuer's Certificate
0010b	Issuer Certificate
0100b	Card Certificate
1001b	Regional Acquirer Certificate
1010b	Acquirer Certificate
1100b	PSAM Certificate
All other values	RFU

18.1.3 AID (Application Identifier for a CEP)

Reference: reference 5, ISO 7816-5

Purpose: Identifier for the application. Used during Application Selection as prescribed in reference 8, EMV.

Format: 5-16 bytes

Contents: RID || PIX where the RID is the five-byte global registered identifier as specified in reference 5, ISO/IEC 7816–5 and the PIX (0–11 bytes) is at the scheme provider's discretion.

18.1.4 ALG_{LSAM} (LSAM Algorithm for Unlinked Loads)

Purpose: Indicates the cryptographic approach used by the LSAM and a SAM at the card issuer during unlinked load transactions.

Format: Binary, 1 byte

Contents: Only valid value is '01'

18.1.5 ALGH (Hash Algorithm code)

Purpose: Indicates the algorithm used to produce a hash value in a public key certificate or signature.

Format: Binary, 1 byte

Contents: '01', indicating SHA-1. All other values are RFU.

18.1.6 ALGP (Cryptographic Algorithm Used with Public Keys)

Purpose: Indicates the Public key algorithm used to produce a certificate or signature. At the same time it indicates the value of the public key exponent that is certified by this certificate.

Format: Binary, 1 byte

Remarks: When ALGP is used in a certificate, it represents the algorithm used to produce the next lower level certificate or signature.

Contents: The coding is defined in Table 115.

Table 115 - Coding of ALGP

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x				Value of public key exponent
0	0	0	0	1				2
0	0	0	1	0				3
1	0	0	0	0				$2^{16}+1$
All other values								RFU for CEPS
					x	x	x	Usage of Public Key Algorithm
					0	0	1	- RSA Dynamic Authentication
					x	x	x	- (xxx ≠ 001) RFU

18.1.7 AM_{CEP} (Authentication Method)

Purpose: Used during purchase transactions to inform the POS device of the level of authentication required by the CEP card to perform purchase transactions.

Format: Binary, 1 byte

Contents: See Table 116 for coding

Table 116 - Coding of AM

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0			RFU for CEPS
						x	x	Authentication Option
						0	0	– Dual authentication, no support for S_3'
						0	1	– Dual authentication, support for S_3'
						1	0	– Mutual Authentication, no S_3'
						1	1	– RFU for CEPS
All other values RFU for CEPS								

18.1.8 AP_{CEP} (Application Profile of a CEP Card)

Purpose: Indicates optional functions that are supported in the card.

Format: Binary, 2 bytes

Contents: A constant stored in the CEP card. Table 117 defines the coding for the first byte and Table 118 defines the coding for the second byte.

Table 117 - Most significant byte of AP_{CEP}

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Implementation Specific
		0	0					All other values RFU for CEPS
				x				Account Selection
				1				Supported
				0				Not supported
					x	x		CVMI:
					x	1		- Off-line clear text PIN supported
					x	0		- Off-line clear text PIN not supported
					1	x		- Off-line encrypted PIN supported
					0	x		- Off-line encrypted PIN not supported
							x	Spontaneous Display:
							0	- not allowed
							1	- allowed

Table 118 - Least significant byte of AP_{CEP}

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Implementation Specific
		x	x					RFU for CEPS
				x				Cancel last purchase is:
				0				- Not supported
				1				- supported
					x			Currency exchange is:
					0			- Not supported
					1			- supported
						x	x	Load transaction support (value of '00' is not allowed)
						x	1	- Unlinked Load supported
						x	0	- Unlinked Load not supported
						1	x	- Linked Load supported
						0	x	- Linked Load not supported

18.1.9 AT (Authentication Token)

Purpose: If the merchant acquirer supports intermediate verification of the CEP card by the POS device, the PSAM must be able to generate an authentication token, a 16 byte DES key, to be used by the CEP card to create the S_3'

Format: Binary, 16 bytes

Notes: The AT will only be generated if the CEP card supports Dual Authentication with an S_3'

18.1.10 AVN_{CEP} (Application version number)

Purpose: Indicates the version of the application. The first byte reflects the CEPS version number. The second byte reflects the version of a proprietary implementation.

Format: Binary, 2 bytes

Contents: '00xx' for this version

18.1.11 BAL (Balance of a CEP card slot)

Purpose: Current balance of a slot, in minor units of the slot currency.

Format: Binary, 4 bytes

Contents: An unsigned binary integer defining the actual balance. The balance is represented in the smallest unit of the currency as specified in the slot's currency ($CURR_{CEP}$).

18.1.12 BALmax (Maximum Balance of a CEP slot)

Purpose: The maximum value (in minor units of the slot currency) of a CEP slot up to which a load transaction is allowed.

Format: Binary, 4 bytes

Contents: An unsigned binary integer defining the maximum balance.

18.1.13 $BALmax_{ISS}$ (Advisory Maximum Balance)

Purpose: An optional maximum balance sent as an advice to the load acquirer by the card issuer, if the amount to be loaded plus the current balance (if there is one) is greater than the maximum balance the card issuer will allow. The load acquirer may use this field, in conjunction with input from the cardholder, to reduce the amount to be loaded to an amount that will be approved by the card issuer. The currency of this field is the same as $BALmax_{CEP}$.

Format: Binary, 4 bytes

Contents: An unsigned binary integer defining the maximum balance.

18.1.14 CALPHA (Alpha Code of a Currency)

Purpose: The alpha code of a currency used by load devices during currency exchange transactions.

Format: Alpha character, 3 bytes

Remarks: This field is used by load devices to display the source currency in a form meaningful to the cardholder during a currency exchange transaction. The content is defined by the card issuer, and placed into the CEP card slot during load or currency exchange transactions.

18.1.15 CC_{ACQ} (Completion Code from Merchant Acquirer)

Purpose: Defines successful completion or errors detected by the merchant acquirer after receiving the transaction from the merchant.

Format: Binary, 2 bytes

Remarks: See *Table 75 - Purchase Transaction Edit Criteria* and *Table 76 - Aggregate Record Edit Criteria*.

18.1.16 CC_{CEP} (Completion Code of a CEP Command)

Purpose: The result of executing a command within a CEP

Format: Binary, 2 bytes

Remarks: Status bytes SW1 SW2 from the card

18.1.17 CC_{ISS} (Completion Code from a Card Issuer)

Purpose: Indicates the status of a transaction as determined by the card issuer.

