Common Electronic Purse Specifications

Business Requirements

Version 7.0

March, 2000

TABLE OF CONTENTS

I. Document Specifics

Objectives

The objective of this document is to define the business requirements for an open, common, interoperable electronic purse environment. It is the source for the functional requirements and technical specifications. The functional requirements document will follow publication of these business requirements and will include more details of the product and systems functionality. The technical specifications document will follow publication of the functional requirements and will enable payment systems to develop electronic purse schemes, and participants of these schemes to develop the products and systems required for implementation.

Scope of Document

The document identifies the market need and drivers, benefits, product mission and description, and the requirements for an overall electronic purse system, including:

- Security
- Card application
- Terminal application
- Load transactions
- Unload transactions
- Currency Exchange transactions
- Point-of-sale transactions
- Public/open networks
- Transaction processing
- Settlement and reconciliation
- Clearing and administration
- Overview of certification procedures

Fees

Fees which may be charged to and by various participants of this electronic purse scheme are not addressed in this document. However, it is recognized that the product must accommodate fees in order to achieve profitability.

Document Structure

The document is structured to explain the need for an open, common, interoperable electronic purse environment and define the requirements to offer and operate electronic purse schemes throughout the world. Sections include:

- Document Specifics
- Introduction
- General Principles
- Security Requirements
- Card Requirements
- Load Requirements
- Unload Requirements
- Currency Exchange Requirements
- Point-of-Sale Requirements
- Public/Open Network Requirements
- Transaction Processing Requirements
- Settlement and Reconciliation Responsibilities
- Clearing and Administration
- Appendices

Document Word Usage

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

- Must
  Defines a product or system capability which is required, compelled and mandatory.
- Should
  Defines a product or system capability which is highly recommended.
- May
  Defines a product or system capability which is optional.

Document Versions

New versions of CEPS must describe a migration path from previous CEPS application versions.

II. Introduction

Background

Worldwide, various electronic purse schemes/system providers and participating financial institutions have already developed and deployed electronic purse systems that are different from each other and are not interoperable. This means that cardholders cannot use cards issued with one scheme/system's technology in terminals that are configured with another scheme/system's technology. Further, most schemes/systems operate in discrete domestic environments without the capability for consumers to use their cards across national borders due to the fact that multiple currencies are not supported on the cards and in the terminals. With the advent of the common European currency, cardholders with a common currency will not be able to use their cards in terminals across national borders. Technology that allows cardholders to use their electronic purse cards on a domestic and/or international basis with the knowledge that the card is accepted wherever the card's acceptance mark is displayed is, therefore, required.

Market Need

Consumers travel internationally with increasing frequency and regularity, and they expect to receive the same service and convenience in making payments while traveling as they receive at home. Cardholders expect to be able to use a card with a given mark at any terminal with a matching mark, just as they do with debit and credit products. Additionally, merchants want to serve all consumers quickly and efficiently.

The credit card and debit card environments today have evolved to a point where these consumer and merchant expectations about convenience and service are met in almost any country in the world. These same expectations will extend to the low value payments that today are typically conducted using cash. The consumer and merchant demand for convenience, speed and efficiency drives the need for an interoperable electronic purse product.

The lack of interoperability will be the single greatest obstacle to cross-border/international and cross-system volume deployment of smart cards. All schemes/systems will need to make some changes to accommodate the interoperability capability. That said, however, electronic purse card scheme/system providers will want to be able to leverage their considerable investments in the technology, infrastructure, marketing and product sales of the different systems that today are not interoperable.

The common system specifications described in this document will allow organizations to confidently proceed with infrastructure and application investments which allow that, and which result in global acceptance, reliability, cost effectiveness and opportunities for differentiation.

Interoperability Definition

Interoperability for the purposes of this document is the following:

- Electronic purse applications that utilize technology-independent, end-to-end transaction processing.
- Devices that allow electronic purse cardholders, merchants and financial institutions, regardless of the underlying technology, to perform electronic purse transactions.
- Systems which clear and settle transactions performed by cardholders and merchants, regardless of the card issuer, acquirer and/or scheme provider.
- Applications, devices and systems which meet electronic purse issuers' expectations of quality, convenience and service for their cardholders.

