Common Electronic Purse Specifications

Functional Requirements

Version 6.3
September 1999

TABLE OF CONTENTS

List of Figures

1. Overview

1.1 Objective

The objective of this document is to define the functional requirements for an open and common interoperable electronic purse environment. This document must serve as the source for the Common Electronic Purse (CEP) technical specifications and as a refinement of the CEP business requirements. Documentation of the technical specifications must follow publication of these functional requirements and must enable payment systems to develop electronic purse schemes, and participants of these schemes to develop the products and systems required for implementation.

1.2 Scope of Document

The document identifies functional requirements that fulfill the requirements for an overall CEP system:

- Security.
- Card application.
- Terminal application.
- Point-of-sale transactions.
- Load transactions.
- Unload transactions.
- Currency exchange transactions.
- Transaction processing.
- Settlement and reconciliation.
- Clearing and Administration.

1.3 Document Structure

The document is structured to explain the functionality needed for an interoperable electronic purse product and to define the requirements to offer and operate such a product throughout the world. Sections include:

- Overview.
- Roles and Responsibilities.

- Security Requirements.
- POS Transaction Requirements.
- Load, Unload and Currency Exchange Requirements.
- Card Requirements.
- Key Management
- Reporting.
- Glossary.
- Acronyms.

1.4 Document References

The following documents are referenced in these requirements:

- *EMV '96 Integrated Circuit Card Specification for Payment Systems* Version 3.1.1 dated May 31, 1998
- *Common Electronic Purse Specifications (CEPS) Business Requirements* Version 6.1 dated September 1998
- *ECBS Technical Committee Draft: The Interoperable Financial Sector Electronic Purse* dated November 1998

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

2. Roles and Responsibilities

This chapter defines the participants in a CEP transaction. Specific functional requirements for each of the following participants are detailed in appropriate sections throughout this document. This does not preclude the participants from sub-contracting these functions to another entity or entities. All of the participants defined in this section are required to conform to the CEP specifications.

2.1 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, as described in these requirements.

The scheme provider must establish 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 ensure that these procedures are followed. If a central data repository exists, data for the investigation of fraud must be forwarded by the card issuer and merchant acquirer.

The scheme provider must establish policies and procedures to ensure that all transactions are secured, as defined in these requirements.

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

- define default routing parameters and procedures, and
- establish a unique scheme identifier in conjunction with other CEP scheme providers

for use in routing transactions when the merchant acquirer does not have an existing relationship with the card issuer.

2.2 Certification Authority

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

2.3 Card Issuer

The card issuer is the organization responsible for the provision and distribution of integrated circuit cards containing a CEP application. The card issuer has the liability for all value loaded onto the CEP card and the management of the funds pool. The card issuer is responsible for making necessary system changes, developing marketing plans, and managing cardholder relationships. The card issuer is responsible for authenticating the CEP card for on-line transactions and authorizing the disbursement of funds to be loaded to a CEP card for a linked load and the transfer of funds for an unload transaction.

A card issuer may issue CEP cards for more than one common electronic purse scheme.

2.4 Funds Issuer

The funds issuer has the responsibility for authorizing the disbursement of funds to be loaded to a CEP card for an unlinked load.

2.5 Cardholder

The cardholder uses the CEP card for loading value, unloading value, exchanging currencies, and making purchases. When made available by the card issuer, the cardholder has the option of locking and/or unlocking the application.

2.6 Load Acquirer

The load acquirer is the entity responsible for establishing a business relationship with one or more scheme providers to process load and currency exchange transactions, and settle unlinked load transactions.

2.7 Merchant

The merchant has responsibility for the use of a POS device to accept CEP cards for payment of goods and services according to the markings displayed on the acceptance devices. The merchant must also display signage for consumer awareness, education, and convenience.

2.8 Merchant Acquirer

The merchant acquirer is the entity responsible for establishing a business relationship with one or more common electronic purse scheme providers to process POS transactions, and settle POS transactions. The merchant acquirer is the organization responsible for the provision and distribution of Purchase Secure Application Modules (PSAMs) that interact with terminals for conducting transactions at the point of sale.

The merchant acquirer is responsible for making necessary system changes, developing marketing plans, and managing merchant relationships.

The merchant acquirer is the organization that collects transactions from POS devices for delivery to one or more card issuers. Merchant acquirers are responsible for paying merchants for electronic purse transaction values and must be able to effect settlement for POS transactions that have occurred at their merchant sites.

The merchant acquirer must provide a mechanism for assigning PSAMs to merchants, which allows for a subsequent reassignment of the PSAM to another merchant.

2.9 Processor

Although transactions may flow directly from a merchant acquirer to a card issuer, some times the transactions must be processed by additional nodes in the network connecting the merchant acquirer and the card issuer and between the load acquirer and the card issuer. This node is identified as a processor.

To ensure 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.
- Participate in the scheme provider dispute resolution process with connecting processors to resolve any issues related to invalid transactions. This resolution process may include a scheme-defined mechanism for repayment of funds associated with invalid transactions.

To ensure the integrity of the data content and the financial effects of transactions, these processing[*] nodes (or processors) must perform the following tasks for load and currency exchange transactions:

- Share an encryption key with connecting processors. Encrypt the PIN block on all transactions sent to another processor using this encryption key. Decrypt and re-encrypt all PIN blocks that should be sent to other entities.
- Send transactions to other processors in the agreed format.

[*] The merchant acquirer, the load acquirer and the card issuer are considered processors as well.

- 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.

3. Security Requirements

3.1 Scope

This chapter describes the use of cryptography to prevent fraudulent transactions from occurring. It does not address the following:

- Physical security of card supplies.
- Pre-issuance security.
- Security of systems and data bases.
- Card internal (cross-application) security.
- Measures to prevent card tampering to extract secret information.
- Cryptographic security requirements for script commands.

The use of cards in balance viewers and personalization devices is outside the scope of these functional requirements. The evaluation and certification requirements for card and devices is also outside the scope of this document.

3.2 Overview

The CEP security system must satisfy the following requirements:

- The card issuer must be able to verify that genuine cards, produced by or on behalf of the card issuer, performed all of the transactions received.
- The merchant acquirer must be able to verify that POS devices under control of the merchant acquirer conducted all POS transactions received.
- The merchant acquirer must be able to ensure that purchase transactions have not been canceled without the merchant acquirer receiving the cancellation transaction information.

3.3 Key and Security Mechanisms

3.3.1 Authentication Method

Successful authentication is a prerequisite for the processing of any on-line or off-line CEPS transaction.

3.3.2 On-line Authentication

On-line authentication must take place between the card issuer and the CEP card for load, unload, and currency exchange transactions. The card issuer and the CEP card share a secret key to generate and verify MACs. Specification of keys and signatures used for CEPS on-line authentication is left to the issuer, however MACs passed over shared networks must be no more than 8 bytes long, binary format.

3.3.3 Off-line Authentication

Off-line authentication must take place between a PSAM in the POS device and the CEP card for purchase and cancel last purchase transactions. The card and the PSAM must use a public key algorithm for mutual authentication and session key exchange, as no permanent shared secret key may exist between the CEP card and the PSAM. RSA is the public key algorithm chosen for CEPS.

3.4 Signature and Transaction Security

This section describes the application signatures used in each transaction.

3.4.1 Load

To load value into a slot of the CEP card securely, the load device establishes a connection between the issuer and the CEP card. The card should use a unique diversified secret key, personalized into the card, to generate and authenticate transaction signatures.

There are two types of load, linked and unlinked, with very different security requirements. In the case of a linked load, funds are not moved between financial institutions. The cardholder has an account relationship with the issuer, and funds are moved from the cardholder account to the funds pool controlled by the issuer. There is little opportunity for fraud. The security requirements for this type of transaction are limited to the issuer’s need to authenticate the card and verify the cardholder, and the card’s need to authenticate that the funds loaded were approved by the issuer.

In the case of an unlinked load, no presumption may be made as to the business relationship between the cardholder, the funds issuer, the card issuer, or the load acquirer. If this is not a cash load, the funds issuer needs to verify that the funds are requested by the legitimate account owner, which is normally done by the presentation of an enciphered PIN. The card issuer needs to ensure that the load acquirer is guaranteeing payment for the electronic value, and that the card is authentic. The load acquirer needs to ensure that the issuer is the true owner of the card, and, in the case of an apparent failure of the load, the load acquirer needs the card presented to authenticate the failure. Finally, the load acquirer and issuer need to ensure that the load cannot be completed by another entity.

Signatures for a linked load transaction are generated and validated in the following way:

- The card generates S_1 using card and load device data, and sends S_1 to the load device to be forwarded to the issuer.
- The load device sends S_1 in an authorization request to the issuer. The load device also provides for verification of the identity of the cardholder (with either on-line or off-line PIN verification) and forwards verification data in the authorization request. The issuer validates S_1 to authenticate the card and the data to be used in the transaction.
- The card issuer determines whether to allow the load to complete, and generates S_2, which secures the issuer's decision and that the issuer received the same data used by the card. The issuer sends S_2 to the load acquirer in the authorization response message.
- The load acquirer sends S_2 to the card to complete the load.
- After validating S_2 and completing the transaction, the card creates S_3, which is logged by the load device or the load acquirer. If there is a reversal message, the S_3 must be sent to the card issuer. If there is a settlement message sent to the card issuer after the S_3 is generated, S_3 should be included.

Signatures for an unlinked load are generated and validated in the following way:

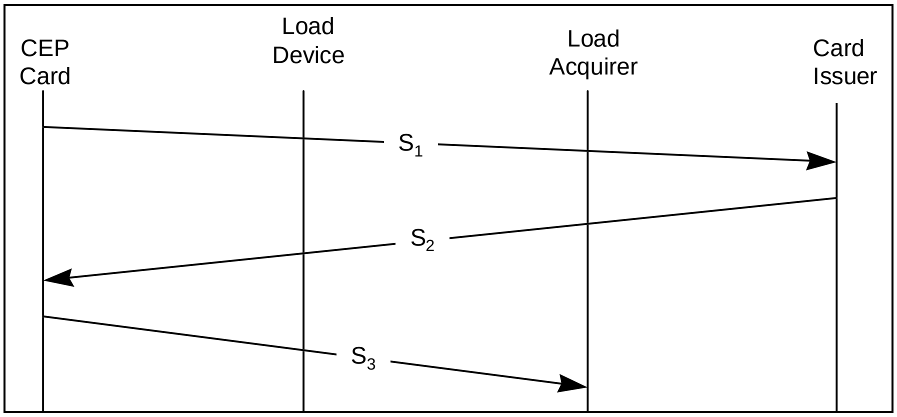
- The card generates S_1 , a random number (R_{CEP}) and a SHA-1 hash (H_{CEP}) containing R_{CEP} and card and load device data, and sends S_1 and H_{CEP} to the load device. H_{CEP} will provide proof to the LSAM of a valid error from the CEP card in a subsequent response to a Credit for Load command.
- The LSAM generates a random number (R_1) to be used as a session key between the load acquirer and the card issuer for this transaction.
- The LSAM encrypts R_1 under a key that allows secure transport to the card issuer.[†]
- The LSAM generates random numbers, R_{LSAM} and $R2_{LSAM}$. R_{LSAM} proves to the CEP card that the Credit for Load comes from a valid device. $R2_{LSAM}$ is used in exception processing to prove the load acquirer no longer owes the transaction amount to the card issuer.

[†] R_1 may be deciphered and re-enciphered by SAMs in intermediate nodes so that it arrives at the issuer in a key known by the issuer.

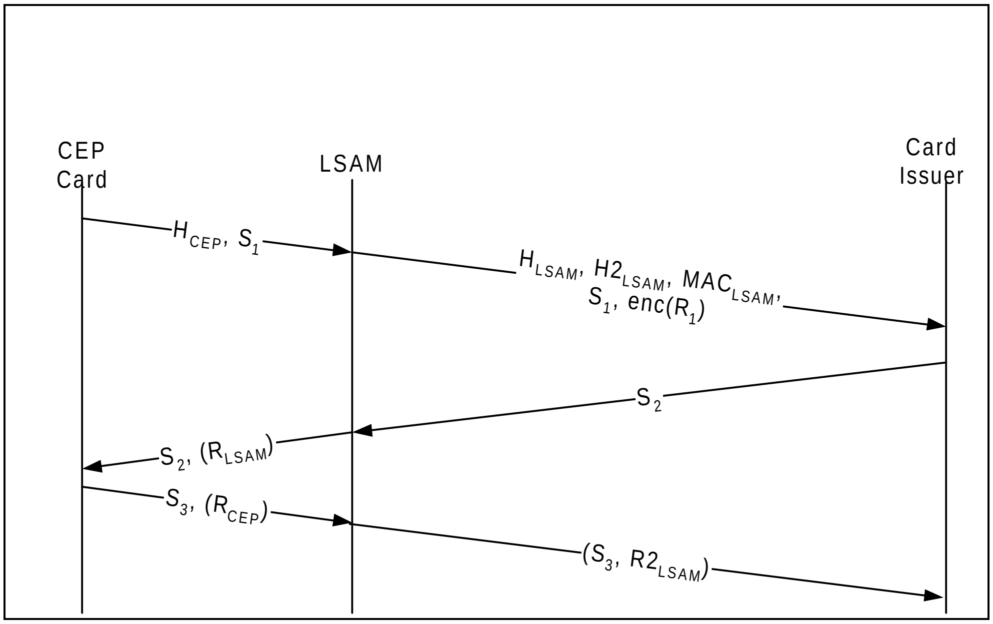
- The LSAM generates SHA-1 hash values, H_{LSAM} and $H2_{LSAM}$, using R_{LSAM}, $R2_{LSAM}$ and transaction data to be sent to the issuer.
- The LSAM generates MAC_{LSAM} to provide protection for the transaction data, H_{CEP}, H_{LSAM}, $H2_{LSAM}$ and S_1. It also provides a guarantee that the load acquirer owes the transaction amount to the card issuer.
- S_1, MAC_{LSAM}, H_{LSAM}, $H2_{LSAM}$ and the enciphered R_1 are sent to the issuer in an authentication request message. The issuer validates S_1 to authenticate the card and the data to be used in the transaction.
- The card issuer determines whether to allow the load to complete, and, for approvals generates a S_2 MAC containing H_{LSAM}, which secures the issuer's decision and that the issuer received the same data used by the card. The S_2 MAC is option for declines. If included on a decline, S_2 must not contain H_{LSAM}.
- After receiving a load approval, the load device proceeds as follows:
  - The Load Device sends S_2 and R_{LSAM} (a component of H_{LSAM}) to the card to complete the load.
  - After validating S_2 and completing the transaction, the card creates S_3 and sends S_3 to the LSAM. R_{CEP} is sent to the LSAM if there is an error.
  - S_3 is sent to the card issuer. $R2_{LSAM}$ is sent to the card issuer in case of an error where S_3 is not available. In case of an error, either the S_3 or the $R2_{LSAM}$ negates the guarantee of the H_{LSAM} and the load acquirer no longer owes the transaction amount to the card issuer.

The data to be protected by the S_1, S_2, S_3 and MAC_{LSAM} MACs and the H_{CEP}, H_{LSAM} and $H2_{LSAM}$ hash values are specified in the CEPS Technical Specifications.

Figure 1 - Linked load transaction signature flow



1. **Figure 2 - Unlinked load transaction signature flow**



3.4.2 Unload

Unloads are permitted only to an account controlled by the card issuer and are performed only at a load device under the control of the card issuer. The cardholder must have an account relationship with the card issuer, and funds removed from the card are credited to the cardholder account only after the card issuer authenticates the card. Cardholder verification is not necessary, but may be done.

Unload transaction security is provided in the same manner as the linked load transaction.

- The card generates S_1 using card and load device data, and sends S_1 to the card issuer to authenticate the card and the data.
- The card issuer validates S_1, and determines whether to allow the unload to complete. The card issuer generates S_2, which secures the card issuer's decision and that the card and the card issuer are using the same data for the transaction.
- After completing the transaction, the card generates S_3, which may be used by the card issuer to verify transaction completion. Since the load acquirer and

the card issuer are the same entity for unload transactions, the validity of S_3 can always be verified before funds are moved.

The data to be protected by the S_1, S_2 and S_3 MACs are specified in the CEPS Technical Specifications.

3.4.3 Currency Exchange

In a currency exchange transaction, funds flow from one slot within the card to another, and from one funds pool to another, both of which are under the control of the issuer. The issuer needs only to authenticate the card, and the card needs only to authenticate the issuer and that the data is the same as used by the issuer.

Signatures for the currency exchange transaction follow the same flow as in the linked load transaction. The load device establishes a connection between the card issuer and the CEP card. All security exists between the card issuer and the CEP card.

The card generates S_1, using data from the card and load device, and sends S_1 to the card issuer to authenticate the card and the data that is to be used in the transaction. The amount to be converted, as well as the amount in the currency it is converted into, is protected by S_2.

The card issuer validates S_1, calculates the amount of the transaction into the new currency, and determines whether to allow the exchange to complete. The card issuer generates S_2, which is sent to the card to allow the card to validate the card issuer's authenticity and to ensure that the data used by the card in the transaction is the same as the card issuer intended.

After completing the transaction, the card creates S_3, which is logged by the load device or the load acquirer or both.

In the case of an unsuccessful completion, exception processing outlined in the On-line Exception Processing section is performed.

The data to be protected by the S_1, S_2 and S_3 MACs are specified in the CEPS Technical Specifications.

3.4.4 Purchase

During a purchase transaction, the CEP card must ensure that it is dealing with an authentic POS device, and it must generate a signature to allow the card issuer to verify the integrity of the transaction. The POS device must ensure that it is dealing with an authentic card, and guarantee integrity of transactions and batches to the merchant acquirer. There is no requirement to validate the cardholder. A

PSAM is used in the POS device for cryptographic purposes.

For multiple step transactions, the CEP card can, at the card issuer's option, re-authenticate the PSAM at each step (mutual authentication), or it can rely on the authentication that was performed during the first step (dual authentication). The PSAM may authenticate the CEP card during each step. In the case of a reversal, the CEP card must re-authenticate the PSAM.

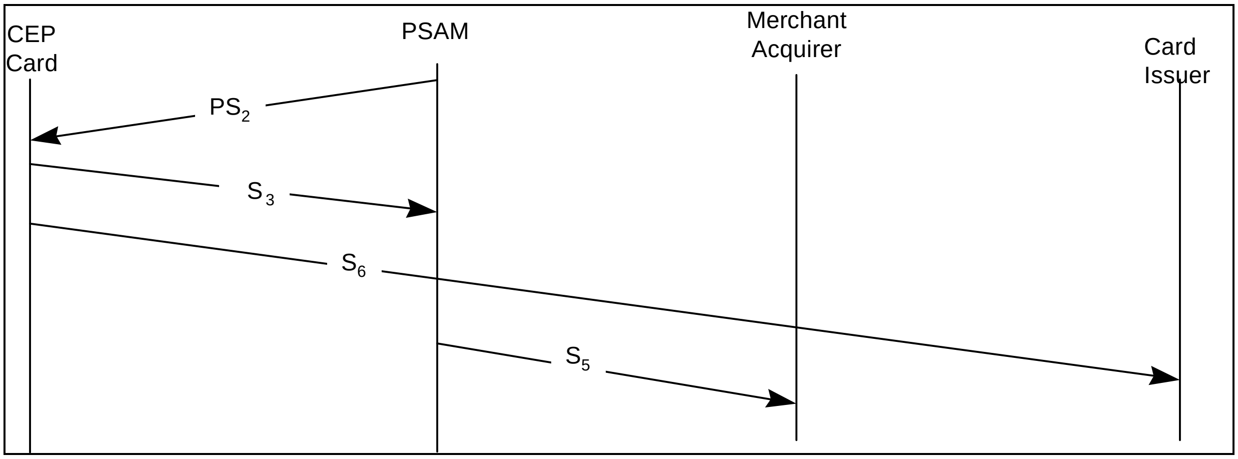
For incremental purchases in some terminal infrastructures (e.g. payphones where the PSAM is remote and inaccessible during voice communications), a merchant acquirer may decide to:

- 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.

Intermediate card validation by the POS device is optional for both the CEP card and the PSAM.

The data to be protected by the PS_2 signature and the S_3, S_4, S_5 and S_6 MACs will be specified in the CEPS Technical Specifications.

Figure 3 - Flow of signatures for a purchase transaction



3.4.5 Cancel Last Purchase Transaction

The Cancel Last Purchase transaction is a very sensitive transaction because, like a load transaction, it may be used to add value to the electronic purse. Thus, it is an attractive target for fraud. However, unlike the load, the Cancel Last Purchase is performed off-line without opportunity for the card issuer to authenticate the card or to approve the transaction. The card must ensure that the transaction is performed by the same POS device as was used for the purchase being canceled, and that the amount of the cancellation is the same as the amount of the purchase, or, in the case of an incremental purchase, the same as the amount of the last step.

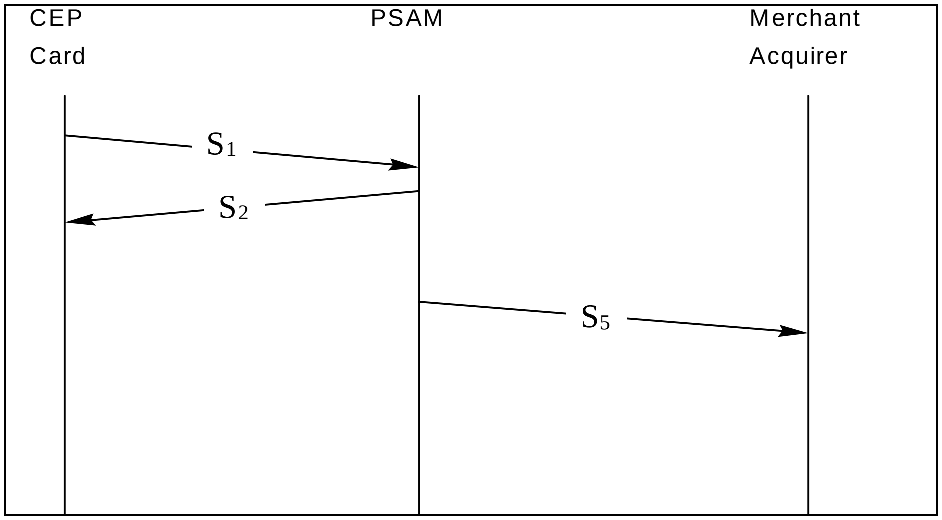
During a Cancel Last Purchase transaction, the CEP card is authenticated by the PSAM in the POS device. The PSAM authenticates that the purchase transaction being canceled was performed by the PSAM, and that the transaction being canceled is part of the active batch. The active batch is the batch that the POS device is currently adding new transactions to. The CEP card authenticates that:

- The PSAM is genuine.
- The PSAM is the same one used for the purchase transaction being canceled.
- The purchase transaction was the last transaction performed by the card.
- The purchase transaction has not previously been canceled.