Format: Binary, 2 bytes

Contents: See *Table 102 - Issuer Validations for Load* and *Table 104 - Issuer Validations for Currency Exchange*

18.1.18 CC_{LACQ} (Completion Code from a Load Acquirer)

Purpose: Indicates the status of a transaction as determined by the load acquirer.

Format: Binary, 2 bytes

Contents: See Table 119

Table 119 - Values of Load Acquirer Status Code

Value	Meaning
'0000'	Successful transaction
'0001'	No valid response from card issuer
'0002'	Data update failed
'0003'	Error response from CEP card
'0004'	No response from CEP card
'0006'	No funds for load

18.1.19 CC_{PDA} (Completion Code from a POS Device)

Purpose: Indicates the status of a transaction as determined by the POS device.

Format: Binary, 2 bytes

Contents: *Table 66 - Transaction Condition Codes Determined by the POS Device*

18.1.20 CC_{TRX} (Completion Code of a transaction)

Purpose: Indicates the completion status of an on-line transaction as determined by the CEP card.

Format: Binary, 2 bytes

Contents: If the transaction is successful, the first byte of this field is set to zero. If the high order bit of the first byte is 1b, an R_{CEP} was returned in the response to the Credit for Load command. All other values are card issuer defined.

18.1.21 CED (Certificate Expiration Date)

Purpose: Date after which a certificate is no longer valid.

Format: BCD, 4 digits (2 bytes) in format MMYY.

18.1.22 CNTRY (Country)

Purpose: To specify the country code of a CEP card or a merchant or load acquirer accepting CEP cards. The field is as defined in reference 8, EMV.

Format: BCD, 3 digits (2 bytes) right justified.

18.1.23 CPO_{CEP} (Card Purchase Options)

Purpose: Indicates whether aggregation is supported by the CEP card. This may be a static setting or it may vary based on variables in the transaction and the CEP card.

Format: Binary, 1 byte

Contents: See Table 120

Table 120 - Coding of CPO

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Implementation Specific
		0	0	0	0	0		All other values RFU for CEPS
							x	Aggregation option
							0	- Aggregation not permitted
							1	- Aggregation allowed

18.1.24 CSN (Certificate Serial Number)

Purpose: Unique number assigned to the certificate by the creator of the certificate.

Format: Binary, 3 bytes

Remarks The $CSN_{REG,ACQ}$ must be unique within a region

18.1.25 CURR (Currency)

Purpose: Identifies the currency of a slot or a transaction.

Format: BCD, 3 bytes in the form '*0c cc 0e*', where *ccc* is the code assigned to the currency by ISO 4217, and *e* is the exponent.

Contents: CURR contains both the currency code (CURRC) and the exponent(CURRE)

18.1.26 CURRC (Currency Code)

Purpose: Identifies the currency of a slot or a transaction.

Format: BCD, 2 bytes in the form '*0c cc'*, where *ccc* is the code assigned to the currency by ISO 4217.

Contents: CURRC contains only the currency code

18.1.27 CURRE (Currency Exponent)

Purpose: Identifies the exponent of the currency of a slot or a transaction.

Format: BCD, 1 byte in the form '*0e*'.

Contents: CURRE contains only the currency exponent

18.1.28 DD (Discretionary Data)

Purpose: Data that is specific to a participant in a CEP transaction

Format: Binary, variable length as stated in command, response, or record coding.

18.1.29 DEXP (Expiration Date for Transaction)

Purpose: Date after which the CEP card is no longer valid for the requested transaction.

Format: BCD, 6 digits (3 bytes) in format YYMMDD.

18.1.30 DOM (Domain)

Purpose: An optional field, the domain is used to specify a subdivision of the country code of a CEP card or a merchant or load acquirer accepting CEP cards. The values of this field will be specified by the country that is subdivided.

Format: Binary, 1 byte

18.1.31 DS (Digital Signature)

Purpose: A digital signature created by the PSAM to allow the CEP card to authenticate the PSAM during purchase transactions.

Format: Binary, variable length. The length of the PSAM public key modulus ($LPKM_{PSAM}$) determines the length of DS.

18.1.32 DTHR (Transaction Date and Time)

Purpose: Provides the transaction local date and time.

Format: BCD, 5 bytes (YYMMDDHHMM)

18.1.33 DTRM (Transmission Date)

Purpose: Provides the date of transmission for a blocking list or certificate revocation list entry.

Format: BCD, 3 bytes (YYMMDD)

18.1.34 E_6 (Encrypted S_6)

Purpose: The card issuer MAC for purchase transactions encrypted by the $SESSKey_{PSAM}$

Format: Binary, 8 bytes

Notes: E_6 is created as follows:

$E_6 = DES3(SESSKey_{PSAM})[S_6]$.

18.1.35 $E_{6'}$ (Encrypted S_6')

Purpose: The card issuer MAC for aggregated purchase transaction encrypted by the $SESSKey_{PSAM}$

Format: Binary, 8 bytes

Notes: E_6' is created as follows:

$E_6' = DES3(SESSKey_{PSAM})[S_6']$

18.1.36 H_{CEP} (Hash Generated by CEP Card)

Purpose: A SHA-1 hash of transaction data including an R_{CEP} generated by the CEP card for the transaction. Only the 10 most significant bytes are used.

Format: Binary, 10 bytes

Contents: See section 6.5.1.7

18.1.37 H_{LSAM} (Hash Generated by LSAM)

Purpose: A SHA-1 hash of transaction data including an R_{LSAM} generated by an LSAM for the transaction. Only the 8 most significant bytes are used.

Format: Binary, 8 bytes

Contents: See section 6.5.1.7

18.1.38 $H2_{LSAM}$ (Hash Generated by LSAM)

Purpose: A SHA-1 hash of transaction data including an $R2_{LSAM}$ generated by an LSAM for this transaction. Only the 8 most significant bytes are used.

Format: Binary, 8 bytes

Contents: See section 6.5.1.7

18.1.39 ID_{ACQ} (Identifier for a Merchant Acquirer)

Purpose: Used to uniquely identify the merchant acquirer. The ID_{ACQ} used in the POS device may not be the actual ID_{ACQ}. The ID_{ACQ} sent from the merchant acquirer to the card issuer must be the actual ID_{ACQ}.

Format: BCD, 4 bytes. Left justified, padded to the right with 'F's.

Contents: As defined by ISO/IEC 7812–1, coded as BCD digits

18.1.40 ID_{BATCH} (Identifier for a POS Transaction Batch)

Purpose: To identify the transactions sent as a single batch. Used for both collection batches ($ID_{BATCH,PSAM}$) and issuer batches ($ID_{BATCH,ACQ}$)

Format: Binary, 2 bytes.