Key Market Drivers

A major market driver for interoperability is the public network segment, including the Internet, telephones, and cable and satellite TV. Electronic commerce over public networks is a rapidly growing market worldwide. The need for a product to handle micropayments is here today, and payment system providers must be prepared with an internationally interoperable product solution.

Another key market driver is the advent of the Euro, the common European currency, which will be issued by most European countries by July, 2002. Cardholders will expect to be able to use their cards in terminals with a matching acceptance mark wherever they travel throughout Europe in countries that have a common currency.

With an interoperable electronic purse product, participants have a tool to meet these evolving customer needs, leverage their investments in existing payment mechanisms, and address growing competitive alternatives in electronic purse payment mechanisms.

Benefits

The various constituents who will benefit from interoperability and an open market include, but are not limited to, cardholders, merchants, issuers, POS and load acquirers, system operators, scheme providers, chip manufacturers, operating system developers, card and terminal manufacturers, and system integrators.

Cardholder Benefits

- Cardholders are offered convenience and consistent service so that they can use their electronic purse cards in a similar manner both domestically and internationally wherever the acceptance mark is displayed.
- Cardholders can load value to their electronic purse cards in an unattended or attended load environment at any load device that displays the common brand.

Merchant Benefits

- Merchants can render services to electronic purse cardholders with cards from any electronic purse scheme supporting the Common Electronic Purse Specifications, assuming the merchants display the acceptance mark that is on the card.
- Merchants can accept any electronic purse card in the same manner when the same acceptance mark appears on the card and terminal.
- Merchants are not precluded from maintaining a single acquirer or multiple acquirer relationships if they so desire.

Acquirer, Issuer Benefits

- Acquirers can clear and settle transactions performed by cardholders and merchants, regardless of the card issuer, acquirer, scheme provider and/or system operator, assuming the business relationship has been established.
- Load acquiring financial institutions may provide the ability for consumers to load/unload their electronic purse cards at any load device displaying the acceptance mark.
- Issuers are able to deliver on the promise of the brand.
- Issuer card products are enhanced.
- Infrastructure costs may be reduced.
- Operating system developers and chip manufacturers are assured that they are competing in an open, inclusive market which facilitates issuer/acquirer cost savings.
- Scheme operators and system integrators are assured that they may deploy an interoperable electronic purse system in any market using the common specifications, thus encouraging systems development at lower costs.
- System operators and system integrators may deploy the interoperable electronic purse system as third-party processors and/or providers, or as part of an issuer's or acquirer's system, which allows issuers and acquirers processing choices.

- Card and terminal manufacturers are able to manufacture cards and terminals that contain common specifications so that economies of scale may be realized and volume production increased.

Product Mission

The mission of the electronic purse common specification is to:

- Provide consumers and merchants worldwide with payment products that are faster, easier, less expensive and more convenient than cash, particularly in small value transactions.
- Ensure that a measure of consistency exists in the acceptance environment.
- Provide an interoperable environment for different technology platforms or schemes.
- Support a multi-currency capability.
- Offer similar convenience to cardholders when making payments while traveling internationally as they receive at home.
- Offer merchants a means to offer electronic purse services to both domestic and traveling cardholders.
- Enable issuers and acquirers to offer international electronic purse services to cardholders and merchants.
- Ensure that the infrastructure can support other products and applications.
- Enhance the current product line.
- Furnish a profit potential for issuers and acquirers by providing the opportunity to gain new customers and provide enhanced services to existing customers.
- Ensure that the electronic purse application may coexist with other applications on the same chip.
- Provide opportunities for brand and market expansion and proliferation.