The card issuer and the merchant acquirer also authenticate the transaction when they receive it.

The data to be protected by the S_1, S_2, S_4 and S_5 MACs are specified in the CEPS Technical Specifications.

Figure 4 - Flow of signatures for a cancel last purchase transaction



3.5 Transmission Security

3.5.1 Host to host

Transmissions between host systems should be protected by MACs based on unique keys that are shared by the nodes involved.

3.5.2 On-line Transactions

The transaction signatures ensure end to end integrity of transmitted data for load, unload, and currency exchange transactions.

3.5.3 Off-line Transactions

Every complete POS transaction is given a MAC by the PSAM and kept in the POS device memory until collected by the merchant acquirer. Each POS transaction is part of a batch of transactions that must be collected at the same time. Each batch must contain the total count and amount of the transactions in the batch. These totals are used by the merchant acquirer to ensure the integrity of the batch. The count and amount of the transactions in the batch must be protected by the S_4 MAC. This information is not part of the card issuer's verification process.

4. POS Transaction Requirements

4.1 Scope

This section defines the requirements for the Point of Sale or Point of Service (POS) transactions. The POS transactions addressed in this section are:

- Purchase.
- Incremental Purchase.
- Cancel Last Purchase.

Additionally, a purchase or the last increment of an incremental purchase may be reversed. This reversal is part of the transaction being reversed and is not a separate transaction.

4.2 Entities

4.2.1 POS Device

A POS device must contain at a minimum:

- A card acceptance device (CAD).
- Secure hardware for storing and processing data used to authenticate processing. This secure hardware is called a Purchase Secure Application Module (PSAM).

The PSAM must be a secure device. Some of the devices that may be used, if the security requirements are met, are a smart card or a hardware security module.

Scheme providers must assign unique identifying numbers to merchant acquirers who provide PSAMs. These merchant acquirers must then assign unique identifiers to PSAMs. As a result, each PSAM must have a unique ID composed of the scheme identifier, a merchant acquirer identifier, and the PSAM identifier. Each PSAM must maintain a transaction count. The unique PSAM ID and the transaction count are used during a conversation with a CEP card. The transaction count must not be reset during the life of the PSAM.

At a minimum, the PSAM must:

- Contain the CA public RSA key, the PSAM’s private RSA key and optionally the certificates that the POS device uses to perform mutual authentication with the CEP card.

- Perform the calculation required to generate a signature using the PSAM's private RSA key, to allow the CEP card to validate the PSAM.
- Contain one or more MAC keys used by the merchant acquirer to ensure the integrity of the data received from the POS device.
- Perform the calculation of MACs using the MAC keys in the PSAM.
- Generate random numbers.
- Contain the latest transaction count and amount of batches that have not been deleted from the POS device by the merchant or merchant acquirer.
- Contain the details of a transaction between the initialize command for that transaction and the initialize command for the next transaction.
- Be the entity that maintains control over the flow of a transaction, ensuring that all security is enforced.
- Perform the verification of signatures and certificates during a purchase and cancel last purchase transaction.

4.2.2 Merchant Acquirer

The merchant acquirer or its processor must:

- Collect and validate all transactions and provide acknowledgments to the POS device or to the merchant.
- Ensure that each batch of transactions is cleared and settled once and only once.
- Send transactions to card issuers or their processors in a standard format defined in agreement with the scheme provider.
- Participate in financial transactions with card issuers and their processors at the time that the transaction is sent. Funds move when the transaction moves.
- Ensure that CA public keys, aggregation parameters, blocking lists and issuer certificate revocation lists from the scheme providers are sent to the POS devices.

4.2.3 Processors

Transactions may flow directly from a merchant acquirer to a card issuer, however, many times the transactions must be processed by additional nodes in the network connecting the merchant acquirer and the card issuer. To ensure 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 MAC keys with connecting processors, create a MAC on each transmission sent to another processor, and verify the MAC on each transmission received from another processor.
- Send transactions to other processors in a standard format defined in agreement with the scheme provider.
- 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.
- If a supported scheme provider has a dispute resolution process, participate in that dispute resolution process with connecting processors to resolve any issues related to invalid transactions. These resolution processes should include a mechanism for repayment of funds associated with invalid transactions.

Processors must be certified by the scheme provider and must act as an agent for one or more of the following entities:

- A card issuer.
- A merchant acquirer.
- A scheme provider.

4.2.4 Card Issuer

The card issuer must:

- Receive POS transactions from one or more merchant acquirers.
- Ensure that the POS transactions are successfully received and logged.
- Settle with the sending processor for all transactions received.
- Confirm that all purchase transactions were made by a valid CEP card by verifying the S_6 MAC placed on each transaction by the CEP card using a derived card MAC key.
- Establish procedures to identify transactions made by counterfeit CEP cards.
- Establish a procedure to identify duplicate or fraudulent transactions.

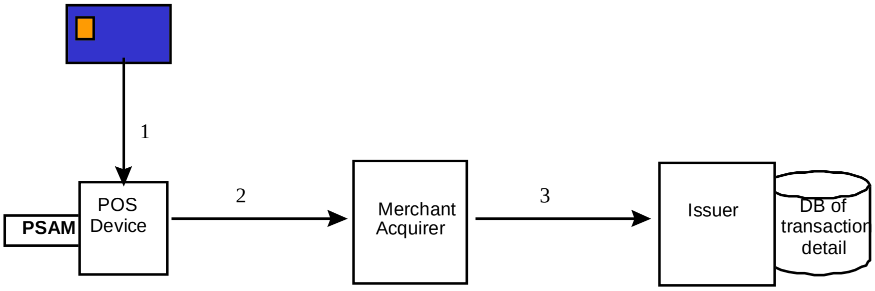
[‡] The merchant acquirer and the card issuer are considered processors, as well.

- Arrange for settlement adjustments for duplicate, invalid, or fraudulent transactions using dispute procedures established by the scheme provider.
- Update its funds pool based on the net value of the POS transactions or advise its funds pool administrators to do so.
- Reconcile its POS transaction data with its purchase processor and funds pool administrator on a regular basis.

4.3 Overview of POS Processing

4.3.1 Processing by Responsible Entity

The diagram below provides an overview of POS processing and indicates which entity is responsible for which processing.



1. The POS process begins with an interaction between the CEP card and the POS device. The CEP card and the PSAM in the POS device perform a mutual authentication process, using a combination of public key and symmetric cryptography. The value of the electronic purse in the CEP card is then adjusted. When the transaction completes, the PSAM computes MACs to validate the transaction and the batch. Information about the transaction is placed in a data store in the POS device.
2. Periodically, the transactions in the POS device's data store are collected by a Merchant Acquirer.

   The Merchant Acquirer performs the following operations:

   - Verification of the MACs placed on transactions by the PSAM.
   - Consolidation of transactions from multiple POS devices.

1. The merchant acquirer sends POS transactions to the card issuer. Settlement takes place. The exact responsibilities for settlement are based on the business arrangement between the card issuer and the merchant acquirer.

Transaction detail is stored by card issuers to support:

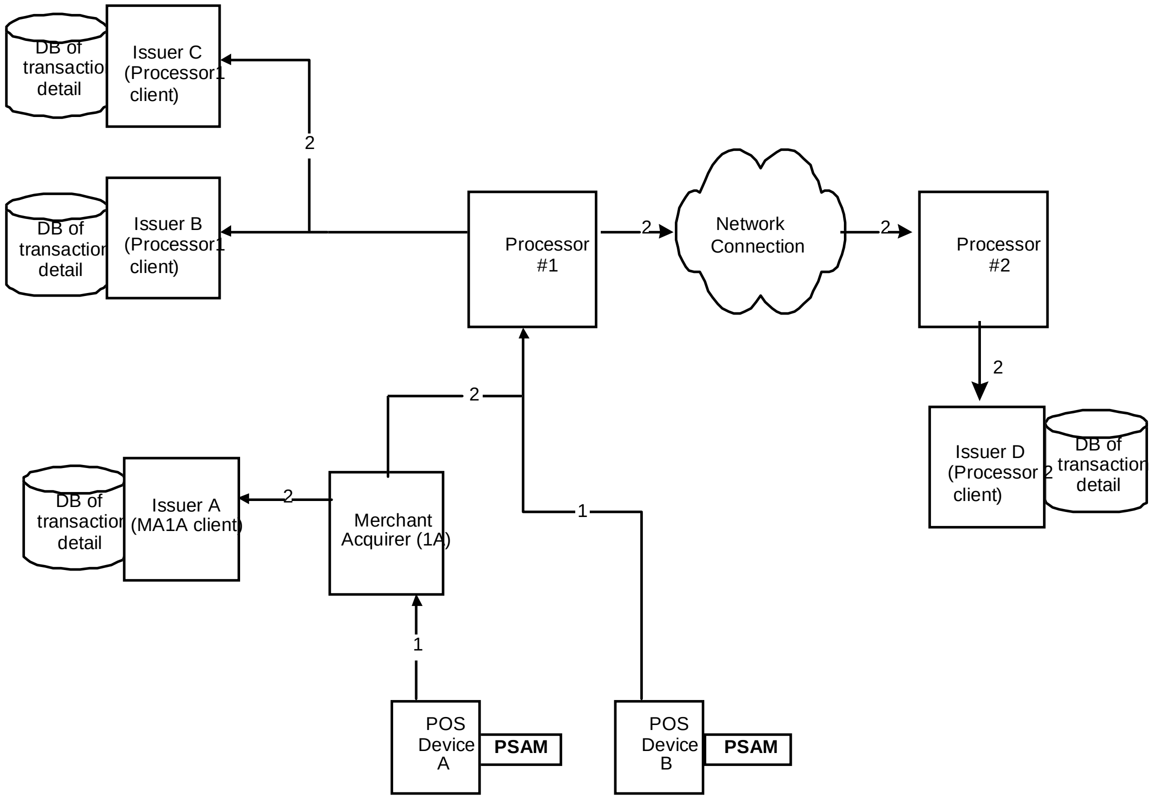
- Settlement reconciliation.
- Liability accounting.
- CEP card history.
- CEP card overspending accounting.
- Fraud analysis.
- Duplicate transaction analysis.
- Load accounting and funds pool administration.

4.3.2 Possible Processing Flows

In some cases, merchant acquirers may have agents or processors performing the responsibilities described above. Figure 5 shows some of the flexibility that is possible for POS processing.

Some schemes allow transactions to be stored by an intermediate processing entity and not routinely sent to the card issuer, This process is called truncation. If the scheme permits truncation, and the card issuer allows the process, transactions may be truncated at any processing entity designated as an agent by the card issuer. The entity truncating the transaction must make the detailed transaction available to the card issuer upon request.

Figure 5 - Possible POS Processing Flow



1. Transactions are transmitted from the POS device to the merchant acquirer processor responsible for collecting POS transactions. In Figure 5 - Possible POS Processing Flow, POS Device A transmits transaction data to Merchant Acquirer 1A, which is acting as its own processor. POS Device B transmits transaction data to Processor #1, in its role of the processor for one or more merchant acquirers.

2. The merchant acquirer processor sends all transactions to the card issuer or to a processor accepting POS transactions on behalf of the card issuer. In Figure 5, Merchant Acquirer 1A transmits transactions directly to Issuer A and sends transactions for Issuer B, Issuer C, and Issuer D to Processor #1. A processor accepts transactions for its card issuers and transmit all transactions for another processor to that processor. In Figure 5, Processor #1 sends transactions directly to Issuer B and Issuer C and sends transactions for Issuer D to Processor #2.

   When an entity in the process sends or receives a transaction, that entity must take part in the settlement process for the transaction. Settlement processing must take place with both the sender of the transaction and the recipient of the transaction. One party to the settlement process must arrange for money to be paid or collected and the other party must reconcile the settlement amount. The exact responsibilities for settlement must be based on the business arrangement between the entities.

4.4 Processing Rules

POS processing must comply with the following rules:

- The scheme provider must ensure that the entire process between merchants, merchant acquirers, card issuers, and processors is auditable and reconcilable.
- Transactions must be archived at all processing points after the POS device. The length of time that the transactions must be archived will vary by type of processing point.
- The card issuer is responsible for funds pool administration.
- Only transactions that have been validated are to be sent to a card issuer for payment. Payment is made when the transaction is received. If errors in the card issuer MAC are discovered by the card issuer during its processing of the transactions, a dispute mechanism, established by the scheme provider, may be used to have money refunded. The card issuer is not required to submit all transactions with MAC errors to the dispute process.
- If a scheme provider establishes a central error repository, all transactions for the scheme with MAC errors must be sent to that central error repository whether or not they are submitted to the dispute process.
- Payment for a transaction is only required when a detail transaction is submitted for payment. A merchant acquirer may choose to pay the merchant using the batch total. Card issuers in a scheme that allows aggregation may choose to pay the merchant acquirer using aggregation totals. The functional requirements for aggregation are described in section 4.6.
- The timing of payment to the merchant must be established between the merchant and the merchant acquirer.
- If another application on a CEP transfers value from the CEP application, the transfer must be reported as a purchase transaction.

4.5 Processing Flows

This section provides the processing flows for transactions that take place at a POS device. All of the flows in this section show processing between the POS device, the merchant acquirer, and the card issuer. However, in many cases, the actual flow must involve one or more processors acting as an agent for either the merchant acquirer or the card issuer. The flows included in this section are:

- Purchase Transaction.
- Subsequent Steps of an Incremental Purchase Transaction.
- Reversal of a Purchase Transaction.

- Cancel Last Purchase Transaction.
- Processing of a Batch of Transactions.

The first four flows show the interaction between the CEP card and the POS device. The final flow shows the processing after a batch is closed and sent to the merchant acquirer.

4.5.1 Purchase Transaction

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.

Symmetric and asymmetric cryptography are used for these transactions. The CEP card performs mutual authentication with the POS device using a combination of a public key algorithm (RSA) and a symmetric algorithm (triple DES), and the CEP card signs each transaction using a symmetric MAC key. This MAC allows the card issuer to authenticate the data and CEP card used in the transaction. The MAC validates all information forwarded to the card issuer that has been seen by the CEP card.

Some local regulations require that a purchase may be made for up to six months after a CEP card has expired. To support this requirement, an additional date, an off-line expiration date, must be on the CEP card. This off-line expiration date must be in the response from the card instead of the actual expiration date for all off-line transaction. Issuers who are not required to allow use of CEP cards after the expiration date must set the off-line expiration date to be equal to the actual expiration date of the card. A CEP application that has been deactivated must not be accepted for a purchase transaction.

Figure 6 - POS Processing Flow 1 - Purchase Transaction

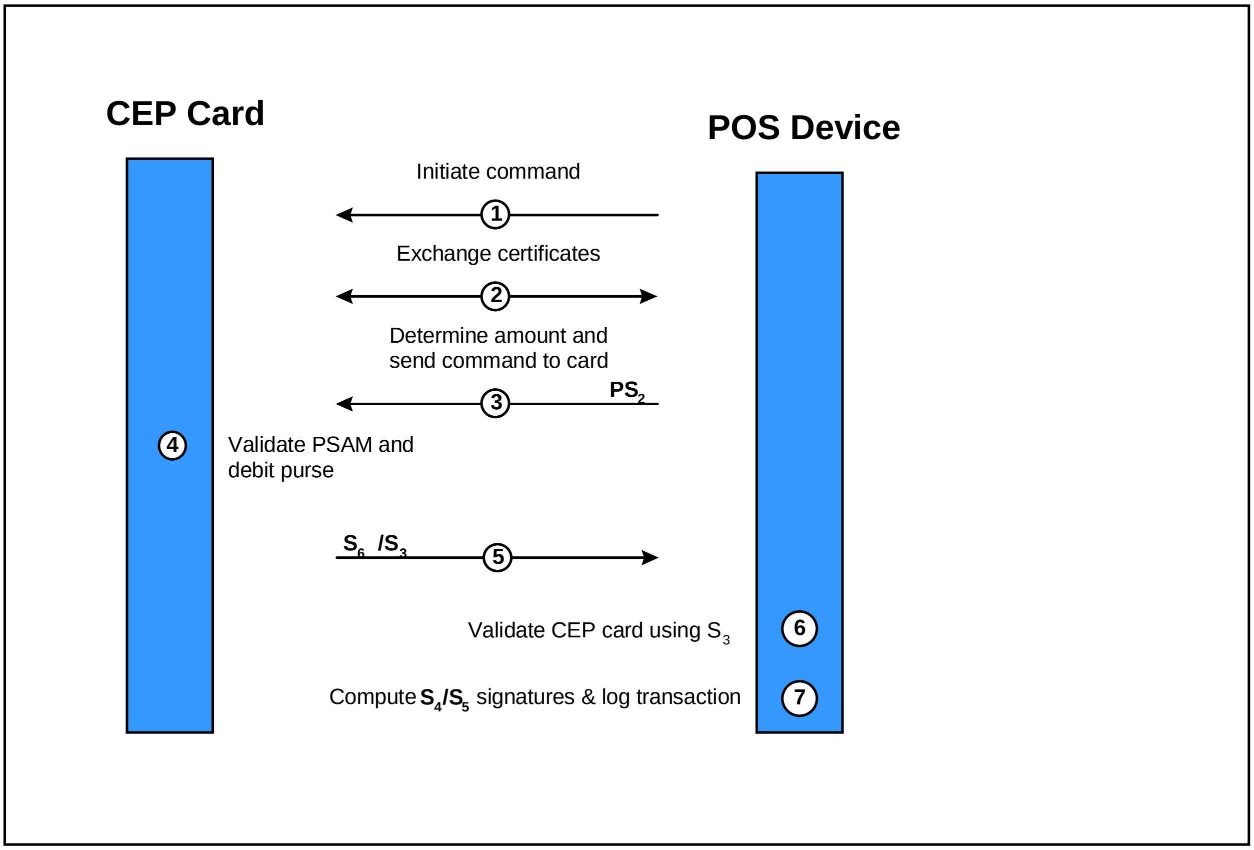

CEP Card
POS Device
Initiate command
1
Exchange certificates
2
Determine amount and send command to card
3
PS$_2$
4
Validate PSAM and debit purse
S$_6$ /S$_3$
5
Validate CEP card using S$_3$
6
Compute S$_4$/S$_5$ signatures & log transaction
7

Figure 6 shows the basic processing flow for a purchase transaction. The steps in the flow are:

1. The POS device initiates the purchase after the CEP card is inserted in the POS device.

   If the POS device supports multiple applications or multiple transaction types, an interaction between the terminal and consumer or sales agent determines the CEP application and the function to be performed (purchase).

   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. A POS device normally only supports one currency and the CEP card must have a slot containing that currency. If a POS device supports multiple currencies, the cardholder selects the currency to be used for the transaction. The CEP card must have a slot containing the currency selected. If the CEP card is locked, the transaction is terminated.

2. The POS device and the CEP card exchange certificates to mutually authenticate the CEP card and the PSAM. In some cases, either the CEP card

or the POS device may already have the appropriate public keys in storage. The exchange may be bypassed if the public keys are in storage.

3. The amount of the purchase is entered into the POS device. The POS device displays the amount of the transaction to be performed to the cardholder. The cardholder is required to accept or reject the transaction. The debit command is sent to the CEP card after the cardholder accepts the purchase amount. The command sent to the CEP card contains the PS_2 signature computed by the PSAM.

4. The CEP card uses the certificates received and the PS_2 to authenticate the terminal.

   The CEP card decrements the value of the purchase from the purse, creates the S_3 MAC and the card issuer S_6 MAC, and logs the transaction.

5. The CEP card sends a response containing the S_3 and S_6 to the POS device.

6. Using the public key signature contained in the response, the POS device validates the CEP card and completes the mutual authentication.

7. If this is not the last step of an incremental purchase, processing continues with step 7 in section 4.5.2. If the transaction is to be reversed, processing continues with step 7 in section 4.5.3. Any transaction aggregation processing if applicable is performed, the amount of a purchase is added to the total amount for the batch, and the count of transactions in the batch is incremented by one. The PSAM in the POS device generates a merchant acquirer S_5 MAC to complete the transaction and logs the transaction. The count and amount of the transactions in the batch must be protected by the S_4 MAC. The transaction and the MACs must be kept in a data store associated with the POS device until the merchant acquirer collects them.

4.5.2 Subsequent Steps of an Incremental Purchase Transaction

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.

This flow begins as a normal purchase transaction, as in 4.5.1. However, step 7 of that flow is replaced by the flow in Figure 7.