Contents: Assigned by the PSAM, the merchant acquirer or an intermediate processing node.

18.1.41 ID_{CEP} (Serial Number of a CEP Card)

Purpose: Unique number assigned to the CEP card by the card issuer.

Format: BCD, 6 bytes. Left justified, padded to the right with 'F's

Remarks: The number of digits in $ID_{ISS,}$ (see 18.1.42) plus the number of digits in ID_{CEP} must not exceed 19 digits.

18.1.42 ID_{ISS} (Card Issuer BIN)

Purpose: Used to uniquely identify the card issuer.

Format: BCD, 4 bytes. Left justified, padded to the right with 'F's.

Contents: As defined by ISO/IEC 7812–1, coded as BCD digits

Remarks: $ID_{ISS,CEP}$ is used when the source of the data is the card. ID_{ISS} is used when the source of the data is the card issuer. The value is the same for both data elements. The number of digits in ID_{ISS} plus the number of digits in ID_{CEP} (see 18.1.41) must not exceed 19 digits.

18.1.43 ID_{LACQ} (Identifier for a Load Acquirer)

Purpose: Used to uniquely identify the load acquirer. The ID_{LACQ} used in the load device may not be the actual ID_{LACQ}. The ID_{LACQ} sent from the load acquirer to the card issuer must be the actual ID_{LACQ}.

Format: BCD, 4 bytes. Left justified, padded to the right with 'F's.

Contents: As defined by ISO/IEC 7812–1, coded as BCD digits

18.1.44 ID_{LDA} (Identifier for a Load Device)

Purpose: Uniquely identifies the load device. Assigned by the load acquirer.

Format: BCD, 6 bytes.

18.1.45 ID_{PSAM} (Identifier for a PSAM)

Purpose: Serial number of the PSAM assigned by the PSAM creator.

Format: Binary, 4 bytes

18.1.46 $ID_{PSAMCREATOR}$ (Identifier for the Creator of a PSAM)

Purpose: Assigned by the owner of the RID_{PSAM}. With the RID_{PSAM}, uniquely identifies the entity creating a PSAM.

Format: Binary, 4 bytes

18.1.47 ID_{REG} (Identifier for a Region)

Purpose: Assigned by the scheme provider. To identify a geo-political region responsible for a regional certification authority.

Format: Binary, 4 bytes

18.1.48 ID_{SCHEME} (Identifier for a Brand or Scheme)

Purpose: Merchant acquirer data element used to identify the scheme owning the CEP card performing a transaction.

Format: Variable

Notes: This is a merchant acquirer data element that is not forwarded. The format is at the discretion of the merchant acquirer.

18.1.49 L (Length of CEPS Data or CEPS DD field)

Purpose: These fields are provided to support migration to new versions of CEPS and new versions of proprietary implementations. These fields indicate the length of CEPS defined data elements (L_{CEPS}) or the length of a discretionary data field (L_{DD}). These fields are found in a command or a response to a command. Note that the length of the data specified by L_{CEPS} does not include L_{DD}. L_{CEPS} is the length of the data starting with the byte immediately after the L_{CEPS} through the byte immediately preceding L_{DD}(if present), or the byte immediately preceding PDATA (if present and no L_{DD}).

Format: Binary, 1 byte

18.1.50 L_{AGGTOT} (Length of Aggregated Totals Data)

Purpose: Indicates the length of a data elements associated with aggregated totals ($MTOT_{AGG}$, NT_{AGG} and ID_{BATCH}). This field is always present in the DS whether the option to aggregate purchase transactions is supported or not by the CEP card, and whether the PSAM supports aggregation or not. If aggregation is not supported by the PSAM, the value of L_{AGGTOT} must be zero.

Format: Binary, 1 byte

18.1.51 L_{AT} (Length of Authentication Token Data)

Purpose: Indicates the length of an authentication token (AT). This field is always present in the DS whether the option to allow intermediate validation of the CEP card by the POS device is supported or not by the CEP card, and whether the PSAM uses the option or not. If the option is not used by the PSAM, the value of L_{AT} must be zero.

Format: Binary, 1 byte

18.1.52 LEN (Length)

Purpose: Indicates the length of a data element in a formatted data structure.

Format: Binary, 1 byte

Notes: The subscript identifies the data element.

18.1.53 LOC_{PDA} (Location Description)

Purpose: A description of the POS device location that can be used by the cardholder during a review of the CEP card log. May be zero if legal considerations prohibit its use.

Format: Alphanumeric, 6 bytes

18.1.54 LPKM (Length of Public Key Modulus)

Purpose: Contains the length of public key modulus.

Format: Binary, 1 byte

Content:

LPKM	Minimum length (bits)	Maximum length (bits)
$LPKM_{CA,ACQ}$	≥ 1024	≤ 1960 (245 bytes)
$LPKM_{REG,ACQ}$	≥ 1024	≤ 1672(209 bytes) < $LPKM_{CA,ACQ}$
$LPKM_{ACQ}$	≥ 896	≤ 1672(209 bytes) < $LPKM_{CA,ACQ}$ < $LPKM_{REG,ACQ}$
$LPKM_{PSAM}$[13]	= 736	= 736
$LPKM_{CA,ISS}$	≥ 1024	≤ 1984 (248 bytes)
$LPKM_{REG,ISS}$	≥ 1024	< 1984 (248 bytes) < $LPKM_{CA,ISS}$
$LPKM_{ISS}$	≥ 896	< 1984 (248 bytes) < $LPKM_{CA,ISS}$ < $LPKM_{REG,ISS}$
$LPKM_{CEP}$	≥768	< $LPKM_{ISS}$

[13] The length of the PSAM modulus must be less than the less of the CEP modulus.

18.1.55 M_{LDA} (Load Device Transaction Amount)

Purpose: Indicates the transaction amount for load or currency exchange transactions. For currency exchange transactions, the amount is in the source currency

Format: Binary, 4 bytes

18.1.56 $Mmax_{ISS}$ (Advisory Maximum Exchange Amount)

Purpose: An optional maximum exchange amount sent as an advice to the load acquirer by the card issuer, if the amount to be exchanged plus the current balance in the target currency (if there is one) is greater than the maximum balance the card issuer will allow. The load acquirer may use this field, in conjunction with input from the cardholder, to reduce the amount to be exchanged to an amount that will be approved by the card issuer. The currency of this field is the same as M_{SOURCE}

Format: Binary, 4 bytes

Contents: An unsigned binary integer defining the maximum exchange amount.