Product Definition

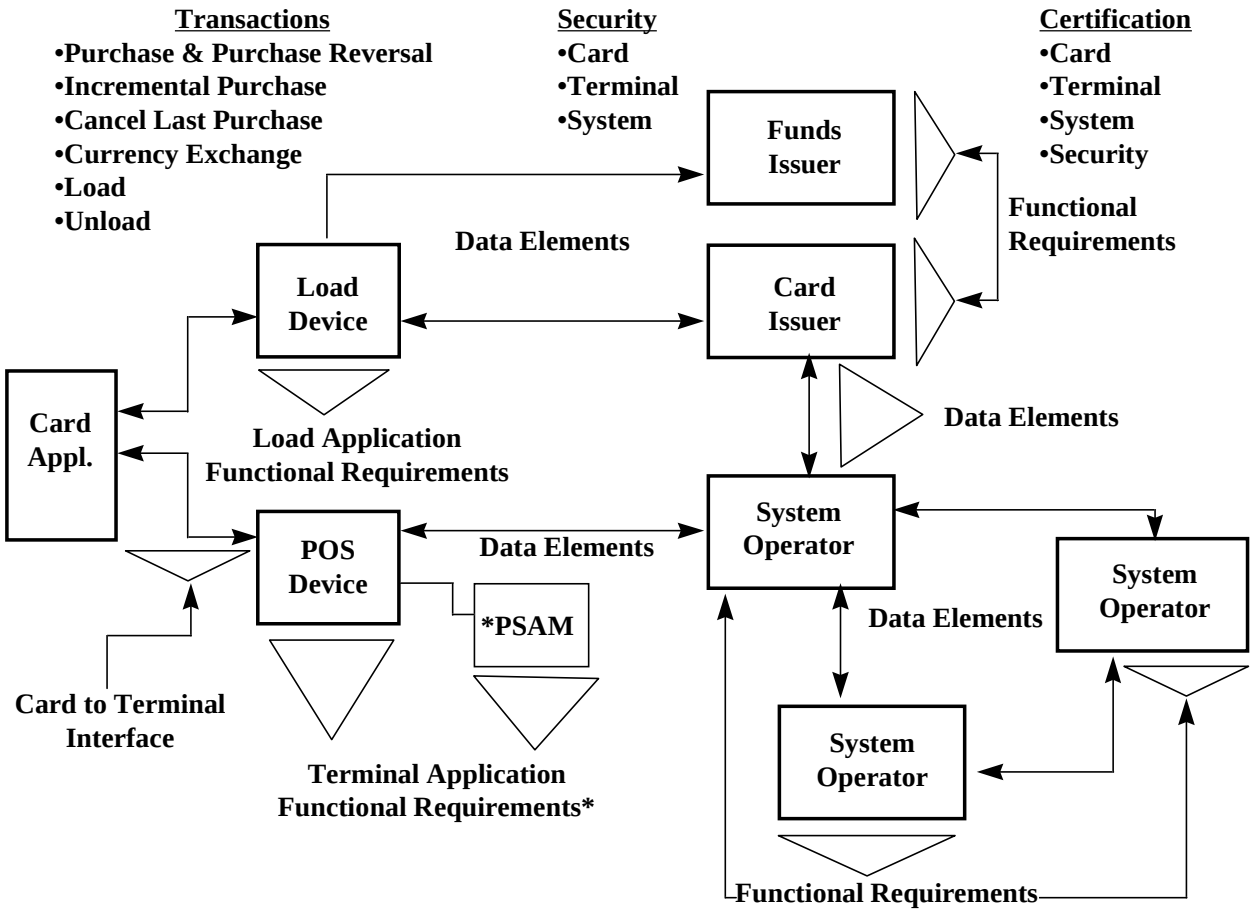
The Common Electronic Purse Specifications will provide new as well as core features of current electronic purse products, adding a multi-currency capability that offers consistent service to cardholders and merchants throughout the world regardless of the underlying technology platform or scheme. In order to encourage an open, competitive, inclusive environment, the specifications will be scaleable enough to support multiple issuers and acquirers. Following is the basic product definition for the interoperable electronic purse product.

- In order to allow issuer choice and encourage marketplace competition, the common specification must not dictate a card operating system, but only an interoperable application.