Figure 7 - POS Processing Flow 2 - Subsequent Steps of an Incremental Purchase Transaction

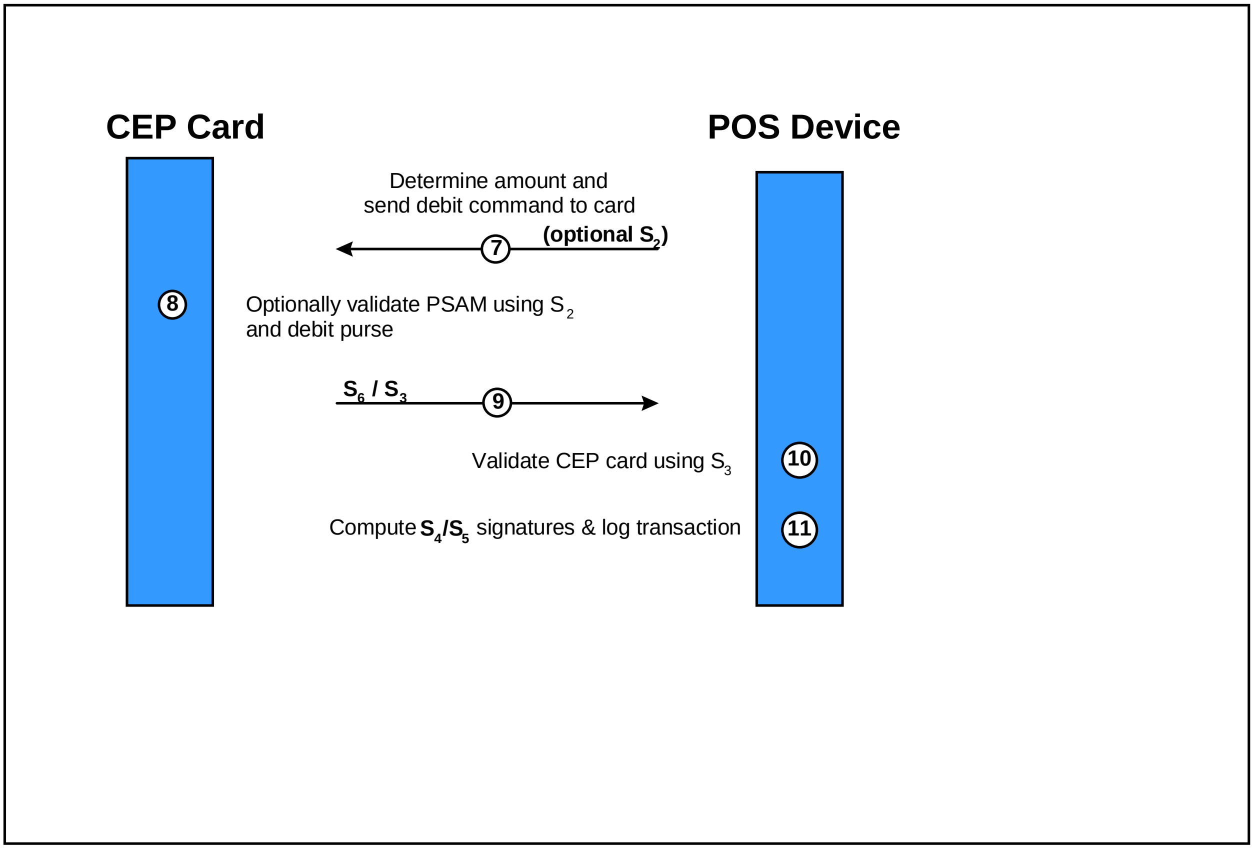

CEP Card
POS Device
Determine amount and send debit command to card
(optional S_2)
7
8
Optionally validate PSAM using S_2 and debit purse
S_6 / S_3
9
Validate CEP card using S_3
10
Compute S_4/S_5 signatures & log transaction
11

Figure 7 shows the basic processing flow for subsequent steps of an incremental purchase transaction. These steps follow step 6 of the purchase transaction processing flow. The steps in the flow are:

7. The amount of the next incremental purchase is determined. If the CEP card settings indicate that mutual authentication is to be used for subsequent steps of an incremental purchase command, the debit command sent to the CEP card contains the S_2 MAC computed by the PSAM.

8. If the S_2 has been sent to the CEP card, the CEP card authenticates the terminal using the previously exchanged session key and the S_2.

   The CEP card decrements the value of the incremental purchase from the purse, creates the S_3 MAC and the card issuer S_6 MAC and updates its internal log with the transaction.

9. The CEP card sends a response to the POS device with the S_3 and S_6.

10. The POS device authenticates the CEP card using the S_3 MAC contained in the response.

11. If this is the last increment of a purchase transaction, the amount of a purchase is added to the total amount for the batch, and the count of transactions in the

batch is incremented by one. The PSAM in the POS device generates a merchant acquirer S_5 MAC to complete the transaction and logs the transaction. The count and amount of the transactions in the batch must be protected by the S_4 MAC. The transaction and the MACs must be kept in a data store associated with the POS device until the merchant acquirer collects them. The logged data must include the total amount of the purchase and the amount of the last increment.

If this is not the last increment of a purchase transaction, processing continues with step 7 of this flow.

4.5.3 Reversal of a Purchase Transaction

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. The CEP card must authenticate the PSAM using certificates previously exchanged.

Only the last increment of an incremental purchase may be reversed. A reversal of a purchase transaction may only occur if:

- the CEP card has not been removed from the POS device, and
- the S_5 for the transaction to be reversed has not been generated by the PSAM.

This flow begins as a normal purchase transaction, as in 4.5.1. However, step 7 of that flow is replaced by the flow in Figure 8.

Figure 8 - POS Processing Flow 3 - Reversal of a Purchase Transaction

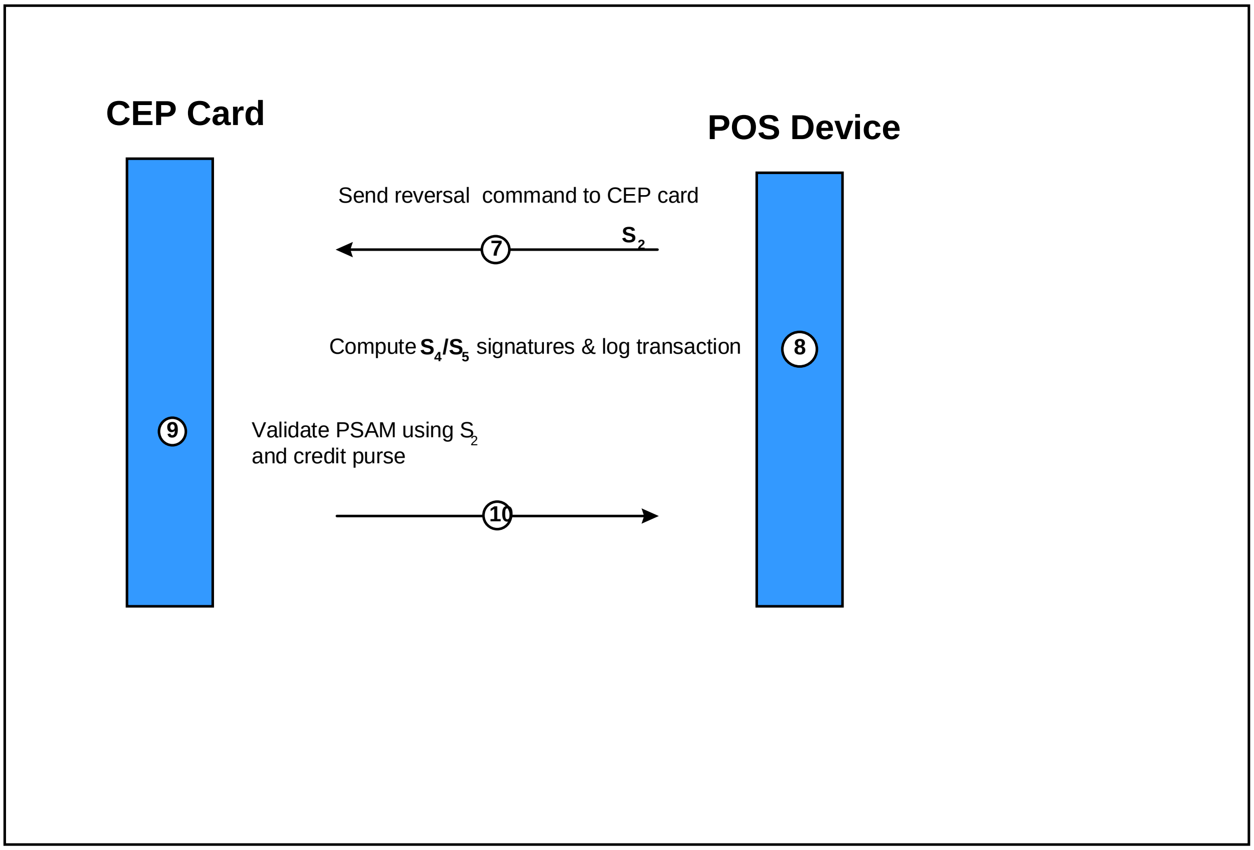

CEP Card
POS Device
Send reversal command to CEP card
S2
7
Compute S4/S5 signatures & log transaction
8
9
Validate PSAM using S2
and credit purse
10

Figure 8 shows the basic processing flow for a reversal. These steps follow step 6 of the purchase transaction processing flow. The steps in the flow are:

7. The amount to be reversed is the amount of the last step of the transaction. The reversal command sent to the CEP card contains a S_2 MAC computed by the PSAM.

8. The PSAM in the POS device generates a merchant acquirer S_5 MAC for the transaction, computes a new S_4 MAC on the updated batch total count and amount, and logs the transaction. The transaction and MACs are kept in a data store associated with the POS device until the merchant acquirer collects them. The logged data must include the total amount of the purchase, the purchase amount that was reversed, and an indication that the transaction was reversed.

9. The CEP card authenticates the PSAM using the certificates previously received and the S_2.

   The CEP card increments the value of the purse and logs the transaction.

10. The CEP card sends a response to the reversal command to the POS device. The reversal is considered to be successful even in the event of a negative response or no response from the CEP card.

4.5.4 Cancel Last Purchase Transaction

POS devices are not required to support the cancel last purchase command. If this command is supported, the POS device must have security to prevent unauthorized or fraudulent use of the transaction. This transaction is only valid if the transaction to be canceled is the last transaction completed by the CEP card. 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.

Figure 9 - POS Processing Flow 4 - Cancel Last Purchase Transaction

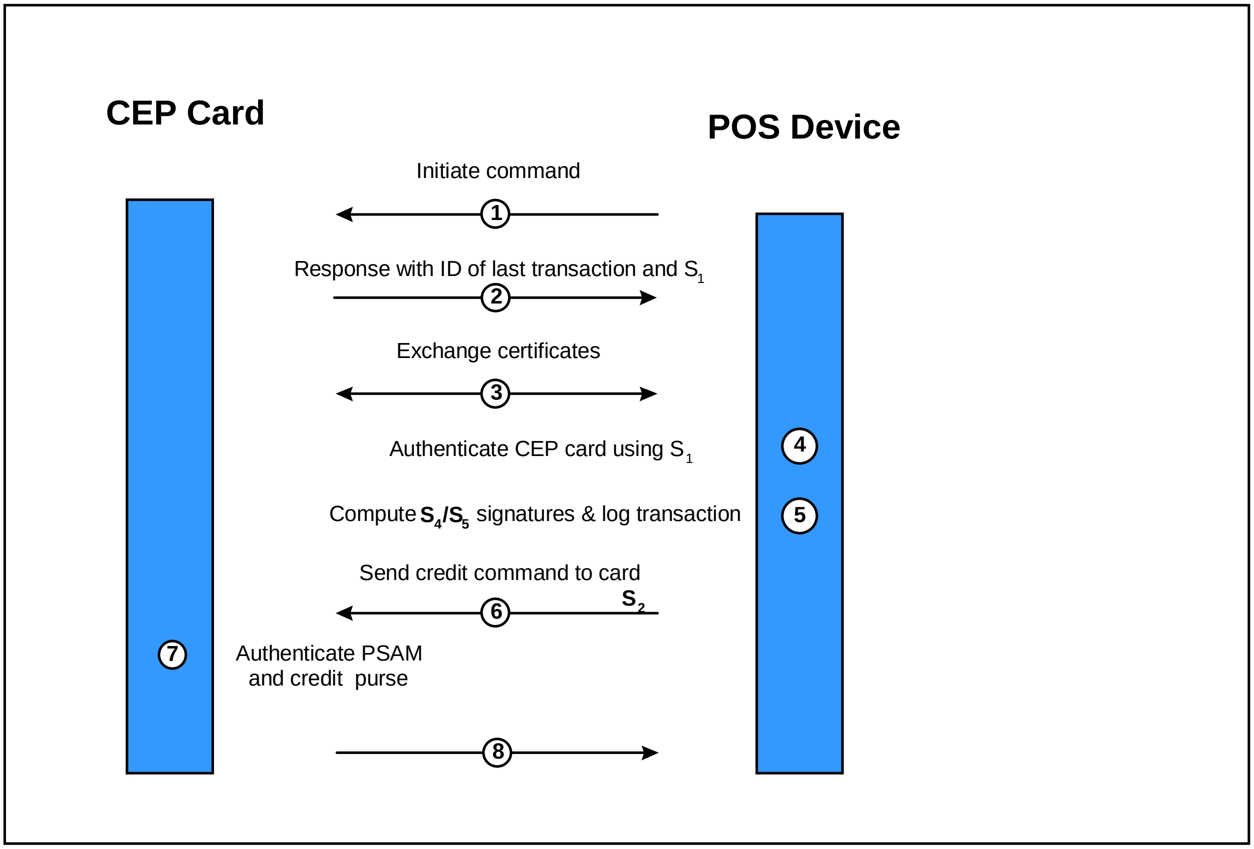

CEP Card
POS Device
Initiate command
1
Response with ID of last transaction and S_1
2
Exchange certificates
3
Authenticate CEP card using S_1
4
Compute S_4/S_5 signatures & log transaction
5
Send credit command to card
S_2
6
7
Authenticate PSAM and credit purse
8

Figure 9shows the basic processing flow for a cancel last purchase transaction. The steps in the flow are:

1. After the CEP card is inserted in the POS device, the POS device initiates the cancel last purchase transaction.

   If the POS device supports multiple applications or multiple transaction types, an interaction between the terminal and consumer or sales agent determines the CEP application and the function to be performed (cancel last purchase transaction).

2. The CEP card verifies that the PSAM is the PSAM used in the original transaction, computes a S_1 MAC using the same DES session key that was used for the purchase transaction being cancelled, and responds to the POS device with the S_1 and the identification of the last transaction. If the purchase transaction to be canceled has been canceled or is not part of the active batch, the command is not allowed.
3. The PSAM either retrieves or re-derives the DES session key used for the purchase transaction being cancelled. The POS device authenticates the CEP card using this key and the S_1 MAC.
4. The PSAM in the POS device generates a merchant acquirer S_5 MAC for the transaction and a new S_4 MAC for the batch total count and amount and logs the transaction. The amount of the canceled last purchase transaction is subtracted from the header amount. The transaction is kept in a data store associated with the POS device until the merchant acquirer collects it.
5. A credit command, which contains the S_2 MAC computed by the PSAM using the session key, is sent to the CEP card.
6. The CEP card authenticates the terminal using the S_2 MAC and the session key from the purchase transaction being cancelled.

   The CEP card increments the value of the purse and logs the transaction. The CEP card verifies that the cancellation amount is equal to the amount of the last step of the purchase transaction.
7. The CEP card sends a response to the POS device.

4.5.5 Processing of a Batch of Transactions

A transaction collection process must exist. Data being transmitted from the POS devices must be transmitted in a manner that ensures integrity of the data. The merchant acquirer must acknowledge the receipt of the batch to either the POS device or the merchant. The timing of the acknowledgment will vary based on the collection process. After a batch has been acknowledged by the merchant acquirer, it may be deleted from the POS device.

The processing of a batch of transactions, after they are collected from the POS device, is the same for all transaction types.

A single collection process for merchants must be available at a POS device. Data being transmitted from POS devices must be transmitted in a manner that ensures integrity of the data.

Figure 10 - POS Processing Flow 5 - Processing of a Batch of Transactions - 1

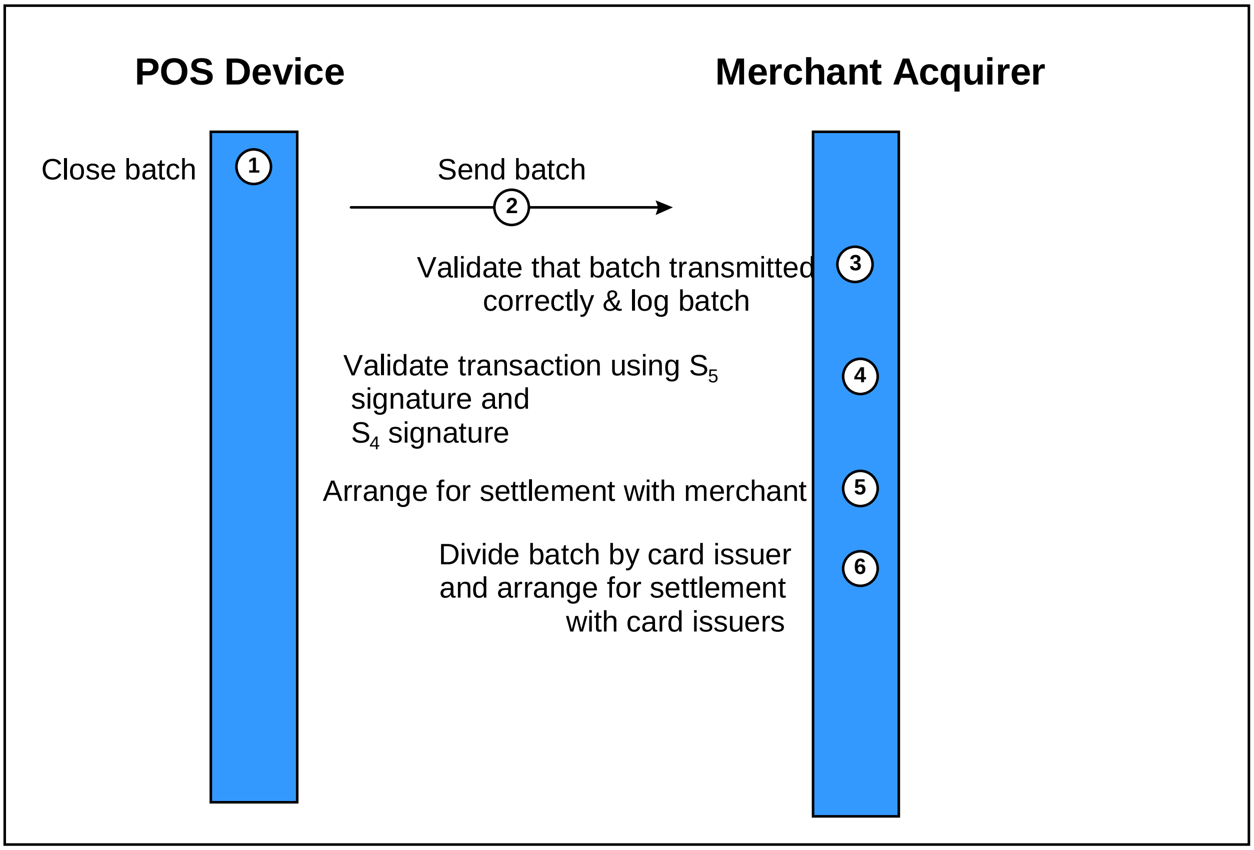

POS Device
Merchant Acquirer
Close batch
1
Send batch
2
Validate that batch transmitted correctly & log batch
3
Validate transaction using S_5 signature and S_4 signature
4
Arrange for settlement with merchant
5
Divide batch by card issuer and arrange for settlement with card issuers
6

Figure 11 - POS Processing Flow 5 - Processing of a Batch of Transactions - 2

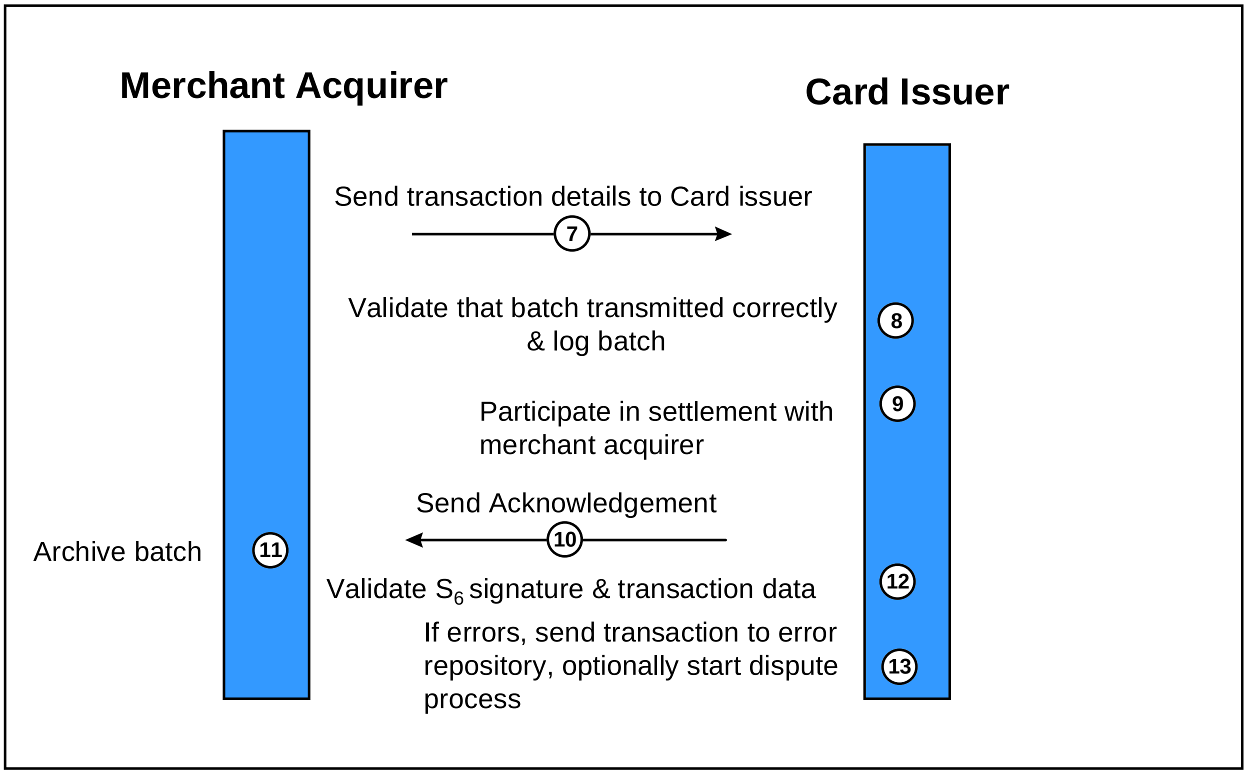

Merchant Acquirer
Card Issuer
Send transaction details to Card issuer
7
Validate that batch transmitted correctly & log batch
8
Participate in settlement with merchant acquirer
9
Send Acknowledgement
10
Archive batch
11
Validate S_6 signature & transaction data
12
If errors, send transaction to error repository, optionally start dispute process
13

Figure 10 and Figure 11 show the basic processing flow for processing a batch of transactions. The steps in the flow are:

1. The POS device closes the batch when the batch is collected. Collection may be initiated by the POS device, the merchant, or by the merchant acquirer.
2. The batch is sent to the merchant acquirer. Delivery may involve transmission to multiple intermediate locations or it may be direct to the merchant acquirer.
3. The merchant acquirer validates the batch to ensure that it has been transmitted correctly and enters it into the log.
4. The merchant acquirer validates the S_5 MAC on each transaction and the S_4 MAC. This validation is proof that all transactions sent to a card issuer occurred as a result of a successful conversation between a valid CEP card and the PSAM in the POS device. The minimum acceptable validation process is the verification by the merchant acquirer of a MAC, created by a symmetric key in the PSAM.
5. The merchant acquirer arranges for settlement with the merchant. The merchant is credited with the value of the batch. The merchant acquirer is debited for the value of the batch. The value of the batch is calculated as follows:

Amount = Purchases - Cancel Last Purchases

6. The merchant acquirer divides the batch by card issuer and arranges for settlement with each card issuer. Each card issuer is debited for the amount of all the transactions sent to that card issuer. The merchant acquirer is credited with the sum of the amounts debited to all card issuers.
7. The merchant acquirer sends the purchase and cancel last purchase transactions to the card issuer. All transactions should be secured using a MAC generated by a shared MAC key.
8. The card issuer validates that the transactions were transmitted correctly and logs the transactions.
9. The card issuer participates in the settlement process with all merchant acquirers that have sent transactions.
10. The card issuer acknowledges the receipt of the transactions to the merchant acquirer. The timing of the sending of acknowledgment will vary based on the connection between the entities involved in the transmission of the transactions. The acknowledgment may be included in the file transmission protocol or be part of standard network processing.
11. The merchant acquirer archives the acknowledged transactions.
12. The card issuer validates the S_6 and the transaction data for purchase transactions.
13. If a bad S_6 is identified during the validation process, the card issuer sends that transaction to the scheme error repository, if a scheme error repository has been established, and may optionally begin the dispute procedure.