18.1.57 M_{PDA} (POS Device Transaction Amount)

Purpose: Contains the amount to be debited/credited for purchase/cancel last purchase transactions. In the case of a Subsequent Debit or Purchase Reversal command, this is the amount of the step.

Format: Binary, 4 bytes

18.1.58 MAC_{LSAM} (LSAM Transaction MAC)

Purpose: Contains a MAC of transaction data for an unlinked load. Created using R_1 as the MAC key.

Format: Binary, 4 bytes

Content: See Table 82 for the contents of the MAC.

18.1.59 MTOT (Total Transaction Amount)

Purpose: Contains the total transaction amount for purchase or cancel last purchase transactions. Computed by the CEP card ($MTOT_{CEP}$) and the POS device ($MTOT_{PDA}$) for purchase transactions and retrieved from the CEP card log ($MTOT_{CEP,LOG}$) for the S_1 MAC in cancel last purchase transactions.

Format: Binary, 4 bytes

18.1.60 $MTOT_{AGG}$ (Issuer Total Aggregation Amount)

Purpose: Contains the total amount of aggregated transactions for a card issuer.

Format: Binary, 4 bytes

Remarks: If a card issuer supports multiple currencies there will be different totals by currency.

18.1.61 $MTOT_{BATCH}$ (Batch Total Transaction Amount)

Purpose: Contains the total transaction amount for a batch.

Format: Binary, 4 bytes

Remarks: If a batch contains multiple currencies, this may be an arithmetic total or may be different totals per currency.

18.1.62 $MTOTmax_{CURR}$ (Maximum Purchase Transaction Amount)

Purpose: For each currency supported by the POS device, the maximum value of a purchase transaction (including all increments). This value is established by scheme providers.

Format: Binary, 4 bytes

18.1.63 NT_{AGG} (Number of Transactions Aggregated)

Purpose: The count of the transactions aggregated in one issuer aggregation record.

Format: Binary, 2 bytes

18.1.64 NT_{BATCH} (Number of Transactions in a Batch)

Purpose: To identify the number of transactions in a batch. If transactions have been aggregated, this number includes a count of the aggregated transactions.

Format: Binary, 2 bytes

18.1.65 NT_{CEP} (Transaction Number for a CEP Card)

Purpose: A number assigned by the card to uniquely identify the transaction.

Format: Binary, 2 bytes

18.1.66 $NT_{LASTCANCEL}$ (Transaction Number of the Last Successful Cancel Last Purchase Transaction)

Purpose: Contains the transaction number assigned by the card for the last successful cancel last purchase transaction it performed.

Format: Binary, 2 bytes

18.1.67 $NT_{LASTLOAD}$ (Transaction Number of the Last Successful Load Transaction)

Purpose: Contains the transaction number assigned by the card for the last successful Load transaction it performed.

Format: Binary, 2 bytes

18.1.68 NT_{PCT} (Transaction Percentage)

Purpose: Based on a random number generated the PSAM, the percentage of the scheme's transactions for which the detail must be captured by a PSAM performing aggregation.

Format: Binary, 1 byte

18.1.69 NT_{PSAM} (Transaction Number of the PSAM)

Purpose: A number assigned by the PSAM to uniquely identify the transaction. This number is the current value of a counter incremented by the PSAM for each transaction.

Format: Binary, 4 bytes

18.1.70 PDATA (Proprietary Implementation Data)

Purpose: This optional field may be used to send proprietary data to a CEP card or received proprietary data from a CEP card.

Format: variable

Notes: This information will only be transmitted between the CEP card and a device if both the device and the CEP card support the same proprietary implementation

18.1.71 $PK_{CA,ACQ}$ (CA Public Key for Recovering PSAM Public Keys)

Purpose: The CA public key that is used by a CEP card to verify the PSAM public key

Format: Binary, variable length (minimum 1024 bits)

18.1.72 $PK_{CA,ISS}$ (CA Public Key for Recovering CEP card Public Keys)

Purpose: The CA public key that is used by a PSAM to verify the CEP card public key

Format: Binary, variable length (minimum 1024 bits)

18.1.73 PK_{ISS} (Issuer Public Key for Recovering CEP card Public Keys)

Purpose: The issuer public key that is used by a PSAM to verify the CEP card public key

Format: Binary, variable length (minimum 896 bits)

18.1.74 PKC_{ACQ} (Acquirer Public Key Certificate)

Purpose: Acquirer public key certificate created by the scheme or regional CA and contained in the POS device or PSAM.

Format: Binary, variable length (minimum 1024 bits)

18.1.75 PKC_{CEP} (Card Public Key Certificate)

Purpose: Card Public Key Certificate created by the issuer and contained in the CEP card.

Format: Binary, variable length (minimum 896 bits).

18.1.76 PKC_{ISS} (Issuer Public Key Certificate)

Purpose: Issuer public key certificate created by the scheme or regional CA and contained in the CEP card.

Format: Binary, variable length (minimum 1024 bits)

18.1.77 PKC_{PSAM} (PSAM Public Key Certificate)

Purpose: PSAM Public Key Certificate created by the merchant acquirer or PSAM creator and contained in the PSAM or POS device.

Format: Binary, variable length (minimum 896 bits).

18.1.78 $PKC_{REG,ACQ}$ (Regional Public Key Certificate)

Purpose: Optional regional public key certificate created by the scheme CA and contained in the POS device or PSAM.

Format: Binary, variable length (minimum 1024 bits)

18.1.79 $PKC_{REG,ISS}$ (Regional Public Key Certificate)

Purpose: Optional regional public key certificate created by the scheme CA and contained in the CEP card.

Format: Binary, variable length (minimum 1024 bits)

18.1.80 PKM_{ACQ} (Acquirer Public Key Modulus)

Purpose: Acquirer public key modulus. The associated private key is used to create PKC_{PSAM}.

Format: Binary. The modulus is variable length (at least 896 bits).

18.1.81 $PKM_{CA,ACQ}$ (CA Public Key Modulus)

Purpose: CA public key modulus used to authenticate the PSAM. The corresponding CA private key is used to create $PKC_{REG,ACQ}$ or PKC_{ACQ}.

Format: Binary. The modulus is variable length (at least 1024 bits).

18.1.82 $PKM_{CA,ISS}$ (CA Public Key Modulus)

Purpose: CA public key modulus used to authenticate the CEP card. The corresponding CA private key is used to create $PKC_{REG,ISS}$ or PKC_{ISS}.

Format: Binary. The modulus is variable length (at least 1024 bits).

18.1.83 PKM_{CEP} (Card Public Key Modulus)

Purpose: CEP card public key modulus. The associated private key is used by the CEP card to verify the PS_2.