- The interoperable application is one single computer program distinguished by one unique application identifier by brand.
- Because of unique market needs and the need for product differentiation, there must be flexibility to support optional product features and system capabilities.
- So that multiple operators may deploy the system as they choose within a domestic environment, the specification must support a distributed, portable, scaleable system capability with interchange.
- The specification must support either a distributed funds pool or a centralized funds pool which is held and managed by participating issuers.
- The following transaction set must be defined in the CEPS documents:
  - Load
  - Currency Exchange
  - Purchase and Purchase Reversal
  - Incremental Purchase
  - Cancel Last Purchase
- The electronic purse specifications must support the ability of the cardholder to view his or her electronic purse card's balance, upon request, from appropriate devices.
- The electronic purse specifications must support the ability of the cardholder to view previous transactions, upon request, from appropriate devices.
- The electronic purse specifications must support the capability to deploy multiple currencies in different slots. The actual number of slots on the card is an issuer option.
- Each slot can be loaded with any currency that is supported by the card issuer and the load acquirer.
- No currency conversion occurs at the point of sale until the technology and business needs support it. The currency of the terminal at the point of sale must have been loaded into a slot on the card to enable use.
- Terminals and/or acquirers must be able to route transactions appropriately for interchange purposes.
- The electronic purse application must support the ability to be linked to a specific funding account, or to be independent of any specific funding account.
- The architecture, technology and infrastructure for the interoperable electronic purse product must support truncation and aggregation at the option of the scheme and its issuers.
- To ensure the perception of relative security, the lock and unlock capability must be included in the common specification, with locking enabled at issuer option and implemented at cardholder option.

- The technology deployed for the CEP components and systems must not unreasonably degrade the performance of the electronic purse product from a consumer or merchant perspective.

The following diagram illustrates the scheme participants, transaction set, data elements and rules to be developed in the business requirements, functional requirements and technical specifications for the interoperable product:



III. General Principles

Participation and Timing

Participants of a purse scheme moving to the common specifications described in this document are encouraged to convert their systems as soon as possible following the publication of the Technical Specifications. Moving quickly ensures timely market response to the competition, and moves cards and equipment to the common specifications before large numbers of cards and terminals with systems that must be converted are deployed. However, the intent is to be as supportive of participants as possible, whatever their strategy for implementation.

In the case of the euro-zone, the implementation of the systems supporting the European common currency is required to be complete on July 1, 2002. Therefore, the last possible date for the implementation of specifications is the same. Schemes adopting these specifications should begin to migrate to support them no later than eighteen months after the publication of the Technical Specifications.

Migration

- A migration plan to the initial version of CEPS is to be developed by each scheme.

Standards and Specifications

International Standards Organization (ISO)

The electronic purse common specifications must conform to all applicable ISO standards including the following:

- ISO 7810 - Nominal dimensions for bank cards, including standards for edge burring not to exceed 0.008 mm (0.003 in.), surface distortions and signature panels.

- ISO 7811, 7812 - Magnetic stripe surface profile.

- ISO 7811, 7814 - Location of magnetic stripe material.

- ISO 7813 - Specifies that the dimensions of financial transaction cards shall be 0.76 + or - 0.08 mm (0.030 + or - .0003 in.) thick, 85.47 mm (3.375 in.) wide and 54.03 mm (2.127 in.) high.

- ISO 7816 - Standards for integrated circuit cards with contacts:
  * Part 1 - Physical characteristics

- Part 2 - Dimensions and location of contacts
- Part 3 - Integrated circuit electronic signal and exchange protocols
- Part 4 - Inter-industry commands
- Part 5 - Registration system

- ISO 14443 - Identification cards - Proximity Integrated Circuit Cards evolving standard. Evolving are the following standards:
  - Part 1 - Physical characteristics
  - Part 2 - Radio frequency interface and parameters
  - Part 3 - Electronic signals and transmission protocols
  - Part 4 - Security features

The electronic common specifications must also comply with any other applicable ISO standards.

Other Relevant Standards

The common specifications must take into account work already done by relevant standards bodies such as EMV and ECBS and takes into consideration the work done by the Commission for European Normalisation (CEN) prEN1546. Applicable EMV standards include the following:

- Terminal Types and Capabilities
- Functional Requirements
- Physical Characteristics
- Security Requirements
- Terminal Software Architecture
- Software Management
- Data Management
- Cardholder and Attendant Interface
- Acquirer Interface
- Electromechanical Characteristics, Logical Interface and Transmission Protocols
- Data Elements and Commands
- Application Selection

Certification

Certification must be obtained by all system participants prior to issuing and accepting cards and processing transactions. Certification for the Common Electronic Purse system should be integrated into each scheme provider's certification procedures. The purpose of certification is:

- To ensure interoperability.