4.6 POS Aggregation

4.6.1 Overview

POS aggregation is a feature that may only be available at the discretion of the scheme providers and their card issuers and is optionally supported at POS devices. The use of aggregation increases the card issuer’s risk as not all of the detail records will be available to the card issuer for risk management. Aggregation affects the auditability of a CEP system. It demands a high dependency on IC hardware security.

Only certain POS devices, which have been installed at merchants approved for aggregation by both the scheme provider and merchant acquirer, must be permitted to aggregate transactions. Card issuers must determine if their CEP cards must allow aggregation. POS devices must only aggregate transactions from CEP cards when the CEP card allows aggregation.

The PSAM must only be permitted to aggregate transactions for a scheme with which the merchant has an aggregation agreement. The AID of the card application must be used to determine the scheme. For each scheme that allows this merchant to perform aggregation, the PSAM must have a monetary amount above which it is not permitted to aggregate.

The decision to aggregate cannot be made until the last increment of a purchase transaction is complete. Cancel last purchase transactions must not be aggregated.

4.6.2 Processing

If the business rules allow this transaction is to be aggregated, the PSAM must determine if it has an aggregation record for the card issuer. If the PSAM does not have an aggregation record for the card issuer, a new aggregation record for the card issuer must be created. If the PSAM has insufficient space to create a new aggregation record for the card issuer, the transaction must not be aggregated.

If the transaction is to be aggregated, the amount of the transaction must be added to the aggregation record for the card issuer. The count of aggregated transactions in the aggregation record must be increased by 1. The PSAM must create a MAC on the updated aggregation record. Aggregation records by card issuer must be stored in the PSAM. They may also be stored in the POS device as well. The PSAM must increase the total count and amount of the active batch by the amount of the aggregated transaction.

The aggregated totals by card issuer must be transmitted to the merchant acquirer at the same time and manner as the non-aggregated detail transactions in the batch.

4.7 Exception Processing

This section describes the required exception processing for the merchant acquirer and card issuer based on their validation of the POS data.

1. Each POS transaction completed at the POS device is given a S_5 MAC by the PSAM, which is used by the merchant acquirer to validate that the transactions were made at a POS device with a valid PSAM. The batch total count and amount must be protected by the S_4 MAC, which must also be validated by the merchant acquirer.

2. The merchant acquirer validates the PSAM's MACs prior to accepting the POS transactions for payment. In addition, selected data elements are validated to ensure correct processing by the POS device and its PSAM.

3. Each purchase transaction is signed by the CEP card with a S_6 MAC, which is used by the card issuer to validate that the transaction was made with a legitimate, not counterfeit, CEP card. The card issuer validates the CEP card's MAC.

4. Payment decisions are based on signature validations, scheme provider rules, and merchant and merchant acquirer agreements.

5. Errors may be introduced by a malfunctioning PSAM or POS device software, by key management problems, or through the transmission process, as well as through fraudulent activities of another entity. When a batch or POS transaction fails validation, the merchant acquirer or card issuer must follow exception procedures that affect payment to the merchants and payment from the card issuer. The batch must be analyzed to determine clearable transactions out of a corrupted batch.

6. A transaction that fails a merchant acquirer validation cannot be forwarded for payment unless resolved.

7. After investigation, if the merchant acquirer decides, based on scheme rules, to accept the transactions, a method must exist to settle them and forward them to the card issuer.

8. Procedures for investigation, resubmission, and manual adjustment may be established between the merchant acquirer and its merchants for batches containing rejected transactions.

9. A transaction that passes merchant acquirer validations and is forwarded to the card issuer is paid for by the card issuer. If the transaction does not pass card issuer validations, the card issuer may follow the scheme provider's dispute procedures.

10. Purchase transactions that have an invalid MAC are forwarded to the scheme provider for analysis if the scheme provider has established a central error repository.

11. Merchant acquirers may institute pay on header arrangements for providing payment to their merchants. In this arrangement, the merchant acquirer relies on the header validation to determine payment to the merchant if transaction detail is missing due to some problem. The specific rules covering pay on header arrangements are outside the scope of this document.

12. Pay on detail is the default payment arrangement for merchant acquirers to provide payment to their merchants. In this arrangement, the merchant acquirer relies on the POS transaction S_5 MAC to determine acceptance. Merchants are paid only for valid POS transactions.

13. Valid batch total counts and amounts are required in any payment arrangement. Batches where the totals have errors that cannot be resolved through investigation must be rejected.

14. All POS transactions, except for duplicates, are forwarded to the card issuer.

    The following transactions are forwarded to the card issuer for payment and for CEP card history information:

- POS transactions that were accepted by the merchant acquirer.
- POS transactions that have resolved errors are additionally flagged with an error code indicating the type of validation failure.

The card issuer pays based on the total amount of transactions forwarded by the merchant acquirer for payment.

POS transactions that were rejected for payment by the merchant acquirer are flagged with an error code indicating the type of validation failure and are forwarded to the card issuer for CEP card history information only.

5. Load, Unload, and Currency Exchange Requirements

5.1 Scope

This sections defines the requirements for processing load, unload, and currency exchange transactions within an electronic purse scheme.

All load transactions are on-line transactions. Authorization of funds for load transactions must require a form of cardholder verification. The load device must support on-line encrypted PIN or off-line PIN verification. Off-line PIN verification must include both encrypted and unencrypted PIN. The card verification method indicator (CVMI) in the CEP card must specify support of on-line PIN verification and at least one method of off-line PIN verification (encrypted or unencrypted). Where it is necessary for a CEPS system component to distinguish between on-line and off-line cardholder PIN verification, a flag must be set in the transaction. Since these transactions are on-line to the issuer, the issuer has the opportunity to lock the card or the application. These transactions are not available to a card that has already been locked.

The definition of funds account access and the computation and collection of fees are outside the scope of this effort.

5.2 Load Requirements by Entity

The following entities perform the load, unload and currency exchange functions for CEPS transactions and are described in more detail below:

- Load device.
- Load acquirer.
- Funds issuer.
- Card issuer.
- Network nodes and processors.

5.2.1 Load Devices

Load devices may be modified ATMs, cash acceptance devices, personal ATMs, and other devices that support load of value over the public networks such as the telephone and the Internet.

Load devices that are accessible for use by the general public should support multiple sources of funding for the load transaction, and should support linked and unlinked load transactions. Load devices provided by financial institutions that issue CEP cards may also support the unload transaction.

Load devices must be on-line capable devices with a secure PIN pad. Load devices must provide either a secure on-line method of PIN encryption or both encrypted and unencrypted off-line PIN verification. Either the load device or the load acquirer must have an LSAM for cryptographic processing.

Load devices that are not interoperable are outside of the scope of this requirement.

5.2.2 Load Acquirer

The load acquirer is responsible for:

- The load host system.
- The load device.
- The LSAM.
- Participating in the settlement process for unlinked loads with the funds issuer and the card issuer.
- Monitoring and reconciling both completed and uncompleted transactions.

The load acquirer must ensure that mutual authentication is performed between the load device and the load host system.

The load acquirer’s load host system is comprised of hardware and software that is required to perform the following:

- Process load requests on-line.
- Communicate with the load device.
- Communicate with a network.
- Initiate a card authentication request to the card issuer.
- Initiate a funds authorization request to the funds issuer for unlinked loads.
- Receive and process approvals and declines from both card issuers and funds issuers, when applicable.
- Handle exception processing.
- Identify suspect transactions appropriately and initiate notification to the card issuer.
- Log all transactions.

- Provide reporting to the load acquirer for reconciliation and auditing.

The load acquirer must participate in the following processing required for a load, unload, or currency exchange transaction:

- The authentication of a CEP card, including handling of responses.
- The authorization of funds, including handling of responses.
- The updating of CEP card value in the currency selected by the cardholder.
- The settlement process with funds issuers and card issuers for unlinked loads.
- Send reversal transactions when required.

Additionally the load acquirer must:

- Keep a log of all load transactions switched through their systems, regardless of completion status.
- Ensure that their system balances on a regular basis.
- Provide cardholders with the option of a receipt, as appropriate and subject to local regulations.

5.2.3 Funds Issuer

The funds issuer must:

- Be able to process funds requests for unlinked load transactions as uniquely identified electronic purse transactions.
- Participate in the settlement process for all load transactions that have been authorized by their network.
- Ensure that their system balances on a regular basis.
- Authorize or decline all funds requests assigned to them on their funds accounts.

5.2.4 Card Issuer

The card issuer must:

- Be able to process funds requests against cardholder accounts for linked load transactions.
- Support on-line authentication for linked and unlinked load transactions by checking the S_1 MAC in the request.
- Generate the second S_2 MAC and other cryptographic elements.

- Returning the S_2 MAC and other cryptographic elements to the load acquirer.
- Participate in the settlement process for unlinked load transactions.
- Be able to recognize and track suspect transactions, based on information received from the load acquirer.
- Update and reconcile all changes to card liability and funds pools as a result of load, unload, and currency exchange transactions.
- Optionally lock the card or application using either a script command or a proprietary method.
- Optionally deactivate the application by including a deactivation date in the authentication response.

5.2.5 Network Nodes/Processors

Transactions may flow directly from a load acquirer to a card issuer and a funds issuer. However, many times the transactions may be processed by additional nodes in the network connecting the load acquirer and the issuers. To ensure the integrity of the data content and the financial effects of transactions, these processing[§] nodes (or processors) must perform the following tasks:

- Share an encryption key with connecting processors. Encrypt the PIN block on all transactions sent to another processor using this encryption key. Decrypt and re-encrypt all PIN blocks that should be sent to other entities.
- 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.

Additionally, each processing node should generate and send a MAC on each message flowing between network nodes.

5.3 Overall Requirements

- Currency exchange rates for the currency exchange transaction must be established by the card issuer.
- Currency exchange rates for unload transactions must be established by the card issuer when the currency being unloaded and the destination cardholder account are in different currencies.

[§] The load acquirer, the funds issuer and the card issuer are considered processors as well.

- Currency exchange rates for an unlinked load transaction must be established according the rules of the network or networks processing the transaction. However, for linked load transactions, the currency exchange rates must be established by the card issuer.

- The card issuer must manage its currency liabilities.

- Load acquirers, card issuers, and funds issuers must log all transactions.

- Card issuers must inform their cardholders as to which currencies they support in electronic purses.

- Load acquirers must determine the currencies that they must support for load transaction.

- The following business rules must be used for suspect transactions when the final status of the transaction at the card is not definitively known:

  - **Load** - Assume the transaction completed successfully. Funds are debited from the cardholder account and credited to the funds pool. The card issuer liability is increased.
  - **Unload** - Assume the transaction did not complete successfully. Funds are not withdrawn from the funds pool and liabilities are not altered.
  - **Currency Exchange** - Assume the transaction completed successfully. The funds pool and liability positions are adjusted to reflect a decrease in the “from” currency and an increase in the “to” currency.

- The load acquirer must notify the card issuer of all suspect transactions.

- The CEP application must contain data that indicates the presence of a linked financial institution. If a linked financial institution is established for the CEP application, then linked loads must be allowed and data in the application must indicate whether linked loads are supported.

- Flexibility is required to accommodate the variety of environments where unlinked loads may be implemented. As a result, the design specification must not preclude dual-leg transactions[**] from taking place either sequentially or in parallel. The design of a given implementation will vary depending on the device, host, and network capabilities.

- Card issuers must support load transactions.

- Unload and currency exchange transactions are optional for CEP card issuers. The CEP card must indicate whether the card issuer supports these transactions. However, if a card issuer issues multi-currency capable cards, it must provide its cardholder with a facility to remove any remaining value. As a

[**] Dual leg transaction are transactions where participation is required by both a funds issuer and card issuer.

result, if a card issuer supports loading of multiple currencies onto a card, then it must support the unload or currency exchange transaction or both.

- For unload transactions, the load acquirer and card issuer must be the same financial institution. Load devices or load acquirers must be able to identify their own institution's CEP cards.
- The card issuer must establish its policies for assigning and adjusting slot maximum balances. These policies may require the card issuer to maintain a card database.
- Currency exchange rate fluctuations may increase the card issuers liability. The card issuer must be able to adjust maximum balances to bring them in line with their policies. The card issuer may update the maximum balances as part of a load, a partial unload, and a currency exchange transaction. On a currency exchange transaction, only the "to" currency maximum balance may be updated.
- The maximum balance for a currency must never be less than the existing balance for that currency plus the amount to be loaded, in case of a load transaction.
- A CEP card may contain currencies that the load acquirer does not support. As a result, load devices must use the alphabetic issuer-supplied currency code and currency exponent from the CEP slot(s) to display the source amounts for the currency conversion transaction.
- Card issuers must provide an alphabetic currency code in each message that establishes a new currency. This alphabetic currency code and the currency exponent will be used by the load device to display currency balances. This allows the cardholder to identify the currency being displayed.
- Script messages that conform to EMV specifications[††] may be included as part of load, unload and currency exchange messages from the card issuer to the CEP card. An update key must be used when card parameters are changed. Script messages may be sent to the CEP card either before or after the credit for load, debit of unload and currency exchange commands.
- All on-line messages must have the ability to include card issuer discretionary data from the CEP card.
- The card issuer must notify the cardholder if the assessment of service fees by the card issuer during the currency exchange transaction may result in a balance of zero after the transaction has completed.

[††] Script messaging is described in EMV '96 Integrated Circuit Card Application Specifications for Payment Systems, section 7.10.

- The card issuer must have the ability to deactivate a CEP application in the response to a load or currency exchange transaction.

5.4 Processing Flows

This section describes the transaction flows that take place at a load device. All of the flows in this section show processing between the load device, the load acquirer, the funds issuer, and the card issuer. However, in many cases, the actual flow will involve one or more networks acting as an agent for the load acquirer, the funds issuer, or the card issuer. Placement of functions and process flow for load acquiring will vary depending on the device, host, and network capabilities. The acquiring function includes the load device and the load host system. Steps for these two entities are grouped together in these flows.

The flows included in this section are:

- Unlinked Load Processing Flow.
- Linked Load Processing Flow.
- Unload Processing Flow.
- Currency Exchange Processing Flow.

5.4.1 Unlinked Load Processing Flow

Two types of load processing may be supported by CEP cards. Some card issuers will support linked loads, some will allow loading from other sources of funds. If the load is to be performed from another source of funds, the cardholder will have to indicate the source of those funds to the load device during the load process.

Figure 12 - Unlinked Load Processing Flow - Initiate

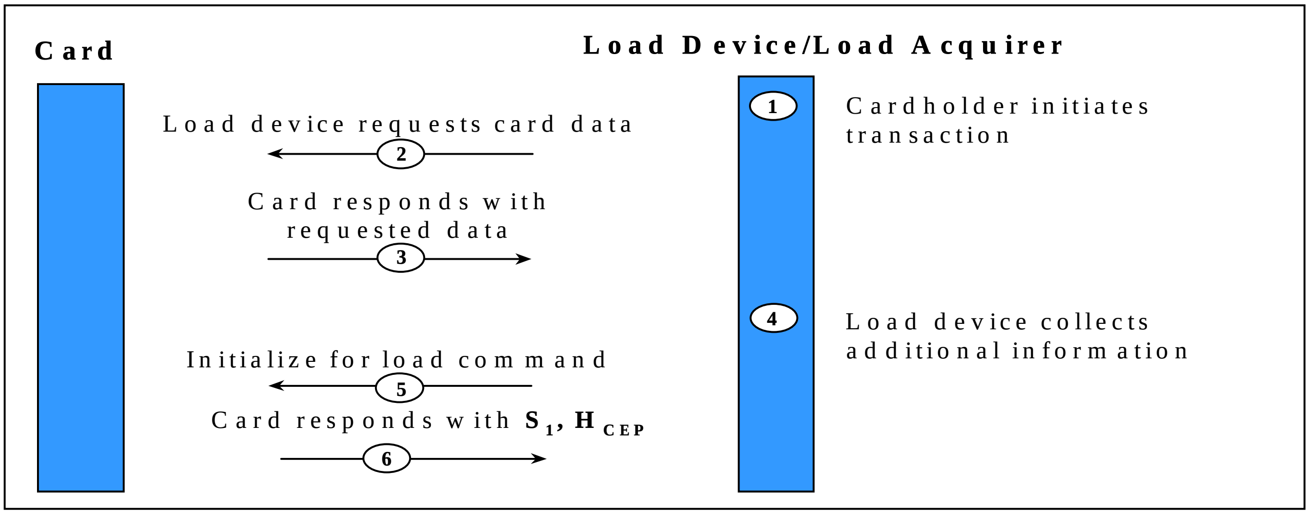

Card
Load Device/Load Acquirer
1
Cardholder initiates transaction
Load device requests card data
2
Card responds with requested data
3
4
Load device collects additional information
Initialize for load command
5
Card responds with **S**$_1$, **H** $_{CEP}$
6

Figure 13 - Unlinked Load Processing Flow - Prepare Messages

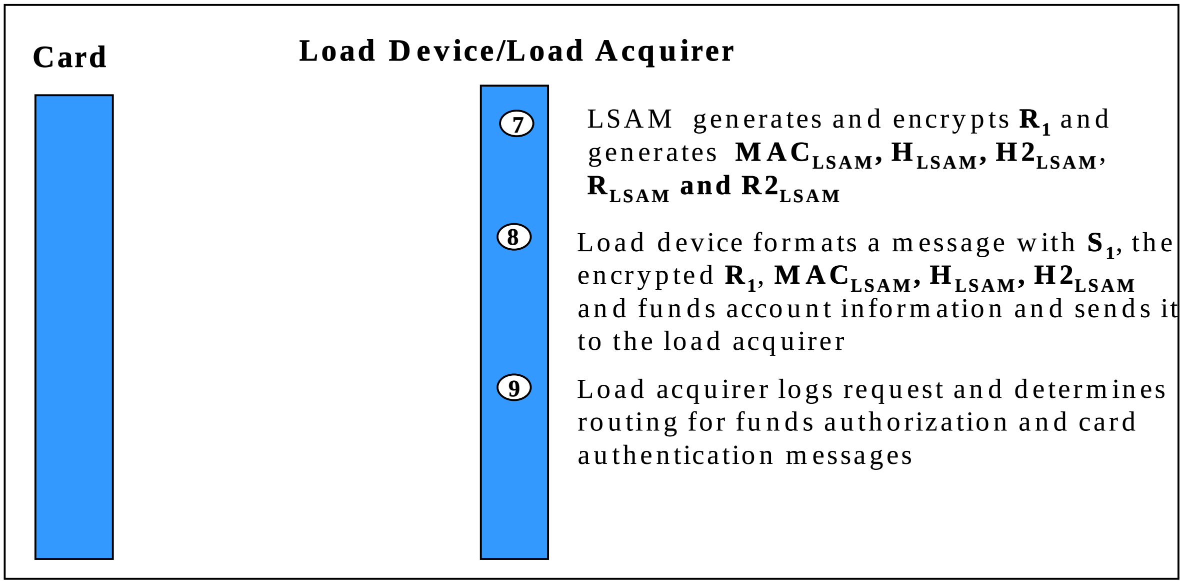

Card
Load Device/Load Acquirer
7
LSAM generates and encrypts **R**$_1$ and generates **MAC**$_{LSAM}$, **H**$_{LSAM}$, **H2**$_{LSAM}$, **R**$_{LSAM}$ **and R2**$_{LSAM}$
8
Load device formats a message with **S**$_1$, the encrypted **R**$_1$, **MAC**$_{LSAM}$, **H**$_{LSAM}$, **H2**$_{LSAM}$ and funds account information and sends it to the load acquirer
9
Load acquirer logs request and determines routing for funds authorization and card authentication messages

Figure 14 - Unlinked Load Processing Flow - Obtain Funds

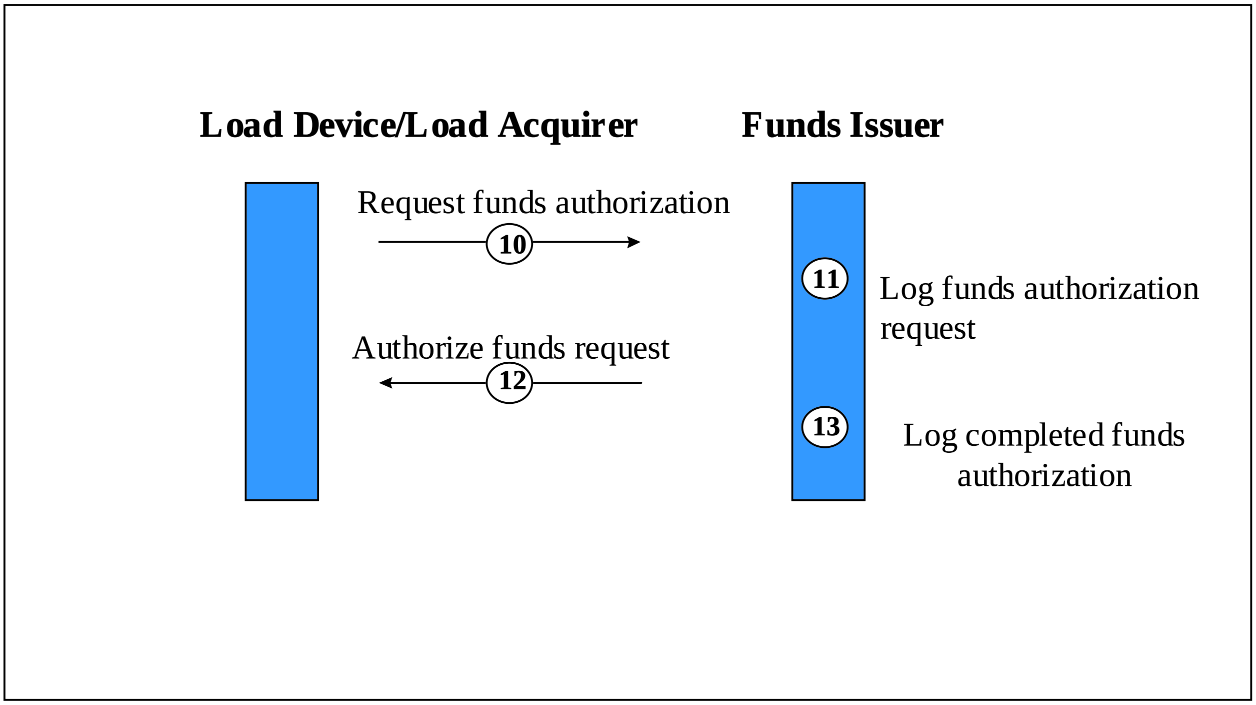

Load Device/Load Acquirer
Funds Issuer
Request funds authorization
10
11
Log funds authorization request
Authorize funds request
12
13
Log completed funds authorization