Format: Binary. The modulus is variable length (at least 768 bits).

18.1.84 PKM_{ISS} (Issuer Public Key Modulus)

Purpose: Issuer public key modulus. The associated private key is used to create PKC_{CEP}.

Format: Binary. The modulus is variable length (at least 896 bits).

18.1.85 PKM_{PSAM} (PSAM Public Key Modulus)

Purpose: PSAM public key modulus. The associated private key is used by the PSAM to create dynamic digital signatures for POS transactions.

Format: Binary, fixed length (736 bits)

18.1.86 $PKM_{REG,ACQ}$ (Region Public Key Modulus)

Purpose: Optional regional public key modulus. Used to authenticate the PSAM. The associated regional private key is used to create PKC_{ACQ}.

Format: Binary. The modulus is variable length (at least 1024 bits).

18.1.87 $PKM_{REG,ISS}$ (Region Public Key Modulus)

Purpose: Optional regional public key modulus. Used to authenticate the CEP card. The associated regional private key is used to create PKC_{ISS}.

Format: Binary. The modulus is variable length (at least 1024 bits).

18.1.88 PKR (Public Key Remainder)

Purpose: Contains the rightmost part of the Key Modulus when the entire modulus will not fit into the public key certificate

Format: Binary, variable length

Remarks: The subscript is used to denote the associated public key, as in $PKR_{REG,ACQ}$, $PKR_{REG,ISS}$, PKR_{ACQ}, PKR_{ISS}, PKR_{CEP}, PKR_{PSAM}

18.1.89 PS_2 (Public Key Signature of the PSAM)

Purpose: A digital signature created by the PSAM to allow the CEP card to authenticate the PSAM during purchase transactions and to convey the DES key to be used for subsequent MACs.

Format: Binary, variable length. The length of the CEP public key modulus ($LPKM_{CEP}$) determines the length of PS_2.

18.1.90 R_{CEP} (Unique Number for a Load Transaction from the CEP Card)

Purpose: A number generated by a CEP card and recreatable by the card issuer. This number allows the LSAM to authenticate an error received from the CEP card in an unlinked load transaction

Format: Binary, 16 bytes

18.1.91 R_{LSAM} (Random Number for a Load Transaction Generated by the LSAM)

Purpose: A random number generated by an LSAM that allows the CEP card to authenticate that the S_2 was received from a valid load device. Included in S_2 for all load transactions

Format: Binary, 16 bytes

18.1.92 $R2_{LSAM}$ (Second Random Number for a Load Transaction Generated by the LSAM)

Purpose: A random number generated by an LSAM that allows the card issuer to validate that the S_2 was not used to load value onto the CEP card.

Format: Binary, 16 bytes

18.1.93 R_1 (Random Number Generated by an LSAM)

Purpose: Contains the random number generated by the LSAM to be used as a key to create and validate MAC_{LSAM} to ensure the validity of unlinked load messages between the load acquirer and the card issuer.

Format: Binary 8 bytes

18.1.94 REFBALmax (Reference Maximum Balance)

Purpose: The approximate balance limit, in a reference currency, which indicates the approximate amount that the card issuer will allow to be loaded to a slot without an established currency and maximum balance (BALmax).

Format: Binary, 4 bytes

Contents: An unsigned binary integer.

18.1.95 REFCURR (Reference Currency)

Purpose: Identifies the reference currency of the CEP card. Used with the reference maximum balance.

Format: BCD, 3 bytes in the form '*0c cc 0e*', where *ccc* is the code assigned to the currency by ISO 4217, and *e* is the exponent.

Contents: CURR contains both the currency code (CURRC) and the exponent(CURRE)

18.1.96 REFNO (Reference Number)

Purpose: A number assigned to a transaction by an entity, sent with the transaction to another entity to allow the receiver to identify the specific transaction to the sender.

Format: BCD, 3 bytes.

18.1.97 RID_{CEP} (Registered Identifier Of The Scheme for a Transaction)

Purpose: The identifier of the scheme that establishes the rules for a particular CEP transaction, assigned as specified in reference 5, ISO/IEC 7816-5. The first 5 bytes of the CEP card's AID.

Format: Binary, 5 bytes

18.1.98 RID_{PSAM} (Registered Identifier Of The Entity Assigning PSAM Creator Ids)

Purpose: Used to make the identifier of a PSAM creator unique. The identifier of the entity that assigns identifiers to certified PSAM creators, assigned as specified in reference 5, ISO/IEC 7816-5.

Format: Binary, 5 bytes

18.1.99 S_1 (MAC of the CEP card)

Purpose: A MAC created by the CEP card for on-line transactions to allow the issuer to authenticate the card prior to authorizing the transaction.

OR

A MAC created by the CEP card for cancel last purchase transactions that allows the PSAM to verify the authenticity of the card and that the CEP card performed the purchase transaction being canceled

Format: Binary, 8 bytes

18.1.100 S_2 (MAC of the Card issuer host or PSAM)

Purpose: A MAC created by the issuer host SAM in on-line transactions to allow the CEP card to authenticate the issuer prior to adjusting the slot balance. Must contain H_{LSAM} for approved unlinked load transactions[14]. If present for declined load transactions, must contain CC_{ISS} and must not contain H_{LSAM}.

OR

A MAC created by the PSAM

- for cancel last purchase transactions that allows the CEP card to verify the authenticity of the PSAM and that the PSAM performed the purchase transaction being canceled
- in Subsequent Debit commands and in the Purchase Reversal command that allows the CEP card to verify the authenticity of the PSAM

Format: Binary, 8 bytes

18.1.101 S_3 (Transaction MAC)

Purpose: A MAC created by the CEP card for on-line transactions to allow the issuer host to verify the success or failure of the transaction after completion.

OR

A MAC created by the CEP card for purchase transactions that allows the PSAM to verify the authenticity of the CEP card

Format: Binary, 8 bytes

18.1.102 $S_{3'}$ (MAC for POS Device Validation of a CEP Card)

Purpose: The 4 high order bytes of a MAC created by the CEP card for purchase transactions that allows the POS device to verify the authenticity of the CEP card on intermediate steps of an incremental purchase transaction. Created using the authentication token (AT).

Format: Binary, 4 bytes

[14] SHA(R_{LSAM}) will not be sent to the card issuer for linked load transactions, so it is not available for inclusion in the S_2 MAC.

18.1.103 S_4 (MAC of the PSAM for a Batch)

Purpose: A MAC authenticating batch data to the merchant acquirer, proving that the batch totals have not been altered, and that the transactions were performed with a PSAM under control of the merchant acquirer.