- To ensure that all elements of the electronic purse payment process function as expected and comply with all operational and security requirements in such a way that incidents are kept to the minimum level, thus protecting the brand and product.

General Requirements

- There must be a common set of criteria for the certification of electronic purse system components.
- There must be a catalogue of test cases for both positive and negative scenarios for participants to use to become certified.
- There must be test equipment with which to check the relevant components.
- There must be a defined procedure for going through the testing and certification process.
- The process must be flexible enough to support the testing of individual system components, components in various combinations, and systems as a whole.
- There must be a process for communicating certifications.
- Certification must result in a dated certificate which allows the evaluated component(s) to be implemented for a pre-defined period, following which they must be re-certified or removed from use.
- Certification test sites may be operated on behalf of issuers or acquirers for functional testing.
- Technology deployed for the Common Electronic Purse components and systems must not unreasonably degrade the performance of the electronic purse product from a consumer or merchant perspective.
- Performance standards must be established to ensure performance integrity.

Cards

Cardholder

- Cardholder cards must be tested at the physical, electromechanical, protocol level.
- Cardholder cards must be tested at the application level, including functional and security validation.
- Personalization and initialization entities must be certified in order to provide these services for cardholder cards.
- Certification processes must ensure that other applications that may reside on the card do not impact the electronic purse application.

Merchant

- PSAMs must be tested at the application level, including functional and security validation.
- Personalization and initialization entities must be certified in order to provide these services for PSAMs.
- Certification processes must ensure that the PSAM application does not adversely impact the system or its elements.

Terminals

- Point-of-sale terminals must be tested to ensure proper working with the cardholder interface.
- Certification processes must ensure that other applications that may reside on the terminal do not impact the electronic purse application.
- Certification processes must ensure that the terminal does not adversely impact the system or its elements.
- Terminals must be tested at the application level, including functional and security validation.

Balance Readers

- Balance readers must be tested to ensure that they do not damage the chip, contact plate or card, either electrically or mechanically, during normal use.

Systems

- All systems and elements that process or pass electronic purse transactions must be certified to ensure that they are in compliance with prescribed data elements, messages, timing, etc.
- Systems must be tested to ensure that they comply with all functional and security requirements.

Security

Security testing must be accomplished for all components which are, from a system's point of view, security relevant. These components are the following:

Physical

- Integrated circuit chips
  - PSAMs
  - Consumer cards
- PIN pads
-
- LSAMs

Logical

- Integrated circuit chips
  - PSAMs
  - Consumer cards
- PIN pads
-
- LSAMs

Accountability and Auditability

Except where truncation and/or aggregation is supported:

- The system must be able to trace all transactions from the point of origin to the issuer or issuer's agent. This encompasses all transactions that change the balance of the electronic purse.

Truncation

- Truncation, where transactions are stopped at a point in the process and not passed to the issuer or its agent, will be developed in the first offering of the common specifications for optional implementation.
- Support of truncation availability is an option of each electronic purse card issuer within a scheme.

Aggregation

- Aggregation, where the total consists of the sum of all transactions with no individual transaction details, will be developed in the first offering of the common specifications for optional implementation within a country and/or currency.
- Support of aggregation availability is an option of each electronic purse card issuer within a scheme.

Security

The common system's security mechanisms, methods and tools must undergo a thorough, rigorous security analysis, evaluation and certification by an independent entity.

Funds Pool Administration

- Issuers are responsible for maintaining their own funds pools.
- Issuers may delegate funds pool management to a third-party, such as a correspondent bank. However, the card issuer remains liable for the funds.

Liability

Issues that affect liability include outstanding card balances, transactions pending settlement, loss/theft of cards, escheatment of unclaimed balances, and counterfeit.

- Exception processes must be supported.
- The consumer requests customer service from his or her own financial institution.
- Liability resides with the card issuer.
- If funds are managed by a correspondent bank or a domestic funds pools administrator, it must be transparent to the cardholder.

Card Risk

Counterfeit Cards

The inventory controls used to track electronic purse cards must account for legitimate and suspected counterfeit cards.

Electronic Value Transfers

Electronic Purse - Merchant

Electronic value may be transferred from an electronic purse card to a merchant terminal/PSAM.