Figure 15 - Unlinked Load Processing Flow - Authenticate Card

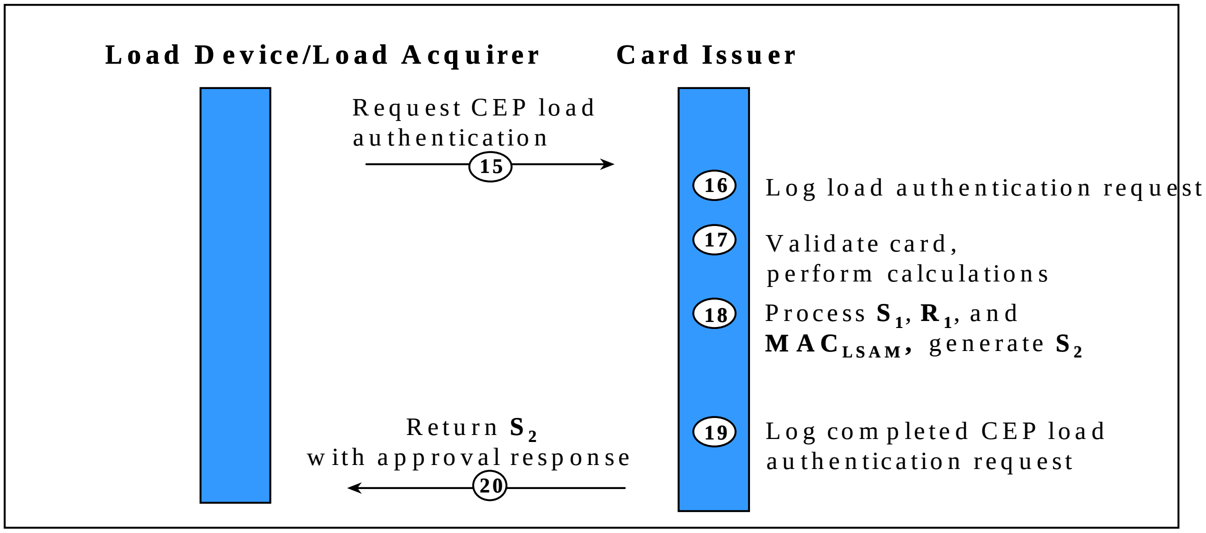

Load Device/Load Acquirer
Card Issuer
Request CEP load authentication
15
16
Log load authentication request
17
Validate card, perform calculations
18
Process S_1, R_1, and MAC_{LSAM}, generate S_2
Return S_2 with approval response
20
19
Log completed CEP load authentication request

Figure 16 - Unlinked Load Processing Flow - Add Value to Card

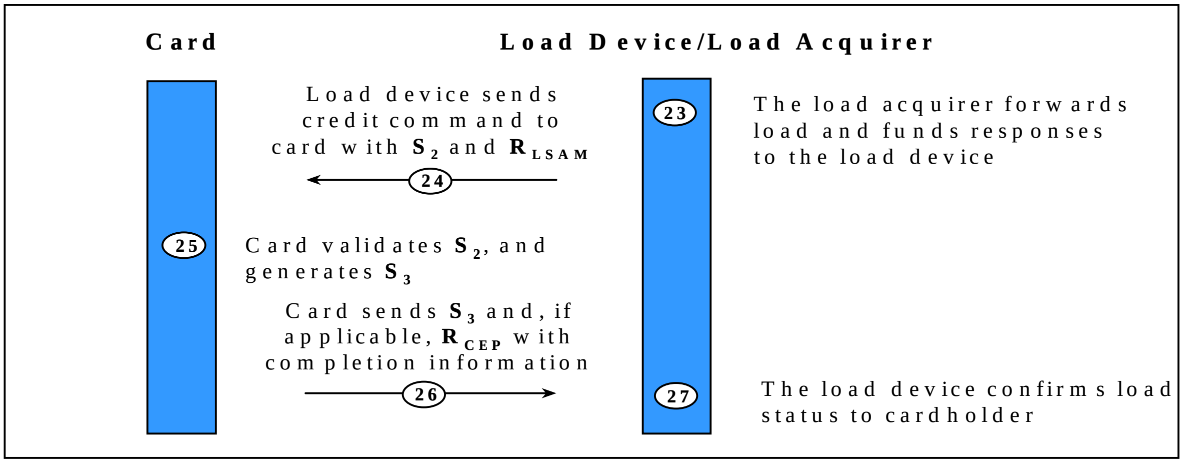

Card
Load Device/Load Acquirer
23
The load acquirer forwards load and funds responses to the load device
Load device sends credit command to card with $\mathbf{S_2}$ and $\mathbf{R_{LSAM}}$
24
25
Card validates $\mathbf{S_2}$, and generates $\mathbf{S_3}$
Card sends $\mathbf{S_3}$ and, if applicable, $\mathbf{R_{CEP}}$ with completion information
26
27
The load device confirms load status to cardholder

Figure 17 - Unlinked Load Processing Flow - Complete

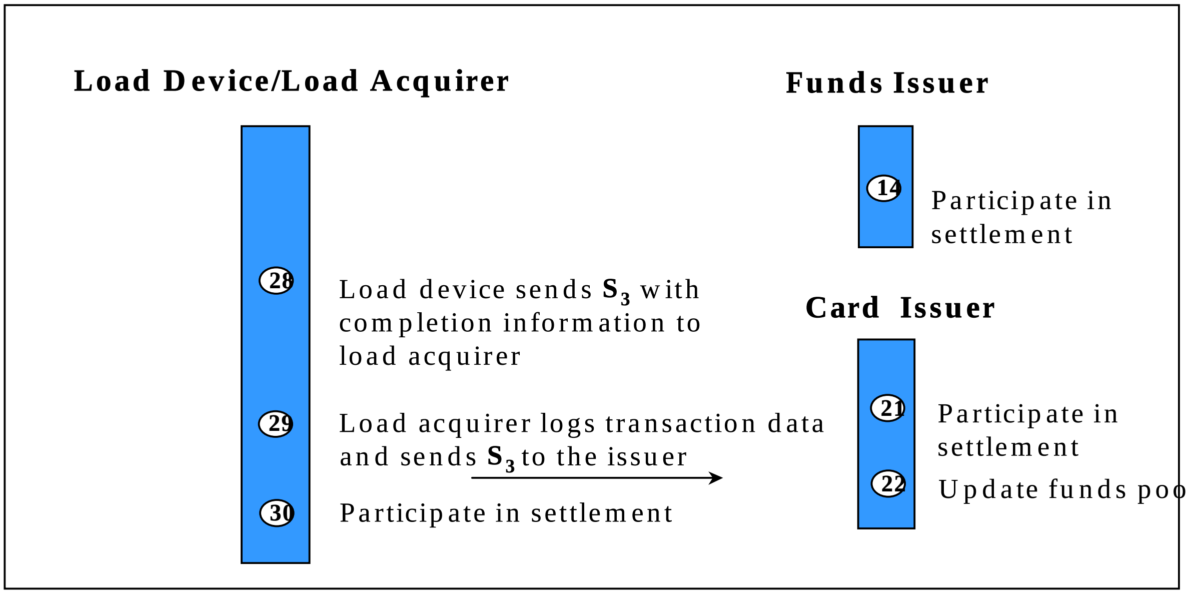

Load Device/Load Acquirer
Funds Issuer
14
Participate in settlement
28
Load device sends $\mathbf{S_3}$ with completion information to load acquirer
Card Issuer
29
Load acquirer logs transaction data and sends $\mathbf{S_3}$ to the issuer
21
Participate in settlement
22
Update funds pool
30
Participate in settlement

Figure 12, Figure 13, Figure 14, Figure 15, Figure 16 and Figure 17 show the basic processing flow for an unlinked load transaction. The steps in the flow are:

1. The cardholder initiates a load transaction. The cardholder interface will vary depending on the device, card, and scheme being used and is outside of the scope of this document.

2. The load device requests information from the CEP card.

3. The CEP card responds with slot information, whether there is a linked financial institution, and with card data that includes the expiration date. If the card has expired, the transaction is terminated. If the CEP card is locked, the transaction is terminated.

4. If there is no linked financial institution, the load device collects funding information and cardholder verification data (for example, PIN). Any funding information edits are carried out. The load device may optionally alert the cardholder when the CEP card is nearing its expiration date.

   The load device displays the currencies available to the cardholder for load and, if it is available, the maximum balance that may be loaded. An issuer-supplied maximum balance will be available for display if the currency already exists on the CEP card. If the currency does not already exist on the CEP card, the load acquirer may optionally access data on the CEP card which provides an approximate balance limit in a reference currency. The load acquirer may then convert the amount in the reference currency to local currency and display the converted amount as the maximum balance. The load device then prompts the cardholder for the amount to be loaded. The cardholder selects the currency, if appropriate, and enters the load amount. This data is sent to the load device.

   The load device performs validations. For currencies that have an existing balance, the amount is verified against the currency maximum balance. Maximum balances do not exist prior to a currency assignment to a given slot.

5. The initialize for load command is sent to the CEP card.

6. The CEP card generates S_1, a random number, R_{CEP}, and a SHA-1 hash value, H_{CEP}, which contains R_{CEP}. The card includes S_1 and H_{CEP} in its response to the load device.

7. If the LSAM is located at the load device, the LSAM generates a random number, R_1,and encrypts that random number under a secret key known by the next processing node. The LSAM then creates MAC_{LSAM} using R_1 as the encipherment key. The LSAM also creates two random numbers, R_{LSAM} and $R2_{LSAM}$, and two SHA-2 hash values, H_{LSAM} and $H2_{LSAM}$, containing R_{LSAM} and $R2_{LSAM}$ respectively.

8. The load request message to the load acquirer is then formatted to include the S_1, the data elements required to verify S_1, the funds account information, the enciphered R_1 , MAC_{LSAM}, H_{LSAM} and $H2_{LSAM}$. If appropriate, the transaction is logged. The load request is sent to the load acquirer. If the LSAM is at the load acquirer, the enciphered R_1 and the other cryptograms do not yet exist.

9. The load acquirer receives and logs the request from the load device, designates a unique identifier for this CEP load transaction, and determines the routing for the funds issuer and the card issuer. The load acquirer formats two messages: one to the funds issuer for authorization and one to the card issuer for authentication This processing may be done either sequentially or in parallel. If the LSAM is located at the load acquirer, the processing described in step 7 above is also accomplished. The unique transaction identifier is used by the load acquirer to manage the process for the duration of the transaction. The load acquirer must keep records, by CEP card number, of all loads that take place at its load devices.

10. The load acquirer sends a message to the funds issuer to secure funds and validate the cardholder.

11. The funds issuer logs the funds authorization request.

12. The funds issuer authorizes the funds request and returns the funds authorization to the load acquirer.

13. The funds issuer logs the completed funds authorization.

14. The funds issuer participates in the settlement process.

15. The load acquirer sends a message to the card issuer to authenticate the CEP card and authorize the loading of value onto the CEP card.

16. The card issuer logs the card authentication request.

17. The card issuer validates the CEP card, checks for expiration, checks it against a revocation list, and validates that the card issuer supports the currency requested. The card issuer determines if there is a need to calculate the maximum slot balance. The maximum balance is included in the message from the load acquirer. A maximum balance of zero indicates that the currency does not exist on the CEP card. For a new currency, a maximum balance must be calculated.

    If the requested amount exceeds a maximum balance the card issuer will support, the card issuer declines the transaction, and sends the supported maximum balance field in the decline.

1. The card issuer validates the S_1, recovers the encrypted random number R_1, and validates the MAC_{LSAM}. If either the S_1 or the MAC_{LSAM} does not pass the validation, the transaction is declined. If both the S_1 and the MAC_{LSAM} are valid, the card issuer generates an S_2, containing H_{LSAM}. If the card issuer

declines the transaction, an S_2 is optional, but if generated must not contain H_{LSAM}. The resulting cryptogram is placed in the message to be sent to the load acquirer in an authentication response message.

2. The card issuer logs the completed card authentication request.
3. The card issuer sends a response to the load acquirer. Any script messages to be sent to the CEP card are included with this response.
4. The card issuer participates in the settlement process.
5. For successful transactions, the card issuer updates its funds pool and card database and adjusts liability accordingly.
6. The load acquirer receives the funds authorization response and the card authentication response. If these are both approved, the load acquirer forwards the approval response to the load device. Any script messages from the card issuer are included in the message to the load device.
7. If the message from the load acquirer contains a script message that is to be sent to the card before the credit command, the load device sends the script message to the CEP card.

   If the message from the load acquirer contains a script message that is to be sent to the card after the credit command, the load device sends the script message to the CEP card.

   The load device sends a credit command with the S_2 to the CEP card. R_{LSAM} is released by the LSAM and sent with the S_2 for an approved load.
8. The CEP card validates the S_2 and generates an S_3. The CEP card updates the slot with the load amount and updates the maximum balance, as appropriate, along with creating a record in its internal transaction log.
9. The card sends the S_3 to the load device along with the completion information. If the CEP card rejects the credit command, it must also send R_{CEP} in the response message.
10. Based on the response received, the load device confirms the CEP card status to the cardholder. If possible, the load device provides a receipt.
11. The load device sends the transaction completion message details along with S_3 to the load acquirer. For successful transactions, the timing of this completion message is at the discretion of the load acquirer. For unsuccessful transactions, the completion message, with its error notification, must be sent immediately to the load acquirer who notifies the card issuer.
12. The load acquirer logs S_3, which is saved for the period of time required by the scheme provider’s operating regulations.

13. The load acquirer participates in the settlement process. The load acquirer is due money from the funds issuer and owes money to the card issuer.

5.4.2 Linked Load Processing Flow

Two types of load processing may be supported by CEP cards. Some card issuers may require a linked financial institution, others may allow loading from other sources of funds. If a linked load is to be performed, the presence of the linked financial institution is indicated by data in the CEP card. In a linked load, the funding source may be any account that the cardholder maintains at the financial institution that issued the CEP card. Some load acquirers may allow the cardholder to select which account is to be used as the funding source. The final selection of the funding account may be performed by the issuer.

Figure 18 - Linked Load Processing Flow - Initiate

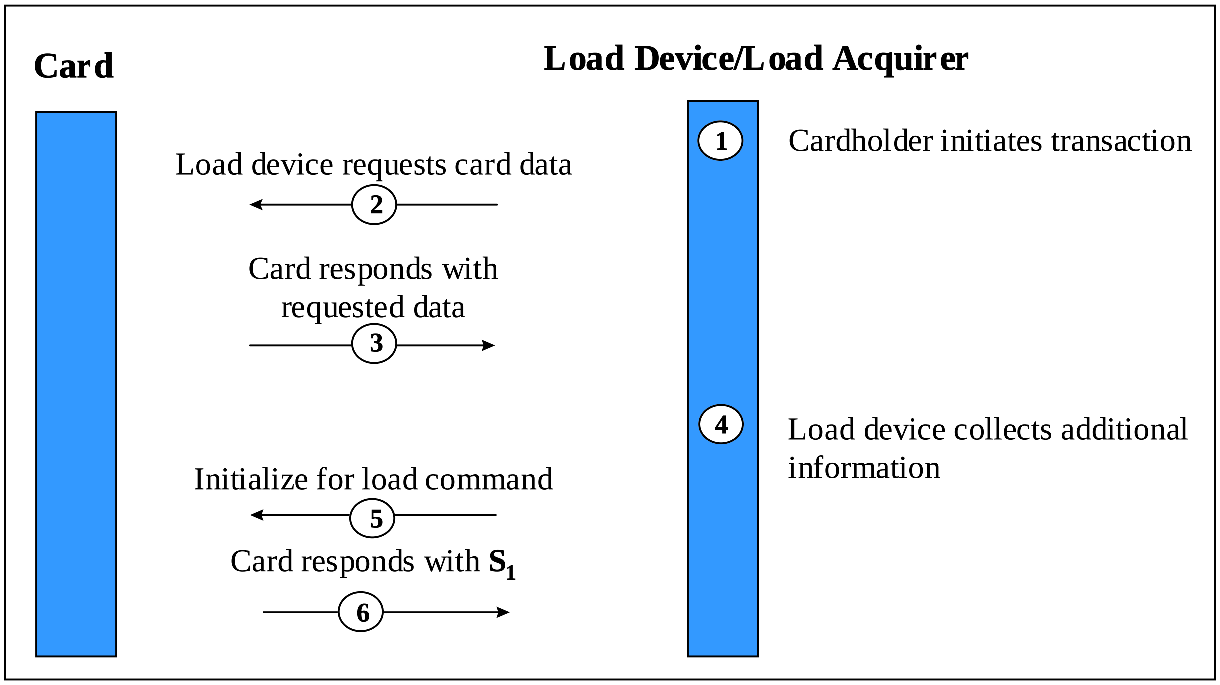

Card
Load Device/Load Acquirer
1
Cardholder initiates transaction
Load device requests card data
2
Card responds with requested data
3
4
Load device collects additional information
Initialize for load command
5
Card responds with S_1
6

Figure 19 - Linked Load Processing Flow - Prepare Message

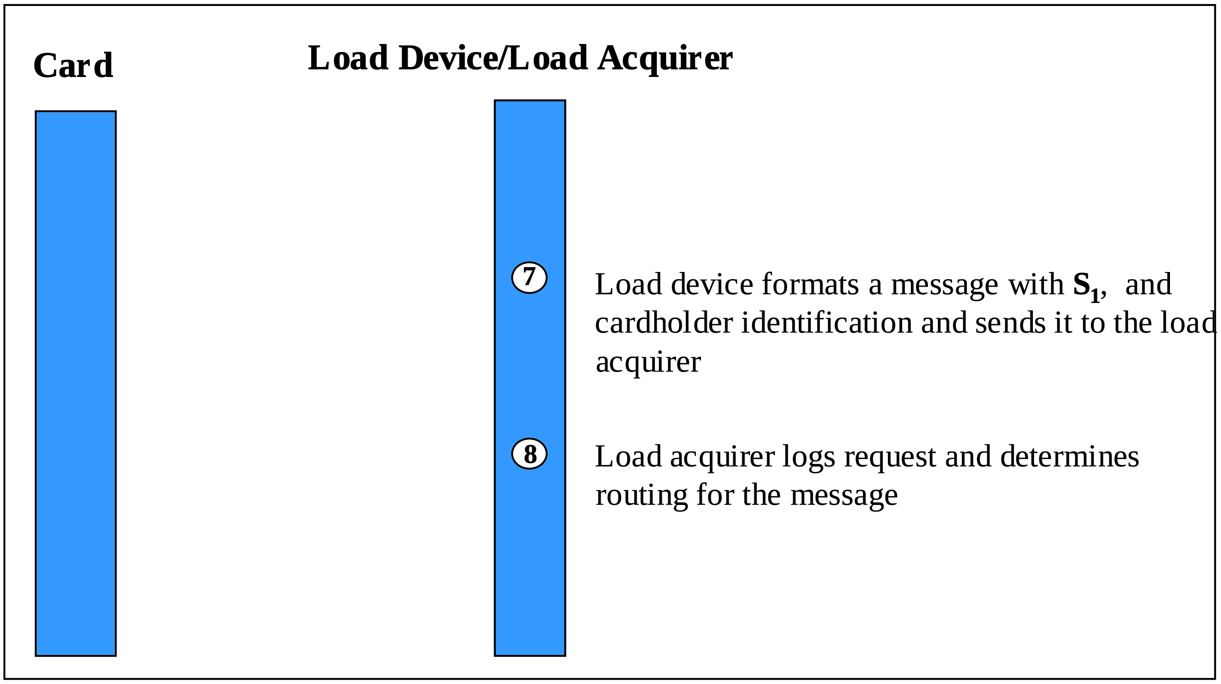

Card
Load Device/Load Acquirer
7
Load device formats a message with $\mathbf{S_1}$, and cardholder identification and sends it to the load acquirer
8
Load acquirer logs request and determines routing for the message