Format: Binary, 8 bytes

18.1.104 S_5 (MAC of the PSAM for a Transaction)

Purpose: A MAC created by the PSAM to authenticate the transactions logged by the POS device to the merchant acquirer.

Format: Binary, 8 bytes

18.1.105 S_6 (Transaction MAC)

Purpose: A MAC created by the CEP card during a purchase transaction, allowing the issuer to verify the transaction.

Format: Binary, 8 bytes

18.1.106 S_6' (MAC on Aggregated Transactions)

Purpose: A MAC created by the CEP card during a purchase transaction, allowing the issuer to verify the total of transactions that have been aggregated.

Format: Binary, 8 bytes

18.1.107 $SESSKey_{PSAM}$ (Session key for Purchase and Cancel Last Purchase)

Purpose: A session key, generated by the PSAM and exchanged with PS_2, used by CEP card or PSAM to create a MAC which will be used for authentication and data integrity protection.

Format: Binary, 16 bytes

18.1.108 SK (Private key)

Purpose: An asymmetric private key used by a PSAM or a CEP card to authenticate a POS transaction.

Format: Binary, variable length minimum 768 bits for CEP card; fixed length 736 for PSAM

Notes: The subscript identifies the entity (PSAM or CEP card) owning the key.

18.1.109 SI (Settlement Indicator)

Purpose: Indicates to the card issuer if the merchant acquirer expects payment from the card issuer for the transaction.

Format: Binary, 1 byte

Content: ‘00’ - transaction submitted for settlement, ‘01’ - transaction submitted for reporting only

Remarks: Generated by Merchant acquirer after collection and verification of a batch and the transactions in the batch.

18.1.110 STI (Suspect Transaction Indicator)

Purpose: Indicates to the card issuer that this transaction may not have completed successfully.

Format: Binary, 1 byte

Content: ‘00’ – normal transaction completion, ‘01’ - transaction completed in a manner that makes its exact status unknown

18.1.111 TI (Transaction Indicator)

Purpose: Indicates the transaction type to the merchant acquirer. For purchase transactions, only the last step of the transaction is coded; the rest are known implicitly.

Format: Binary, 1 byte

Content: See Table 121 for permissible values.

Table 121 - Coding of the Transaction Indicator (TI)

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0							All other values are RFU for CEPS
		x	x					Issuer discretionary use for on-line transactions. Zeros for off-line transactions
				0	x	x	x	Off-line Transactions
				0	0	x	x	Purchase Transaction[15]
				0	0	x	1	- last step reversed
				0	0	1	x	- incremental transaction (includes at least one Subsequent Debit)
				0	1	0	0	Cancel Last Purchase
				1	x	x	x	On-line Transactions
				1	1	0	0	Load Transaction
				1	0	0	0	Currency Exchange
				1	all other values			Issuer discretionary use for on-line transactions. Zeros for off-line transactions

[15] The value of TI for a single step, un-reversed purchase should be '00'.

18.1.112 $VKP_{CA,ACQ}$ (CA Key Version)

Purpose: Indicates the version of CA public key used to produce the acquirer or acquirer regional certificate.

Format: Binary, 1 byte

18.1.113 $VKP_{CA,ISS}$ (CA Key Version)

Purpose: Indicates the version of the CA public key used to produce the issuer or issuer regional certificate.

Format: Binary, 1 byte

Contents A version number of zero is not permitted.

18.1.114 $VKP_{REG,ISS}$ (Regional Key Version)

Purpose: Indicates the version of the regional public key used to produce the issuer certificate.

Format: Binary, 1 byte

19. Glossary

A.

Aggregation

The total amount, consisting of the sum of all transactions in a given batch, is provided to the issuer. Details of the individual transactions that make up the total are not provided, or recoverable.

Application

A computer program and associated data that resides on an integrated circuit chip and satisfies a business function. Examples of applications include: spreadsheets, word processing, databases, electronic purse, loyalty, etc.

Asymmetric Key Cryptography

See Public Key Cryptography and Encryption.

Auditability

The ability to quantify an issuer’s outstanding value to its initialized value.

Authentication

A cryptographic process used to validate a user, card, terminal or message contents in which one entity proves its identity and the integrity of the data it may send to another entity. Also known as a handshake, the authentication uses unique data to create a code that can be verified in real time or batch mode. An umbrella term for several risk management processes that may be performed during chip card transactions.

B.

Balance

The remaining value in an electronic purse (in a specific currency). It is increased by load transactions and cancel last purchase transactions, and decreased by purchase and unload transactions. Currency exchange transactions both increase and decrease slot balances.

Batch

A batch is a group of transactions recognized by the POS device as a logical entity and transmitted at single time for further processing. A total transaction count and net transaction amount for a batch reflect the count and value of the transactions grouped by the POS device into that batch. Each batch must have an identifying number for tracking purposes. An active batch is one into which the POS device is currently placing new transactions. When a batch is closed, that is, it is no longer the active batch, the batch number is incremented by one to create the new batch number, and the total transaction count and amount are reset to zero for the new batch.

C.

Cancel Last Purchase Transaction

The action that increments the balance on an electronic purse card. It is used to correct an amount that was keyed incorrectly at the time of purchase, or to reimburse a customer for the amount of a purchased item that the customer subsequently returned.

Card Acceptance Device (CAD)

The mechanism, a key component of integrated circuit card reader/writers, into which an integrated circuit card is inserted.

Card Authentication Method (CAM)

A cryptographic means of validating a card's legitimacy.

Card Blocking List

A list similar to a “hot card” list which allows a card issuer to block certain cards which have been compromised, for use at POS devices.

Card Issuer

Also known as the Electronic Purse Card Issuer, it is the organization responsible for the provision and distribution of integrated circuit cards. It also authenticates load requests and transaction records, and provides cardholder customer service.

Cardholder Verification Controls

Cardholder verification confirms the identity of the person using the card as the rightful cardholder and signifies cardholder acceptance of the transaction. Chip technology improves cardholder verification in two important ways. First, the chip makes it possible to check PINs off-line. Second, chips can store and process issuer instructions that specify which cardholder verification controls are to be used in different situations at the point of transaction, which further enhances transaction security and improves issuer control. Cardholder verification controls enable issuers to:

- Specify whether on-line or off-line PINs are required for a given chip card application and if off-line PINs are required, whether they are encrypted or not.
- Set a maximum allowable number of PIN tries.

Certificate

A public key and related data signed by a higher level private key.

Certificate Revocation List

A list that identifies issuer public key certificates that are no longer valid. This allows an issuer to block certain cards, where the issuer private key has been compromised, for use at POS devices.