Figure 20 - Linked Load Processing Flow - Obtain Funds and Authenticate Card

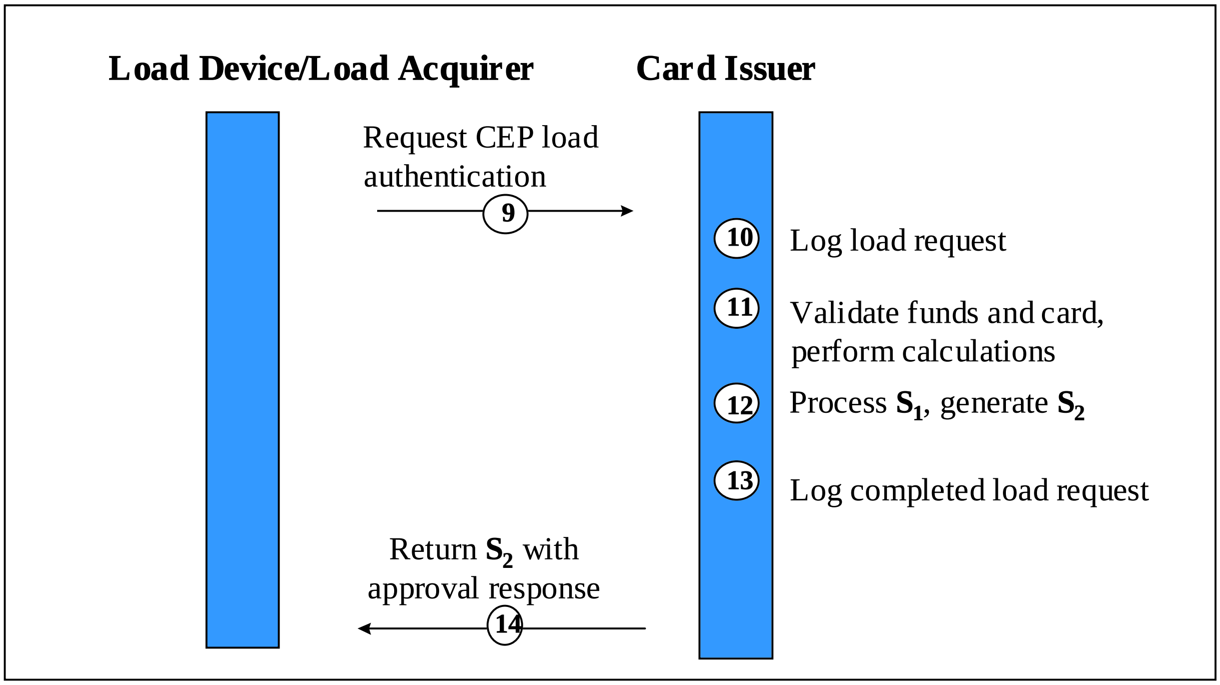

Load Device/Load Acquirer
Card Issuer
Request CEP load authentication
9
10
Log load request
11
Validate funds and card, perform calculations
12
Process $\mathbf{S_1}$, generate $\mathbf{S_2}$
13
Log completed load request
Return $\mathbf{S_2}$ with approval response
14

Figure 21 - Linked Load Processing Flow - Add Value

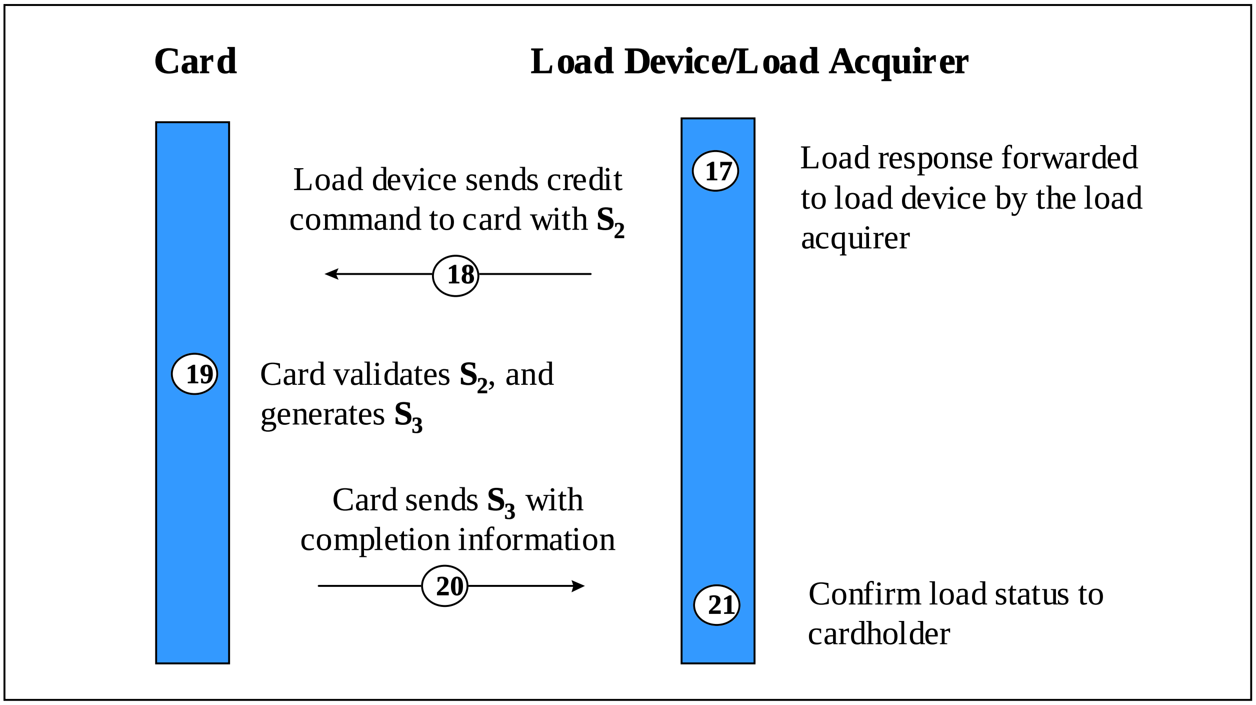

Card
Load Device/Load Acquirer
17
Load response forwarded to load device by the load acquirer
Load device sends credit command to card with S2
18
19
Card validates S2, and generates S3
Card sends S3 with completion information
20
21
Confirm load status to cardholder

Figure 22 - Linked Load Processing Flow - Complete

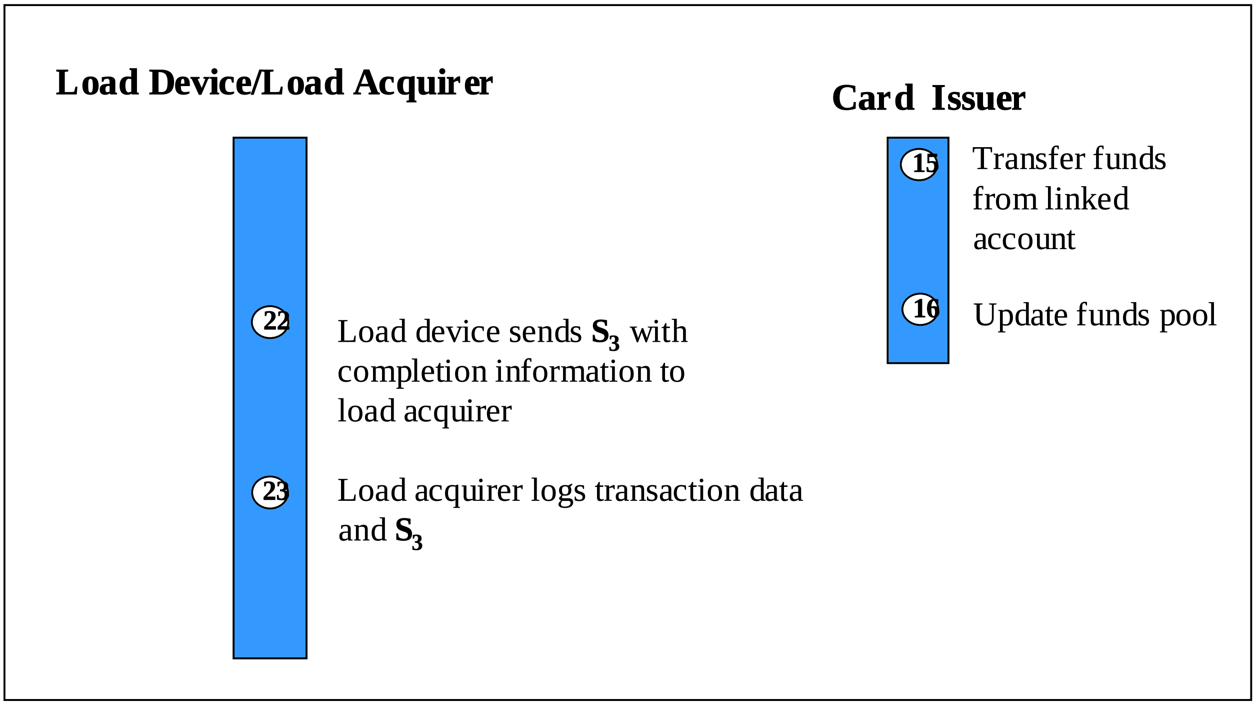

Load Device/Load Acquirer
Card Issuer
15
Transfer funds from linked account
16
Update funds pool
22
Load device sends S3 with completion information to load acquirer
23
Load acquirer logs transaction data and S3

Figure 18, Figure 19, Figure 20, Figure 21 and Figure 22 show the basic flow for a linked load transaction. The steps in the flow are:

1. The cardholder initiates the load transaction. The cardholder interface will vary depending on the device, card, and scheme being used and is outside of the scope of this document.

2. The load device requests information from the CEP card.

3. The CEP card responds with slot information, a field indicating whether there is a linked financial institution, and with card data that includes the expiration date. If the CEP card has expired, the transaction is terminated. If the CEP card is locked, the transaction is terminated.

4. The load device collects cardholder verification data. The CVMI of the CEP card will specify the methods of verification and their priority of use. The CEP card must indicate support for on-line PIN processing and at least one method of off-line PIN verification (encrypted or unencrypted). The method used will be determined by the load device and the CVMI of the CEP card. The load device may alert the cardholder when the CEP card is nearing its expiration date. The load device displays the currencies available to the cardholder for load and if it is available, the maximum balance that may be loaded. An issuer-supplied maximum balance will be available for display if the currency already exists on the CEP card. If the currency does not already exist on the CEP card, the load acquirer may optionally access data on the CEP card, which provides a maximum balance in a reference currency. The load acquirer may then convert the amount in the reference currency to local currency and display the converted amount as the maximum balance. The load device prompts the cardholder for the amount to be loaded.

   The cardholder selects the currency, if appropriate, and enters the load amount. This data is sent to the load device. If the load device supports account selection, the cardholder may select the account to be used for the load.

   The load device performs validations. For currencies that have an existing balance, the amount is verified against the currency maximum balance. Maximum balances do not exist prior to a currency assignment to a given slot.

5. The initialize for load command is sent to the CEP card.

6. The CEP card generates an S_1 MAC, which it includes in its response to the load device.

7. If appropriate, the load device logs the transaction. The load device sends the load request to the load acquirer.

8. The load acquirer receives and logs the request from the load device, designates a unique identifier to identify the CEP load transaction, and determines the routing for the card issuer. The load acquirer formats an authentication message to the card issuer. The load acquirer uses the unique

transaction identifier to manage the processing for the duration of the transaction. The load acquirer must keep records, by CEP card number, of all loads that take place at its load devices.

9. The load acquirer sends the message to the card issuer to authenticate the CEP card and authorize the loading of value onto the CEP card.

10. The card issuer logs the load request.

11. The card issuer accesses the funding account and validates that funds are available to perform the load. The card issuer also validates the CEP card, checks for expiration, checks it against a revocation list and validates that the card issuer supports the currency requested. The card issuer determines if there is a need to calculate the maximum slot balance. The maximum balance is included in the message from the load acquirer. A maximum balance of zero indicates that the currency does not exist on the CEP card. For a new currency, a maximum balance must be calculated.

    If the requested amount exceeds a maximum balance the card issuer will support, the card issuer declines the transaction, and sends the supported maximum balance field in the decline.

1. The card issuer validates the S_1. If the S_1 is valid, the card issuer generates an S_2 MAC. If S_1 is not valid, the transaction is declined.

2. The card issuer logs the completed load request.

3. The card issuer sends a response to the load acquirer. If the load is approved, the response must include the S_2 and, optionally, the new maximum balance. Any script messages to be sent to the CEP card are included with this response.

4. The card issuer transfers funds from the cardholder account to the appropriate funds pool.

5. The card issuer updates the card database and adjusts its liability accordingly.

6. The load acquirer receives the response. If this is an approval, the approval response is forwarded to the load device. Any script messages from the card issuer are included with this response.

7. If the message from the load acquirer contains a script message that is to be sent to the card before the credit command, the load device sends the script message to the CEP card.

    The load device sends a credit command to the CEP card.

    If the message from the load acquirer contains a script message that is to be sent to the card after the credit command, the load device sends the script message to the CEP card.

8. The CEP card validates the S_2 and then generates an S_3 MAC. The CEP card updates the slot with the load amount and updates the maximum balance, as appropriate, along with creating a record in its internal transaction log.
9. The CEP card sends the S_3 to the load device along with the completion information.
10. Based on the response received, the load device confirms the CEP card status back to the cardholder. If possible, the load device provides a receipt.
11. The load device sends the transaction completion message details along with S_3 to the load acquirer. For successful transactions, the timing of this completion message is at the discretion of the load acquirer. For unsuccessful transaction, the completion message, with its error notification, must be sent immediately to the load acquirer for notification to the card issuer.
12. The load acquirer logs S_3, which is saved for the period of time defined in the scheme provider's operating regulations.

5.4.3 Unload Processing Flow

The unload transaction may only be performed when the load acquirer and the card issuer are the same financial institution. Additionally, the unload must be to an account within that same financial institution.

Figure 23 - Unload Processing Flow - Initiate

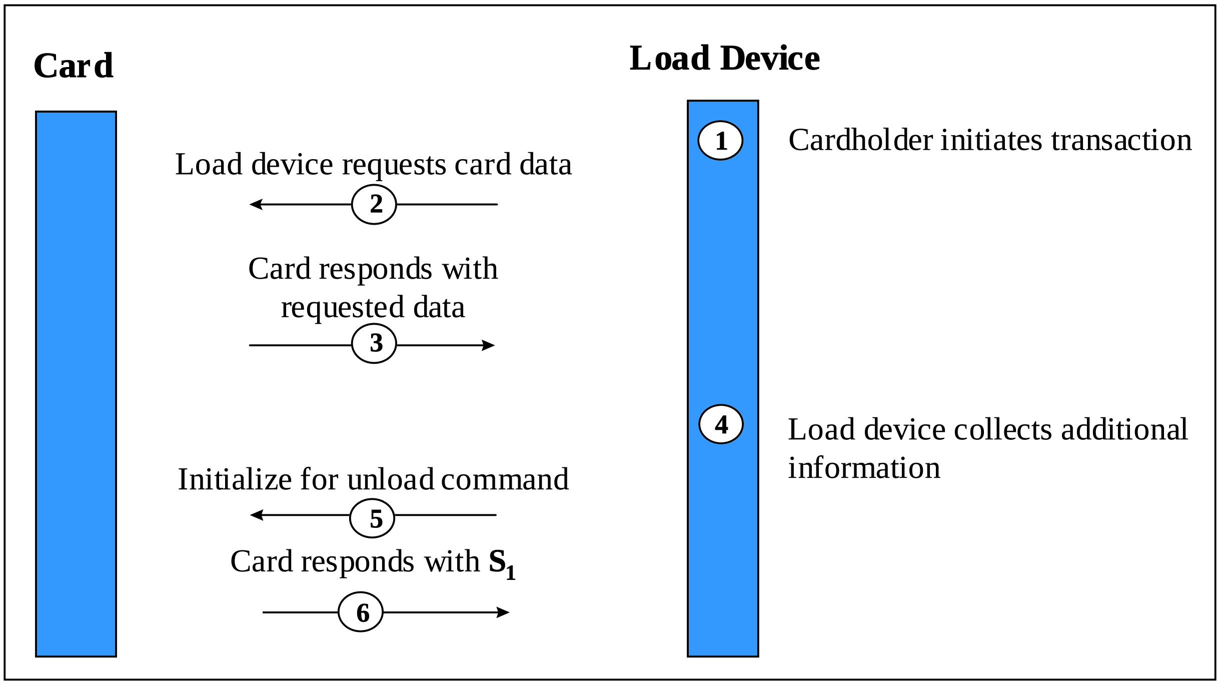

Card
Load Device
1
Cardholder initiates transaction
Load device requests card data
2
Card responds with requested data
3
4
Load device collects additional information
Initialize for unload command
5
Card responds with S_1
6

Figure 24 - Unload Processing Flow - Validate Card

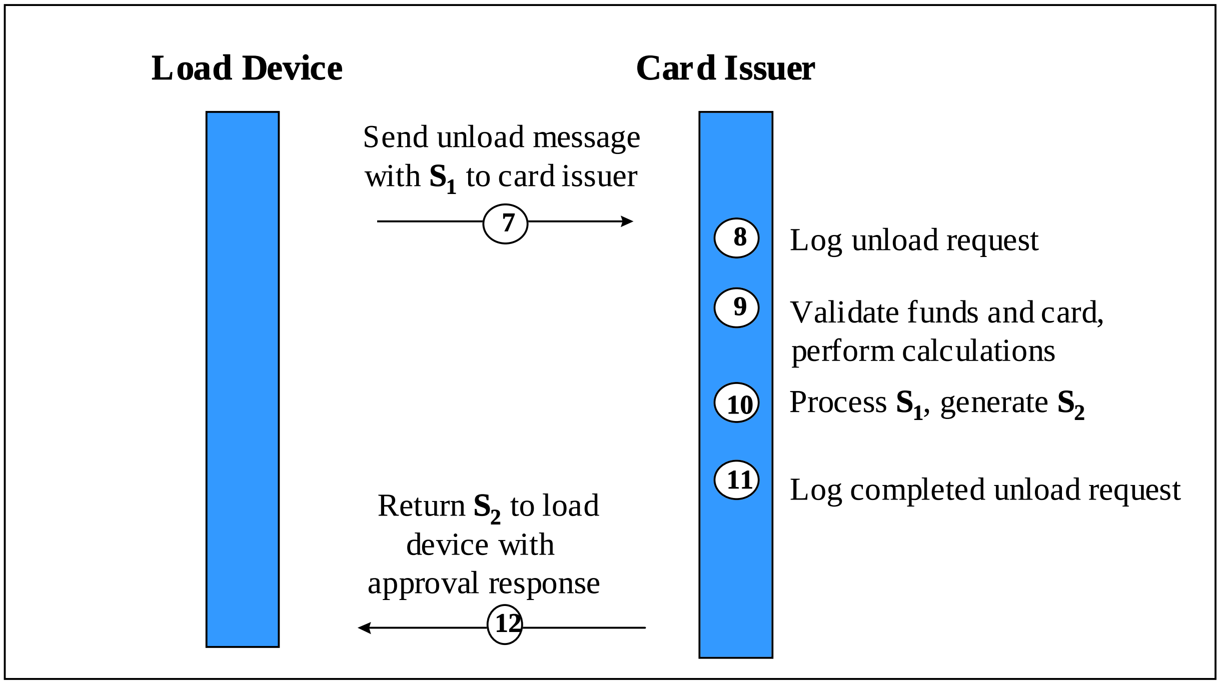

Load Device
Card Issuer
Send unload message with S_1 to card issuer
7
8 Log unload request
9 Validate funds and card, perform calculations
10 Process S_1, generate S_2
11 Log completed unload request
Return S_2 to load device with approval response
12

Figure 25 - Unload Processing Flow - Remove Value

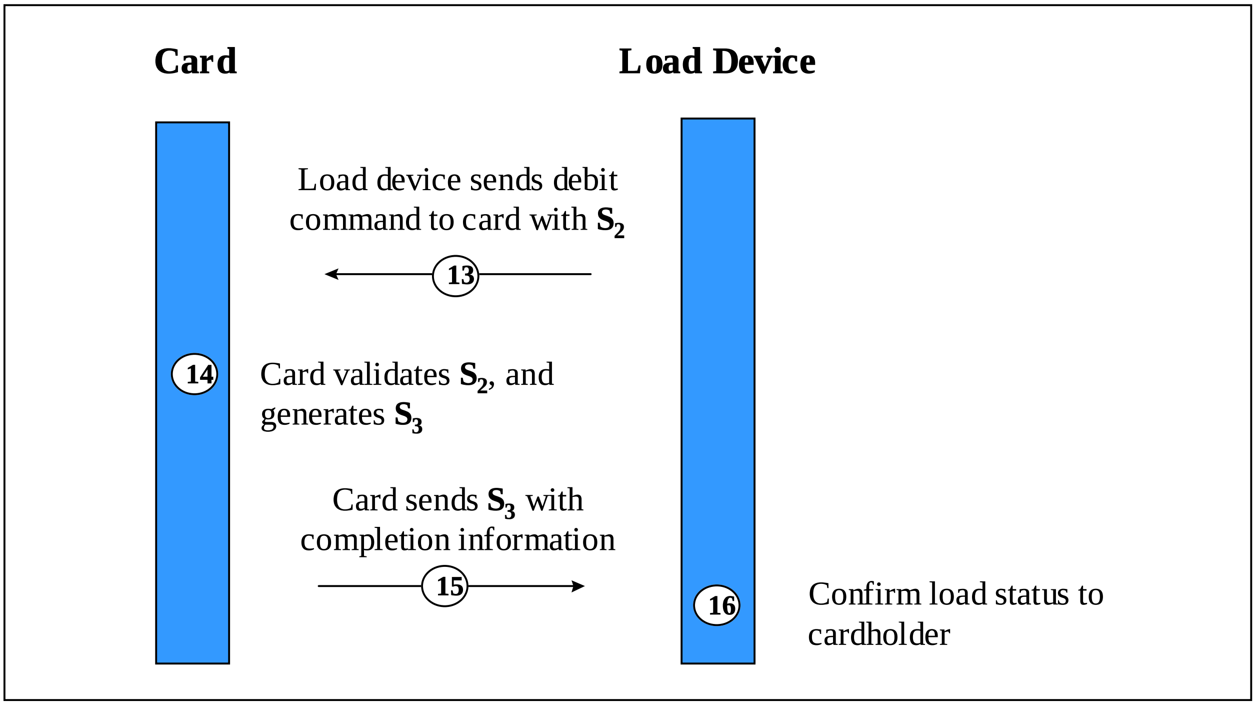

Card
Load Device
Load device sends debit command to card with S_2
13
14 Card validates S_2, and generates S_3
Card sends S_3 with completion information
15
16 Confirm load status to cardholder

Figure 26 - Unload Processing Flow - Complete

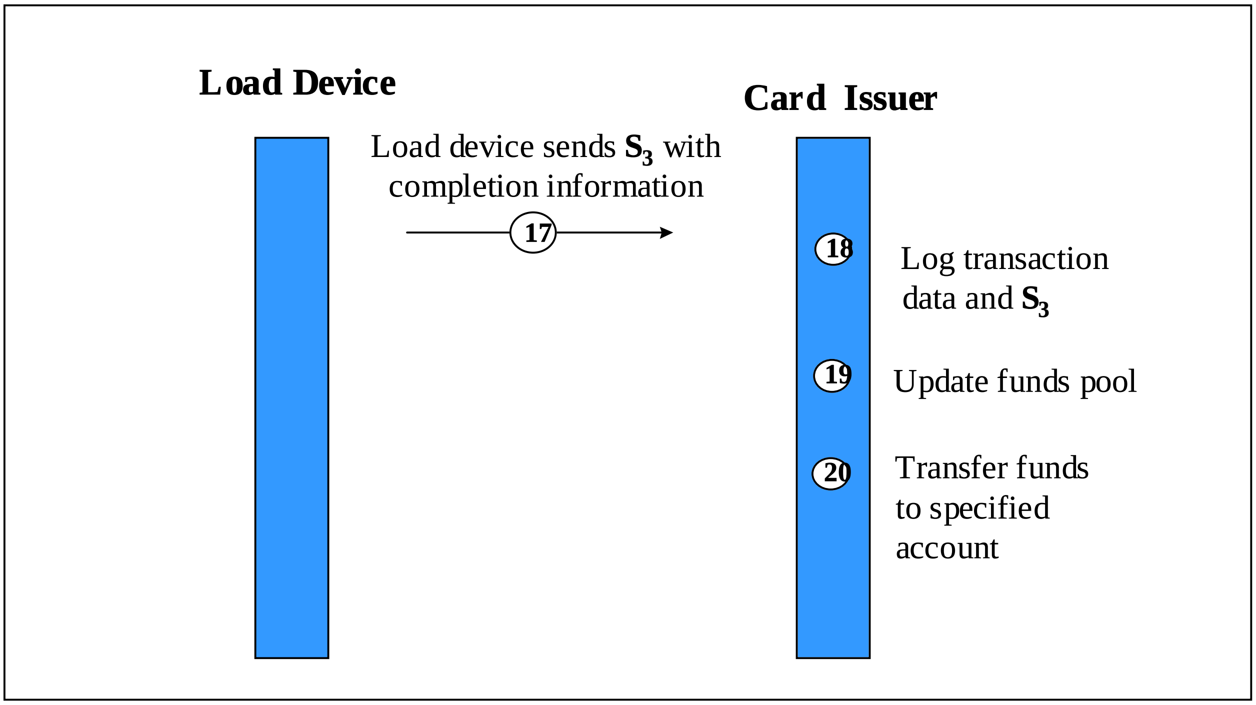

Load Device
Card Issuer
Load device sends $\mathbf{S_3}$ with completion information
17
18
Log transaction data and $\mathbf{S_3}$
19
Update funds pool
20
Transfer funds to specified account

Figure 23, Figure 24, Figure 25, and Figure 26 show the basic processing flow for an unload transaction. The steps in the flow are:

1. Figure 24Figure 26The cardholder initiates the unload transaction.
2. The load device requests information from the CEP card.
3. The CEP card responds with the expiration date, whether the unload transaction is supported, the issuer of the CEP card, and the currency and current balance of all slots with a balance.
4. If the card issuer is not the same financial institution as the load acquirer, or if the CEP card does not support the unload transaction, the transaction is terminated. The load device determines the currencies on the CEP card that may be unloaded. The currencies and the related balances that may be unloaded are displayed to the cardholder. The cardholder enters the currency and amount to be unloaded. The unload account must be an account at the same financial institution as the load acquirer.

   The load device performs validations and verifies the amount against the balance provided by the CEP card.
5. The load device then sends the initialize for unload command to the CEP card.

6. The CEP card responds to the initialize for unload command from the load device by generating an S_1 MAC. The CEP card then sends the S_1 to the load device.

7. If appropriate, the load device logs the transaction. The load device sends the S_1, the data elements required to resolve the S_1 and the unload account information to the card issuer.

8. The card issuer logs the unload transaction.

9. The card issuer validates the CEP card and the unload account.

10. The card issuer processes the S_1. If the S_1 is valid, the card issuer generates an S_2 MAC. If a partial unload is requested, the card issuer determines if a change to the maximum balance for the currency being unloaded is required. If a maximum balance change is needed, the card issuer calculates the new currency maximum balance. If the S_1 is not valid, the transaction is declined.

11. The card issuer logs the completed unload request

12. The card issuer sends a response to the load device which includes the S_2 and any script messages to be sent to the CEP card.

13. If the message from the card issuer contains a script message that is to be sent to the card before the debit command, the load device sends the script message to the CEP card.

    The load device sends a debit command with the S_2 to the CEP card.

    If the message from the card issuer contains a script message that is to be sent to the card after the debit command, the load device sends the script message to the CEP card.

14. The CEP card validates the S_2 and generates an S_3 MAC. The CEP card logs the unload transaction in its internal transaction log.

15. The CEP card sends the S_3 to the load device along with the completion information.

16. The load device confirms the CEP card status back to the cardholder. If the load device is equipped with a printer, it provides a printed receipt.

17. The load device sends the transaction completion message details along with S_3 to the card issuer.

18. The card issuer validates and logs the S_3 MAC, which is saved for the period of time defined in the scheme provider’s operating regulations.

19. The card issuer updates its funds pool, if S_3 is successfully validated.

20. The unloaded funds are credited to the specified account.

5.4.4 Currency Exchange Processing Flow

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

Figure 27 - Currency Exchange Processing Flow - Initiate

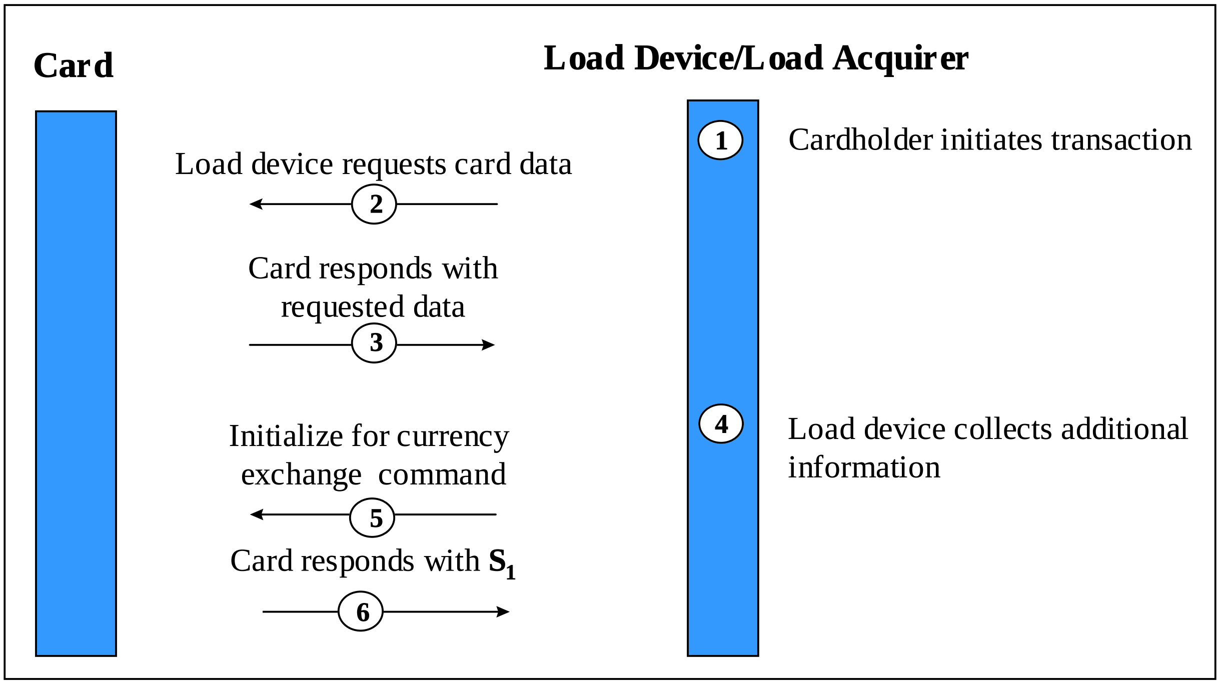

Card
Load Device/Load Acquirer
1 Cardholder initiates transaction
Load device requests card data
2
Card responds with requested data
3
4 Load device collects additional information
Initialize for currency exchange command
5
Card responds with S_1
6

Figure 28 - Currency Exchange Processing Flow - Prepare Message

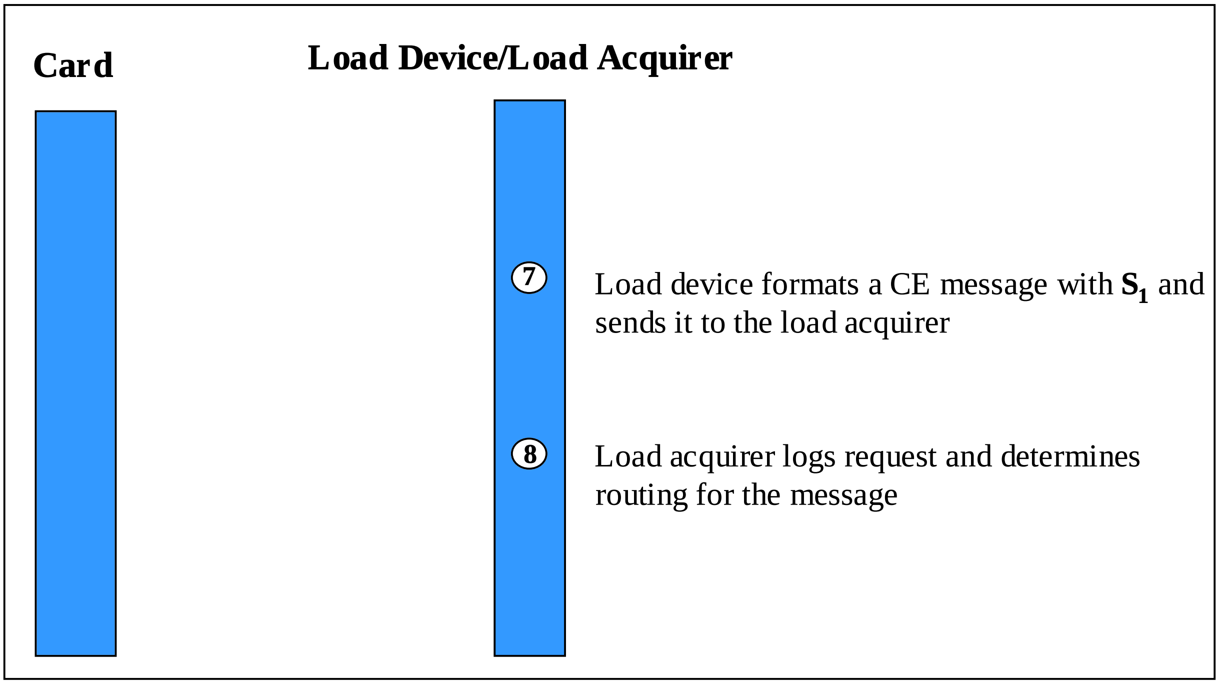

Card
Load Device/Load Acquirer
7
Load device formats a CE message with **S_1** and sends it to the load acquirer
8
Load acquirer logs request and determines routing for the message

Figure 29 - Currency Exchange Processing Flow - Validate Card

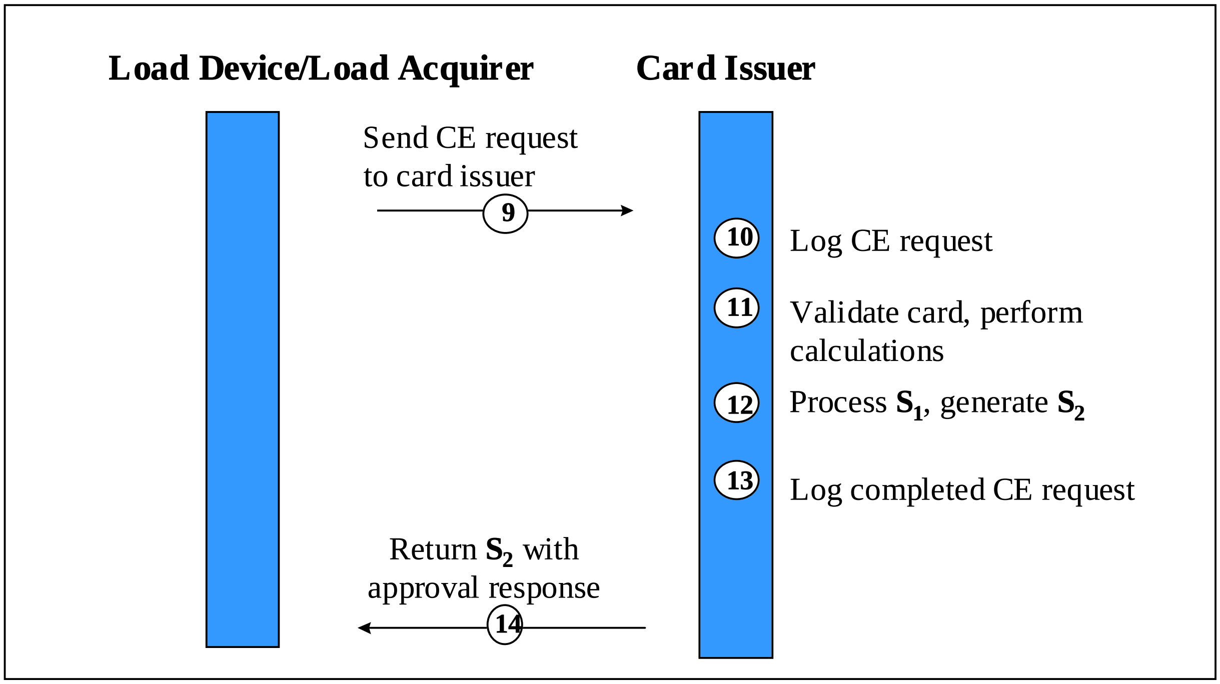

Load Device/Load Acquirer
Card Issuer
Send CE request to card issuer
9
10
Log CE request
11
Validate card, perform calculations
12
Process **S_1**, generate **S_2**
13
Log completed CE request
Return **S_2** with approval response
14

Figure 30 - Currency Exchange Processing Flow - Exchange Currencies

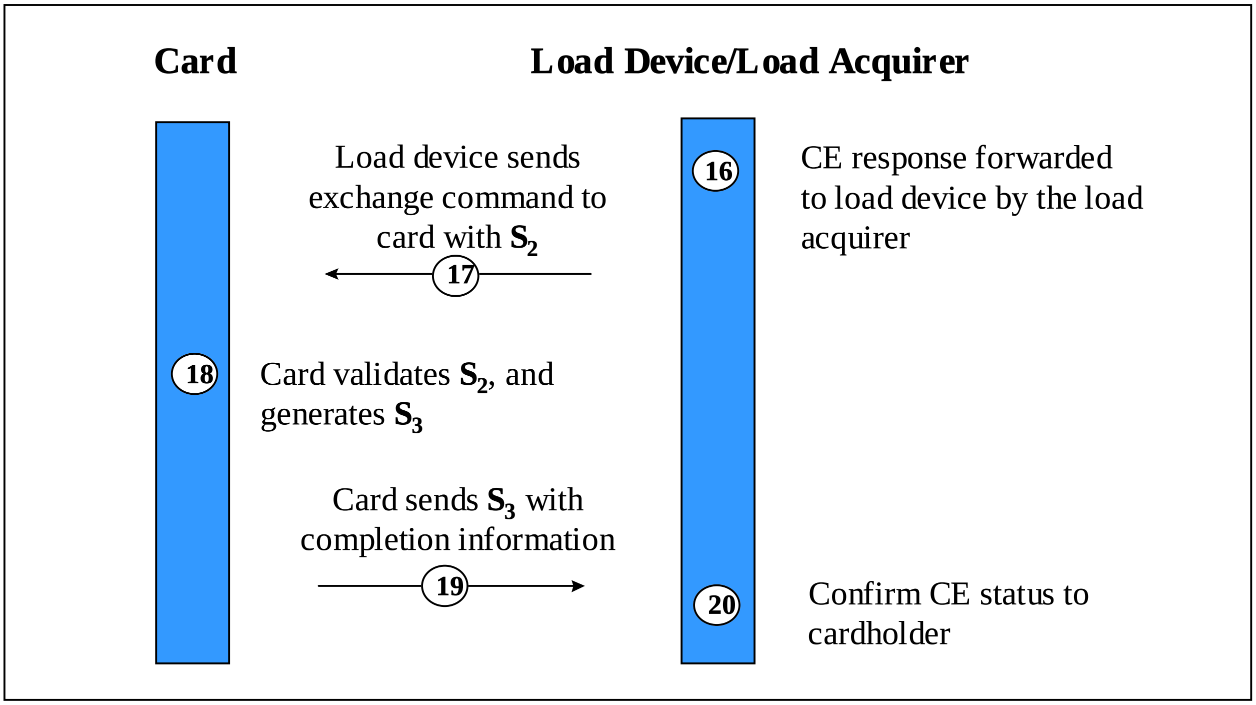

Card
Load Device/Load Acquirer
16
CE response forwarded to load device by the load acquirer
Load device sends exchange command to card with $\mathbf{S_2}$
17
18
Card validates $\mathbf{S_2}$, and generates $\mathbf{S_3}$
Card sends $\mathbf{S_3}$ with completion information
19
20
Confirm CE status to cardholder

Figure 31 - Currency Exchange Processing Flow - Complete

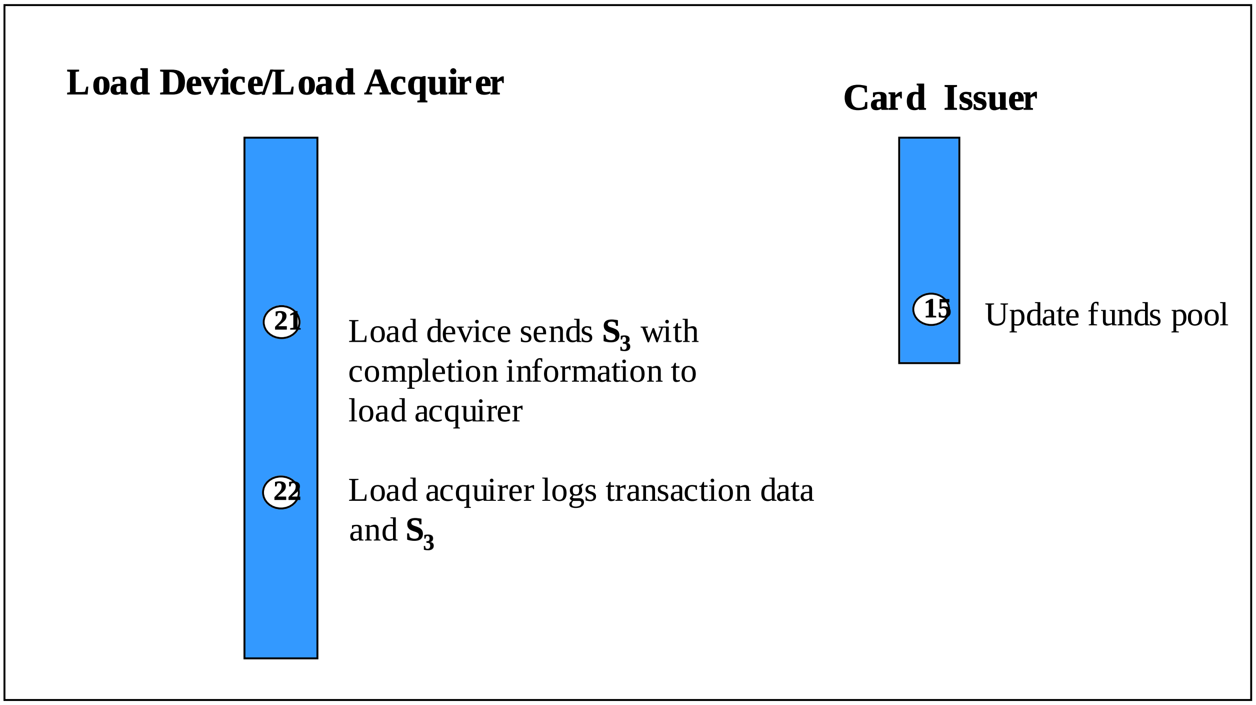

Load Device/Load Acquirer
Card Issuer
21
Load device sends $\mathbf{S_3}$ with completion information to load acquirer
22
Load acquirer logs transaction data and $\mathbf{S_3}$
15
Update funds pool

Figure 27, Figure 28, Figure 29, Figure 30, and Figure 31 show the basic processing flow for a currency exchange transaction. The steps in the flow are:

1. The cardholder initiates the currency exchange transaction. The cardholder interface will vary depending on the device, card, and scheme being used and is outside of the scope of this document. Cardholder verification is not required for a currency exchange transaction.
2. The load device requests card data (the balance of each slot containing currency, current balance, maximum balance, currency code, currency exponent, and the alpha currency code). The assumption is that the cardholder does not know the currencies and balances loaded on the CEP card.
3. The CEP card responds with the data requested and whether it supports the currency exchange transaction, the CEP card expiration date, and the number of available slots.
4. If the CEP card has expired, the transaction is terminated. If a CEP card is locked, the transaction is terminated.

   The load device displays to the cardholder the currency, current balance, and maximum balance for each slot on the CEP card. The load device may optionally provide a warning to the cardholder if the expiration date is approaching

   The cardholder selects the currency to convert from, the “from” currency, enters the amount to convert, and designates the currency to convert to, the “to” currency.

   The load device determines if the “to” currency is already present or if there is an unused slot. If a partial currency conversion is to be performed, either the “to” currency must be present, or there must be an unused slot. If neither of these conditions exist, the transaction is declined.
5. The load device sends an initialize for exchange command to the CEP card.
6. The CEP card generates the S_1 MAC and sends it in a response to the load device. If appropriate, the load device logs the transaction information.
7. The load device sends CEP card information to the load acquirer. Included in the information is the S_1 and the data elements required to verify the S_1.
8. The load acquirer receives and logs the request from the load device.

   The load acquirer designates a unique identifier for the currency exchange transaction and determines the routing for the card issuer. The load acquirer formats a message to the card issuer for authentication, using the unique transaction identifier to manage the load processing for the duration of the transaction. The load acquirer must keep records, by CEP card number, of all currency exchanges that take place at its load devices.

9. The load acquirer sends a message to the card issuer for authentication and authorization to perform a currency exchange transaction.

10. The card issuer logs the request from the load acquirer.

11. The card issuer validates the CEP card as being issued by the card issuer and if the “to” currency is supported. It then obtains the exchange rate for the from/to currencies and calculates the amount in the “to” currency. The card issuer determines if the “to” currency amount plus the current “to” currency slot balance is greater than the “to” currency slot maximum balance.

    If the slot balance is greater than the “to” currency maximum balance, the card issuer must determine the action based on its risk and liability policy for slot balances. These policies are at the discretion of the card issuer, subject to any maximums that are established by the scheme provider or for legal or regulatory reasons. Options include decline the transaction, adjust the maximum slot balance, or offer cardholder a partial currency exchange.

12. The card issuer validates the S_1. If the S_1 is valid, the card issuer generates the S_2 MAC. If the S_1 is not valid, the transaction is declined.