Certification Authority

An entity entrusted by one or more entities to create and assign public key certificates.

Chip Card

A financial or other (for example, identification) card that is embedded with an integrated circuit.

Chip-Reading Device/Terminal

A POS device, ATM, or other device capable of processing chip card-initiated commands.

Collection

The process of transferring transaction data from a POS device to the merchant acquirer.

Completion Code

A part of the response to any component on a given command. It indicates whether the command was successfully performed or not; in the latter case the completion code indicates the reason why it was not successful.

D.

Data Encryption Standard (DES)

The National Institute for Standards and Technology's Data Encryption Standard is the most widely accepted public domain symmetric key cryptography algorithm.

Digital Signature

This prevents denial of a transaction or message by the sender. The technique is being used for electronic mail, financial transactions and in sensitive data system applications. The digital signature is generated using a public key cryptographic algorithm and information that identifies the user, including a cryptographic key. In the public key version, the user signs the message using a private key stored in a smart card or terminal hardware or software. The receiver employs the public key of the sender to authenticate their identity.

E.

EMV Specifications

Technical specifications for credit/debit applications developed cooperatively by Europay, MasterCard and Visa (EMV) to create standards and ensure global interoperability for the use of chip technology in the payments industry.

Error Recovery

A group of transactions used for correcting certain errors observed during processing of normal transactions.

Electronic Purse

An electronic purse uses an integrated circuit for the storage and processing of monetary value that is used for purchase of goods or services. It is generally positioned to displace small value coins and cash purchase amounts. The card may be disposable or reloadable.

Electronic Value

The value stored and exchanged in an electronic purse card system. The electronic value is offset by hard currency in the specified currency.

Encryption

The transformation of data into a form unreadable by anyone without a secret decryption key.

F.

Funds Card

The traditional bank card used to purchase a disposable card or load value to a reloadable card. The card issued to a cardholder by the funding bank.

Funds Issuer

The financial institution that domiciles the accounts used to load value to a reloadable electronic purse card.

I.

Initialization

The process, executed by card supplier that sets data fields on the card.

Integrated Circuit Card (ICC)

See Smart Card.

Integrated Circuit Card Specifications for Payment Systems, and Integrated Circuit Card Terminal Specifications for Payment Systems

Technical specifications developed jointly by Europay, MasterCard and Visa (EMV) to create standards for the use of chip technology in the payments industry.

International Organization for Standardization (ISO)

The major international standards setting organization.

Interoperable Electronic Purse Applications

Electronic purse applications that utilize technology-independent, end-to-end transaction processing coupled with devices that allow electronic purse cardholders, merchants, and financial institutions, regardless of the underlying technology, to perform electronic purse transactions. The applications must be supported by systems that clear and settle transactions performed by cardholders and merchants, regardless of the card issuer, acquirer and/or system operator.

Issuer Certificate Revocation List

A list similar to a “hot card” list which identifies card issuer public key certificates that are no longer valid. This allows a card issuer to block certain cards where the card issuer private key has been compromised, for use at POS devices.

K.

Key Management

A technique for securely distributing cryptographic keys to parties involved in a secure transaction. Key management generally requires a special computer dedicated to distribute keys securely, however, public key cryptography also may be used to establish session keys between two parties without the need for a third party server. It provides for both manual and automated techniques to securely exchange keys and keying material between the various system components, either directly or indirectly using common key management centers to whom responsibility has been delegated by the system operator(s).

L.

Linked Load

A load transaction where the funds issuer and the card issuer are the same financial institution and chooses to process the load as a single transaction.

Load Acquirer

An organization through which a load transaction is initiated.

Load Device

A physical device (e.g., ATM) operated by a load acquirer and used by an electronic purse card cardholder to transfer value from the cardholders funds account to the electronic purse card. The device must be capable of communicating with the reloadable card and of communicating on-line with the funds issuer and the electronic purse card issuer.

Load Transaction

An on-line transaction performed using a load device, such as an ATM, telephone, etc., whereby value from the cardholder’s source of funds (e.g., funding account) is transferred to an electronic purse card. In return, the electronic purse card issuer receives payment from the cardholder’s funding source.

Load Value Transaction

Consumer initiated transaction that adds value to electronic purse cards at

load devices.

Load and Unlocking CEP cards

The card issuer or the cardholder may lock or unlock an activated CEP application through a command sent to the CEP card. A cardholder must not be allowed to unlock a card locked by the card issuer. This feature may be used to prevent use of a card at a POS device. If this feature is used, on-line transactions should be allowed for a locked card to enable the card issuer to unlock card.

LSAM (Load SAM)

A SAM installed at the load device or load acquirer host providing the necessary security for the communication between the load acquirer and the card issuer.

M.

Magnetic Stripe Card

A card that contains a magnetic stripe material technology that can store approximately 130 characters or numbers, which provides information about the account and the cardholder.

Merchant

The organization delivering goods and/or services to the cardholder.

Merchant Acquirer

An organization that collects and possibly aggregates transactions from several purchase devices for delivery to one or more system operators.

Message Authentication Code (MAC)

A digital code generated using a cryptographic algorithm, which establishes that the contents of a message have not been changed. Taking all or part of a message, such as the amount and account number, and processing it through the algorithm, usually DES, generates a MAC. The resulting code is appended to the message. The receiver, using the same algorithm and secret key processes the message to see if the same MAC results. If not, there has been an error in the transmission or data has been purposely changed. Messages with MACs do not necessarily need to be scrambled, as data integrity, not data secrecy, is the primary objective.

Microprocessor/Microcomputer

The brain of the smart card, which functions as the central processing unit and executes application and security functions. A true smart card contains a microcomputer that includes EEPROM, a microprocessor CPU, ROM (which stores operating, security and application programs) and RAM (which provides temporary registers for interim processing steps).

Multi-Application Card

A smart card that supports more than one application (e.g., electronic purse, debit, credit, loyalty, etc.).

Multi-Currency Support

Capability to handle more than one currency and provide foreign currency exchange functions.

Mutual Authentication

The process of authentication where the cardholder's card validates the terminal and the terminal validates the card. See also Two-way Authentication.

N.

Nibble

A byte consists of two nibbles. The first nibble is the first four bits of the byte. The second nibble is the last for bits of the byte.

Non-Repudiation

Providing cryptographic proof that neither the originator nor the receiver can repudiate having sent/received a given message with its original contents.

O.

Off-line Transaction

A transaction that does not require real-time connection to a card issuer.

On-line Authorization

The process whereby the funds for a load transaction for a specified

amount is approved or declined on-line by the funds issuer or the funds issuer's designated processor.

On-line Transaction

A transaction that requires s real-time connection to a card issuer.

One-Way Authentication

The authentication process wherein either the cardholder's card determines that the terminal is valid, or the terminal determines that the cardholder's card is valid, but not both. One-way authentication always refers to card authentication.

P.

Personal ATM

An easy to use, handheld appliance that can connect to a communications line for use as a load device when the card issuer is also the load acquirer.

Personal Identification Number (PIN)

A code used by a cardholder for identification and subsequent access to financial or non-financial data.

Personalization

The process of initializing a card with data that makes it unique from all other cards. This includes account data and cardholder information in the case of credit or debit accounts.

Point of Sale (POS)

The environment in which a consumer purchases goods or services. Also referred to as point of transaction (POT), point of use (POU), and point of service (POS).

Private Key

That key of an entity's asymmetric key pair that should only be used by that entity. In the case of a digital signature scheme, the private key defines the signature functions.

Public Key

That key of an entity's asymmetric key pair that may be made public. In

the case of a digital signature scheme, the public key defines that verification function.

Public Key Cryptography and Encryption

An asymmetric cryptographic method using two different mathematically related keys for encryption and decryption. One key remains private and is maintained by the user in a terminal or smart card. The other key since it cannot be used to derive the private key is made public. When encrypting data, the sender looks up the public key of the receiver and uses it to encrypt the message. Only the user possessing the associated private key can decrypt the message. As the sophisticated and extensive mathematics that allows this cipher system to work, public key cryptography is generally not used for encryption of large amounts of data. Instead, it has found the most favor as a way of generating a digital signature, which is attached to a message or transaction to confirm the identity of the sender. In this process, the user employs their own private key on part of the message, including identification information. Anyone receiving the message may authenticate the sender's identity by decrypting the digital signature using the sender's public key. The message also may be scrambled to ensure the secrecy of the message contents. PKE techniques are also popular to establish session keys for symmetric key encryption of data between two parties, without the need for a central key distribution facility.

Purchase Log

Data in a electronic purse card non-volatile memory used to record information on at least the latest purchase transaction.

Purchase Secure Application Module (PSAM)

A PSAM is a secure device, typically, a chip that is embedded typically on a card that resides in a card acceptance device (CAD) or a hardware security module (HSM). The PSAM contains security keys and performs the functions of authenticating an electronic purse card during a purchase transaction and securing the payment and collection totals.

R.

RSA

A public key cryptography algorithm developed by mathematicians Rivest, Shamir and Adleman of MIT. See Public Key Cryptography and Encryption.

Reconciliation

The process of validating that appropriate credits and debits are processed for load and unload transactions. An audit process that ensures that data residing on more than one database is in balance.

Refund

The return of goods by a consumer in exchange for the return of money (electronically or otherwise) paid for the goods.

Reloadable Card

An electronic purse card that has the capability for a consumer to add value or unload value from the card.

Repudiate

The act of rejecting, renouncing or disclaiming a transaction that was previously accepted.

S.

Scheme

An electronic purse card system including the card and terminal application, central system, and security.

Scheme Provider

The electronic purse card authority that defines the program operating rules and conditions. The organization is responsible for the overall functionality and security of an electronic purse card system.

Secret Key

A key used with symmetric cryptographic techniques and usable only by a set of specified entities. The key is kept secret at both the originator and the recipient locations.

Secure Application Module (SAM)

A logical device used to provide security for insecure environments. It is protected against tampering, and stores secret and/or critical information.

Security Architecture

The utilization of detailed security mechanisms, including cryptographic algorithms and the key management necessary to implement security requirements.

Settlement

A process performed by the system operator. Based on data from purchase and load transactions, payment is effected from the system operator to the acquirers and in some cases from the load acquirers to the system operator.

Signature

A cryptographic algorithm used in security protocols to authenticate both devices and the integrity of data.

Slot

A set of data elements associated with a specific currency.

Smart Card

A card that contains an integrated circuit for data storage and processing. A typical smart card chip includes a microprocessor or CPU, ROM (for storing operating instructions), RAM (for storing data during processing) and EPROM or EEPROM memory for non-volatile storage of information.

Symmetric Key Cryptography

Cryptographic processes in which encryption and decryption rely on the same secret key. An example is the Data Encryption Algorithm (DEA); however, a host of other proprietary algorithms are also available. The strengths of the approach are its security and speed, especially when implemented in hardware. The major disadvantage is the complex key management procedures required to securely distribute keys. Symmetric key cryptography may also be used to protect the integrity of data by generating message authentication codes (MAC) and to sign messages with digital signatures. The latter process, however, requires special procedures to guarantee protection of keys. See DES.

T.

Truncation

Transactions are stopped at some point in the process and not passed to the issuer or its agent. If necessary, the issuer could retrieve the transaction.

Two-Way Authentication

The process of authentication where the cardholder's card validates the terminal and the terminal, in turn, validates the card. See also Mutual Authentication.

U.

Unlinked Load

A load transaction with two separate transactions, one to the card issuer to authenticate the card, and the second to secure funding for the load. The source of funds may be cash or it may be a cardholder account.

Unload Transaction

The on-line process of unloading value from a electronic purse card to an account.

20. Acronyms

Acronym or Data Element	Description
ACQ	Acquirer
ATM	Automatic Teller Machine (Unit)
ATR	Answer-to-Reset
BIN	Bank Identification Number
bps	Bits per Second
CA	Certification Authority
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CEN	European Committee for Standardization
CEP	Common Electronic Purse
CEPS	Common Electronic Purse Specifications (or System)
DB	Database
DDA	Dynamic Data Authentication
DES	Data Encryption Standard
DF	Dedicated File
EEPROM	Electronically Erasable Programmable Read-Only Memory
EF	Elementary File
EMV	Europay, MasterCard and Visa
FCI	File Control Information
FI	File Identifier
IC	Integrated Circuit
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
IFD	Interface Device
ISO	International Organization for Standardization
ISAM	Issuer SAM

Acronym or Data Element	Description
ISS	Issuer
LDA	Load Device Application
MAC	Message Authentication Code
PDA	Purchase Device Application (Purchase Device)
PIN	Personal Identification Number
PK	Public Key
POS	Point of Sale/Point of Service
PSAM	Purchase Secure Application Module
RFU	Reserved for Future Use
RSA	Rivest, Sharmir and Adleman (Cryptographic Algorithm)
SAM	Secure Application Module
SFI	Short File Identifier
SHA	Secure Hash Algorithm
TLV	Tag, Length, Value
Var	Variable