13. The card issuer logs the CEP currency exchange request.

14. The card issuer sends the S_2 in the response to the load acquirer and the new maximum slot balance, if appropriate. Any script messages to be sent to the CEP card are included in this response.

15. The card issuer updates its funds pool. The card issuer decrements the “from” currency funds pool and increments the “to” currency funds pool. It updates the card database with transaction detail and adjusts liabilities as appropriate.

16. The load acquirer sends the response to the load device. Any script messages from the card issuer are included in the message to the load device.

17. If the message from the load acquirer contains a script message that is to be sent to the card before the currency exchange command, the load device sends the script message to the CEP card.

    The load device sends the currency exchange command to the CEP card.

    If the message from the load acquirer contains a script message that is to be sent to the card after the currency exchange command, the load device sends the script message to the CEP card.

18. The CEP card validates the S_2, decrements the “from” value, increments the “to” value, adjusts the maximum balance, as appropriate, and generates an S_3 MAC. It then creates a record in its internal transaction log.

19. The CEP card sends a confirmation status to the load device.

20. The load device displays a message to the cardholder advising of the new balances in the “from” and “to” slots. If possible, it issues a receipt. The load device logs the transaction, if applicable.

21. The load device sends a transaction completion message with the S_3 to the load acquirer. For successful transactions, the timing of the completion message is at the discretion of the load acquirer. For unsuccessful transaction, the completion message, with its error notification, must be sent immediately to the load acquirer who notifies the card issuer.

22. The load acquirer receives and logs the S_3 which is retained for the period of time defined in the scheme provider’s operating regulations.

5.5 On-line Exception Processing

The load acquirer’s load host or load device or both may experience exception processing conditions when processing a load, unload, or currency exchange transaction. This section describes the actions that the load acquirer must take for specific exception conditions, some of which require reversing transactions.

Receipt of a positive completion response with an S_3 MAC from the CEP card is proof to the load acquirer that the transaction completed. To guard against fraud in an unlinked load transaction, the load acquirer must test receipt of a negative completion message from the CEP card by comparing the S_3’ returned from the card with the S_3’ received from the card issuer.

When a completion response to a load, unload, or currency exchange transaction is not received by the load acquirer, the load acquirer must log the transaction as a suspect transaction. A suspect transaction is one whose completion status is unknown. The load acquirer must advise the card issuer of all suspect transactions. In addition, there must be a procedure to notify the card issuer if the status of a suspect transaction is changed to positive or negative completion.

In linked loads, unlinked loads from cash and currency exchange transactions, the load acquirer and the card issuer are the only two entities involved. After the card issuer has sent the approval response with S_2, the card issuer moves funds on the presumption that the transaction concluded successfully unless a reversal transaction is received from the load acquirer.

Unload transactions are always on-us where the load acquirer, card issuer and funds issuer are always the same financial institution. In an unload transaction, funds move only on receipt of a positive completion message with a valid S_3.

6. Card Requirements

6.1 Compatibility

The CEP application must be implemented only in cards that comply with EMV version 3.1.1 Part I and Application Selection as specified in EMV Part III. Refer to the Document References section.

The card must support either T=0 or T=1 as described in EMV. Other applications may be on the card.

6.2 Multiple Currencies

The CEP card may support multiple currencies. Each currency occupies a “slot” within the CEP. The slots are defined by the currency supported. The currency for an individual slot is determined during load or currency exchange. Currency exchange could apply to a single slot, and then only for the total balance.

It is a card issuer’s decision to determine the currencies that are allowed to occupy slots in the CEP card. This decision is made by the card issuer during the load or currency exchange transaction, by approving or rejecting the request to authorize the transaction.

A single currency cannot occupy more than one slot. The CEP card must not permit a slot to be assigned a currency if another slot in the CEP card has already been assigned to that currency.

The CEP card limits each slot to a maximum balance. The maximum balance for a slot is established when a currency is assigned to the slot, and is determined externally by the card issuer or by CEP card data which indicates a maximum balance in a reference currency. There is no requirement that all slot maximums have the same relative value, and there is no requirement for the card to maintain a maximum total value.

The card must not allow a slot to exceed the maximum balance, and must reject any command that would raise the current balance above the maximum.

6.3 Data Integrity

The card must provide integrity of data for purchase, load, unload, currency exchange and purchase cancellation transactions. For example, a cardholder might remove the card from the interface device during processing of the transaction. A hardware malfunction may cause the same effect. Regardless of the point of processing within the card that such an interruption occurs, integrity of the card data must be maintained, using internal checksums.

6.4 Card Security Functions

The card must securely maintain the keys and certificates identified in the security section of this document, including:

- The symmetric load key.
- The RSA key used for authenticating the card to the PSAM (CSK).
- The regional(optional), issuer and card certificates (RCERT(optional), ICERT and CCERT) used to support the cryptogram generated by CSK.
- The CA public key (modulus and exponent) used to authenticate the acquirer certificate from the PSAM.

Only one version of the CA public key is required in the card. This requires that the PSAMs with which the CEP card exchanges cryptograms must be capable of generating and validating cryptograms using the relevant keys from all current cards.

The number and management of symmetric keys in the card beyond the mandatory requirements is at the discretion of the card issuer.

The above keys and certificates must not be able to be altered or revealed externally by any command or process that is not described in this document or the personalization document to be written by the issuing payment scheme. The card must be capable of supporting RSA cryptographic algorithms and DES with a 16 byte key (triple DES). Any alternative symmetric methods used for the issuer MACs (such as the S_6 MAC for purchases) must provide at least equivalent strength to triple DES.

7. Key Management

Private and public keys are required in both the CEP card and the PSAM during transaction processing at a POS device. During personalization the data elements containing card/PSAM private keys and CA public keys are created and stored in the nonvolatile memory of the ICC.

These keys in the CEP card may be accessed or updated later by the electronic purse card issuer while connected on-line to the card, when the load acquirer and card issuer are the same institution. Keys in the PSAM may be updated during collection processing. During these update processes, the confidentiality of the keys must be protected by encipherment.

7.1 Certificate Hierarchy

The hierarchy of public keys used to authenticate a CEP card in a POS transaction must consist of a minimum of three levels. A three-level hierarchy is comprised of a CA public key (contained within the PSAM), an issuer public key (contained within an issuer certificate in the CEP card), and a card public key (contained within a card certificate in the CEP card). The CA private key is used to create the issuer certificate, and the issuer private key is used to create the card certificate.

With a four-level hierarchy, a regional public key is inserted between the CA public key and the issuer public key, and resides within a regional certificate in the CEP card. In this case, the CA private key is used to create the regional certificate, the regional private key is used to create the issuer certificate, and (as in three-level) the issuer private key is used to create the card certificate.

The hierarchy of public keys used to authenticate the PSAM in a POS transaction uses a similar structure. It, too, may be of either three or four levels, with a CA public key, a regional public key (optional), an acquirer public key, and a PSAM public key. Only the highest level, the CA public key, resides in the CEP card.

Both the CEP card and PSAM must be capable of recovering the appropriate keys and certificates from either a three-level or four-level hierarchy.

7.1.1 Creating Issuer and Acquirer Certificates

Certification authority providers must be able to generate public and private key pairs, receive regional or issuers’ and merchant acquirers’ public key data through the scheme provider for certification, and deliver the certificates to regions, issuers and merchant acquirers.

During implementation, identification of certification authorities must be determined. However, the PSAM must be able to contain multiple CA public keys, regional certificates (when they are used), and acquirer certificates for each active

CA public key. The number to be stored must be decided by the scheme provider during implementation.

Certification authorities must certify the regional or issuer and acquirer public keys. Where regional authorities exist, they must certify the card issuer and merchant acquirer public keys within their regions. Card issuers must certify card public keys, and merchant acquirers must certify PSAM public keys.

The public key data of the region must be signed by the regional private key when conveyed to the CA. After receiving the region's input file from the scheme provider, the CA uses the regional public key to verify the signature and generate the regional certificate.

The public key data of the issuer must be signed by the issuer's private key when conveyed to the CA or the region. After receiving the issuer's input file from the scheme provider, the CA or region uses the issuer's public key to verify the signature and generate the issuer's certificate.

The acquirer public key data must be signed by the acquirer's private key when conveyed to the CA or region. The CA or region provider, after receiving the merchant acquirer's input file from the scheme provider, uses the acquirer's public key to verify the signature and generate the acquirer's certificate.

If a region is used, the scheme provider must securely send the regional certificates to the region. The region or scheme provider must securely send the issuer's and acquirer's certificates to the issuer and merchant acquirer. Details of secure distribution of these certificates are outside the scope of this document and will be determined during implementation. During personalization, the region and acquirer certificate is loaded into the PSAM and the region and issuer certificate is loaded into the CEP card. The appropriate CA public keys are also downloaded during personalization.

The format of issuer and card certificates must comply with EMV'96 - refer to the Document References section. According to EMV'96, public key exponents used for all public keys must be 2, 3, or 2^{16}+1.

To distribute certificates, scheme providers are responsible for the interface between the CA, region (if applicable), issuers and merchant acquirers. Scheme providers must also manage the issuer certificate revocation lists and issuer's and acquirer's certificates.

7.1.2 Security Maintenance in the PSAM

New CA public keys may be distributed (on-line or off-line) to active PSAMs, or are loaded into the PSAM during personalization.

New acquirer certificates may be distributed (on-line or off-line) to active PSAM's, or are loaded into the PSAM during personalization.

Issuer certificate revocation lists are distributed to active PSAMs.

All updates to security mechanisms in the PSAM, whether performed on-line or during personalization, must be secured cryptographically to allow the PSAM to validate that the updates originated from the merchant acquirer

7.1.3 Key Lengths

The public key minimum lengths are:

- 1024 bits for the scheme provider.
- 1024 bits for the regional authority.
- 896 bits for the card issuers and merchant acquirers.
- 768 bits for the CEP card.
- 736 bits for the PSAM keys.

Longer keys may be mandated by individual schemes for all except the PSAM keys, but must follow EMV policies.

7.2 CEP Application Personalization

This section provides the key management requirements for CEP application personalization. The processing details of CEP application personalization vary by scheme provider.

The following cryptographic elements must be placed onto a CEP card during the personalization process:

- A diversified CEP card load key that controls security for load and, optionally, unload transactions.
- A diversified CEP card currency exchange key that controls security for currency exchange transactions.
- A diversified CEP card purchase key that controls security for purchase transactions.
- An optional diversified CEP card update key that controls security for the update process.
- An optional diversified CEP card unload key that controls security for the unload process.
- A CEP card RSA key pair.

  The private key portion must be stored in a secure location in the CEP card.

This data must only be accessible by the CEP card for its own processing. There must be no mechanism to retrieve the CEP card private key from the CEP card. The public key modulus is stored in a CEP card certificate which is signed by an issuer private key. Other card public key information (version, algorithm code, exponent and possibly a key remainder) must also be stored.

- An issuer certificate.

  An issuer certificate contains the RSA key modulus of the key used to create the CEP card certificate. Other card public key information (version, algorithm code) must also be stored.

- An RSA certification authority public key that is used to authenticate a PSAM.

  Additional cryptographic elements may be placed onto a CEP card to support the personalization process.

7.3 PSAM Personalization

This section provides the key management requirements for PSAM personalization. The processing details of PSAM personalization vary by scheme provider.

When a PSAM is personalized, it must be assigned a unique identification number. This number may be extended with a scheme provider identifier and a merchant acquirer or system operator identifier to ensure that the PSAM identifier is unique across schemes.

The following cryptographic elements must be placed onto a PSAM during the personalization process:

- An update key that allowing for secure updates during the life of the PSAM.

  This update capability is optional if there exists a mechanism to replace the PSAMs when updates are required.

- A merchant acquirer key for creating MACs on transactions and batch headers during the POS transaction process.

- An optional merchant acquirer key to ensure that acknowledgments to delete a transmitted batch are valid. This may be the same key as used for creating MACs.

- A PSAM RSA key pair.

  The private key portion must be stored in a secure location in the PSAM. This data must only be accessible by the PSAM for its own processing. There must be no mechanism to retrieve the PSAM private key from the PSAM. The public key portion is stored in a PSAM certificate which is signed by a merchant acquirer private key.

- Merchant acquirer certificates.

  An acquirer certificate contains the public key portion of the same RSA key pair as the private key used to create the PSAM certificate.

  If a scheme has multiple public keys that allow CEP cards to validate PSAMs, the PSAM must have an acquirer certificate created by the private portion of each of those keys.

- A scheme RSA public key that is used to authenticate the CEP card.
- There may be multiple scheme RSA public keys and certificates in the PSAM.

  While all of this data must be placed onto the PSAM prior to its use, not all of the information must be placed onto the PSAM in a single process. Whether a single process is used or multiple processes are used, the method of placing data onto the PSAM must ensure the confidentiality of the secret data and the integrity of all other data.

7.4 Key Management Entities

The key management process involves the following entities:

- The scheme provider.
- The scheme certification authority.
- The regional certification authority (optional).
- The card issuer.
- The merchant.
- The merchant acquirer.

Each of these entities is described below.

7.4.1 Scheme Provider

The scheme provider is responsible for:

- Providing a scheme certification authority.
- Arranging to have one or more scheme RSA key pairs for CEP card verification generated and assigned version numbers.
- Arranging to have one or more scheme RSA keys pairs for PSAM verification generated and assigned version numbers.
- Distributing the public key portions of the scheme RSA key pairs for CEP card verification, along with their version numbers, to all PSAM personalizers.

- Distributing the public key portions of the RSA key pairs for PSAM verification, along with their version numbers, to all card issuers.
- Establishing a process that allows the card issuers, merchant acquirers and regions to obtain certificates. This may include establishing or certifying regional certification authorities.
- Receiving and forwarding the requests for generating regional or issuer and acquirer certificates to the CA provider.
- Distributing CA public keys to regions, or to card issuers and merchant acquirers.
- Distributing aggregation parameters to merchant acquirers.
- Distributing blocking lists to merchant acquirers.
- Distributing issuer certificate revocation lists to merchant acquirers.

7.4.2 Scheme Certification Authority

The scheme certification authority is responsible for:

- Generating, labeling, and storing the scheme RSA key pairs, as requested by the scheme provider.
- Providing the scheme RSA public keys to the scheme provider for distribution.
- Where regional certification authorities exist, scheme certification authorities must sign regional public keys to create regional certificates.
- Where regional certification authorities do not exist, signing issuer and acquirer public keys with the active scheme private key to create certificates.

7.4.3 Regional Certification Authority (optional)

The regional certification authority is responsible for:

- Generating, labeling, and storing the region RSA key pairs, as requested by the scheme provider.
- Providing the region RSA public keys to the scheme provider for certifying.
- Signing issuer and acquirer public keys with the active regional private key to create certificates.

7.4.4 Card Issuer

The card issuer is responsible for generating the following keys:

- Card issuer RSA key pairs.
- Card RSA key pairs.
- Card RSA key certificates and associated data.
- Card load key.
- Card currency exchange key (optional).
- Card diversified key (for generating S_6).

The card issuer is also responsible for ensuring that the cards are personalized with the following keys and certificates:

- Regional certificates (where they exist).
- Issuer certificate.
- Card certificate.
- Card private key.
- Card load key.
- Card diversified key.
- Certification authority public key.

Additionally, the card issuer is responsible for:

- Establishing key life cycles consistent with card issuer risk management policies.
- Submitting the card issuer public key for certification to the scheme provider or regional authority.
- Maintaining a list of issuer certificates and associated certificate identifiers.
- Notifying the scheme provider when issuer public keys have been compromised and identifying the key.
- Generating, using, and storing all keys using appropriate security practices.
- Authenticating and authorizing load, unload, and currency exchange transactions.
- Validating purchase and purchase cancellation transactions.
- Generating the symmetric master keys that are used to diversify the CEP card symmetric keys.
- Generating one or more issuer RSA key pairs.

- Interfacing with the scheme or regional certification authority to obtain an issuer certificate for each RSA key pair generated.
- Obtaining the RSA public key for PSAM verification from the scheme provider or regional authority.
- Generating an RSA key pair for each CEP card.
- Generating a certificate for each CEP card.
- Generating diversified symmetric keys for each CEP card.
- Ensuring that all CEP card keys are placed onto the CEP card in a secure manner.
- Generating keys to be provided to card suppliers and card personalizers to ensure the security of unpersonalized CEP cards and CEP card secret data during transport.
- Maintaining a cross-reference between the number of each CEP card personalized and the number of the card issuer certificate on the CEP card.
- Maintaining a cross-reference of all of the identification numbers of all of the applications personalized on an CEP card.

7.4.5 Merchant

The merchant is responsible for:

- Receiving, maintaining, and securing PSAMs.
- Maintaining, in the terminal, the current date, time and static data required for transaction processing.
- Receiving and passing to the PSAM updates to:
  - Certification authority public keys.
  - Issuer certificate revocation list.
  - Aggregation parameters.
  - Blocking lists.

7.4.6 Merchant Acquirer

The merchant acquirer is responsible for:

- Generating acquirer RSA key pairs.

- Submitting acquirer public keys for certification to the scheme provider or regional authority.
- Creating PSAM RSA key pairs and certificates.
- Personalizing and installing PSAMs.
- Distributing CA public keys to all PSAMs through personalization or updating active PSAMs.
- Generating, using, and storing keys using appropriate security practices.
- Distributing issuer certificate revocation lists, blocking lists and aggregation parameters to all merchants with active PSAMs.
- Generating the symmetric master keys that are used to diversify the PSAM symmetric keys.
- Generating diversified symmetric keys for each PSAM.
- Ensuring that all PSAM keys are placed onto the PSAM in a secure manner.
- Generating keys to be provided to PSAM suppliers and PSAM personalizers to ensure the security of un-personalized PSAMs and PSAM secret data during transport.

8. Reporting

8.1 Types of Reporting

Reporting should be regarded as sensitive information. All applicable data protection laws must be followed. Required reporting categories are:

- Reconciliation/Accounting

  This is a process that ensures that data residing on more than one database is in balance. Reconciliation reports or extracts of data are required to ensure system integrity. Accounting reports for each participant provide the bookkeeping to track CEP card activity for the functions performed by the participant.

- Audit Reporting

  This consists of reports and data to ensure each component of the system is operating properly. An audit trail must be traceable to identify the source transactions used when providing summarized data in reports.

- Risk Management

  This provides the participant with data to identify fraud or system-related financial risk; for example, cards or transactions not generated by the system or processed multiple times. Each participant is required to proactively identify suspicious activity or fraud for its environment and to notify the appropriate risk group if suspicious activity exists. The risk groups require access to system data for risk analysis.

8.2 Minimum Reporting Requirements

This section describes the minimum reporting requirements to support an interoperable CEP system. These are:

- Settlement reporting must come from the entity creating the settlement transaction and validating the transactions.

- A processor must provide detailed reconciliation reporting for participants.

- Exception reporting must be supported and robust enough to ensure transaction integrity.

- Purchase transactions that have MACs must be stored with their MACs and must be made available to the card issuer according to currency.

- Load data must be available to the card issuer’s system that maintains the card issuer liability.

- Card issuers and merchant acquirers must send suspicious transactions to a scheme provider central data repository for additional analysis if the scheme has a central repository.
- It must be possible to determine the source and detail of all transactions included in consolidated and summarized data.

9. 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.

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. Transactions in a batch must have consecutive numbers assigned by the PSAM. 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 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.

Card to Card Transaction

Transferring value from one electronic purse card to another electronic purse card.

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.
- Specify different cardholder verification control policies and hierarchies for different types of transaction, terminal types, merchant categories, and transaction amounts.
- 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 purchase terminals.

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.

Disposable Card
An electronic purse card that is personalized with a monetary value at the time of manufacture, lacks the ability to add funds to it, and cannot be used once the funds are depleted.

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.

K.

Key Management

A technique for securely distributing cryptographic keys to parties involved in a secure transaction. The primary standard for key management is known as ANSI X9.7. Other techniques, including proprietary methods, are used for government classified information systems. 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, PIN-based 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.

LSAM (Load SAM)

A SAM installed at the load device or load 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, in turn, validates the card. See also Two-way Authentication.

N.

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

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 (PKE)

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

A file 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.

Purse to Purse Transactions

Transferring value from one electronic purse to another electronic purse.

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.

10. Acronyms

Acronym or Data Element	Description
ACERT	Acquirer Public Key Certificate
ALGCCEP	Conversion algorithm identifier
ALGL	Load Algorithm Identifier
ALGPA	Purchase Key Algorithm Used by the CA to Produce the Acquirer’s Certificate Contained in the PSAM
ALG_{PDA}	Cryptographic Algorithm to Use in Purchase
ALGPI	Purchase Key Algorithm Used by the CA to Produce the Issuer’s Certificate Contained in the Card
ALGPS	Symmetric Cryptographic Algorithm Used to Create the S_3 Signature (MAC) on a Purchase Transaction
AM_{PDA}	Authentication Method Used in Purchase
ATM	Automatic Teller Machine (Unit)
ATR	Answer-to-Reset
BIN	Bank Identification Number
CA	Certification Authority
CAD	Card Acceptance Device
CBC	Cipher Block Chaining
CCERT	Card Public Key Certificate
CEN	European Committee for Standardization
CEP	Common Electronic Purse
CEPS	Common Electronic Purse Specifications (or System)
$CERTIDA_{CEP}$	Identifier of the Acquirer’s Certificate Contained in the Card
CSK_{CEP}	Card Private Key (RSA)
CURR	Currency
DB	Database
DDA	Dynamic Data Authentication
DDEA	Deactivation Date
DDF	Directory Definition File
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DEXP	Expiration Date
DF	Dedicated File
EEPROM	Electronically Erasable Programmable Read-Only Memory
EF	Elementary File
EMV	Europay, MasterCard and Visa

Acronym or Data Element	**Description**
FCI	File Control Information
FI	File Identifier
GSM	Global System Mobile
IC	Integrated Circuit
ICC	Integrated Circuit Card
IFD	Interface Device
ISO	International Organization for Standardization
Iss	Issuer
LCD	Liquid Crystal Display
LDA	Load Device Application
LRC	Longitudinal Redundancy Check
MAC	Message Authentication Codes
MF	Master File
PAN	Application Primary Account Number
PDA	Purchase Device Application (Purchase Device)
PIN	Personal Identification Number
PK	Public Key
POS	Point of Service
PSAM	Purchase Secure Application Module
RAM	Random Access Memory
RFU	Reserved for Future Use
ROM	Read Only Memory
RSA	Rivest, Sharmir and Adlemen (Cryptographic Algorithm)
SAM	Secure Application Module
SFI	Short File Identifier
SHA	Secure Hash Algorithm
TLV	Tag, Length, Value
Var	Variable