Merchant - Electronic Purse

Electronic value must only be transferred from a merchant terminal/PSAM to an electronic purse card to support a cancel last purchase transaction or a purchase reversal transaction.

Merchant - Acquirer - System Operators - Networks

Value may be transferred from a merchant terminal/PSAM through to a merchant acquirer, system operator(s) and network(s) as part of the clearing and settlement process.

Electronic Purse - Electronic Purse

Electronic value must not be transferred from one electronic purse card to another.

Merchant - Merchant

Electronic value must not be transferred from one PSAM or merchant terminal to another except in environments where a controller terminal acts as a transaction consolidator for other terminals of the same merchant.

Card Issuer - Electronic Purse

Value may be transferred from an electronic purse card issuer to an electronic purse to perform a load transaction.

Electronic Purse - Card Issuer

Electronic value may be transferred from an electronic purse to an electronic purse card issuer to perform an unload transaction.

Electronic Purse - Other Non-Financial Application On the Same Card

Electronic value may be transferred from the purse application to non-financial application(s) on the same chip on the card.

Disposable Cards

Although disposable cards are not part of the Common Electronic Purse Specifications, the system must not preclude support of disposable cards for business reasons in certain localities.

IV. Security Requirements

Security for the common specification must allow the product to be capable of existing within a multi-applications environment, compatible with other certified applications, with security such that no application affects the integrity or functioning of the other. Tools must be made available to ensure the integrity of the entire security process.

Authentication

General Principles

- Two-way, or mutual, authentication, where the card authenticates the terminal and the terminal authenticates the card for each transaction, must be performed for off-line transactions.
- The electronic purse product must use dynamic data authentication at the following points:
  1. Load
  2. Unload
  3. Currency Exchange
  4. Purchase, Purchase Reversal
  5. Incremental Purchase
  6. Cancel Last Purchase
  7. Personalization
  8. On-line Updates to the Application

Cryptography

For increased security and convenience, asymmetric cryptography must be used as the authentication security for off-line transactions. Using asymmetric cryptography will enable the exchange of authenticated messages and secret data without exchanging the secrets needed for performing authentication. Symmetric key cryptography is used for on-line transactions and to protect the integrity of data by generating message authentication codes (MAC). Therefore, the system must:

- Support asymmetric cryptography.
- Support symmetric key cryptography.
- Support the capability to change cryptographic keys on a regularly defined basis, as well as in emergency situations.

Card Authentication

- The card must use asymmetric cryptography for off-line transactions.
- The card must use symmetric cryptography for on-line transactions.
- The card must be loaded with the following keys to affect purchase transactions:

  - Symmetric MAC Key
  - Card private key
  - Card public key certified by the issuer with its private key
  - Issuer public key certified by a Certification Authority with its private key
  - Certification Authority's public key
- The card must authenticate the terminal at the point of sale, ensuring that it is genuine and valid, and use a two-way authentication process.

Point-of-Sale/Terminal Authentication

- The terminal must support asymmetric cryptography.
- The terminal must be loaded with the following keys:
  - Terminal private key
  - Terminal message authentication codes (MAC keys)
  - Terminal public key certified by the acquirer with its private key
  - Acquirer public key certified by a Certification Authority (the same Certification Authority as that of the card) with its private key
  - Certification Authority's public key
- The terminal must authenticate the card and the transaction at the point of sale, ensuring that they are genuine and valid.
- The terminal must participate in a two-way authentication process with the card.
- For cancel last purchase transactions, the terminal must validate the card and sign the cancellation.
- The terminal must have the capability to accept a completion code from the card.
- The terminal must secure transactions by retaining the card's symmetric MACing key signature as part of the transaction.
- The terminal must generate a symmetric MACing key signature and send it to the merchant acquirer.
- Incremental purchase transactions must use two-way authentication for the initial session authentication, and at least one-way, with the terminal authenticating the card, for the remaining increments or some of the remaining increments.
- Tools must exist to be able to prove that all security processes were performed correctly.

Load and Unload Authentication

- Load and unload functions must be authenticated using end-to-end security between the card and the card issuer.
- Master load keys must be installed at a hardware security module or under protection of a hardware security module which will work in concert with a host load application at the issuer host.

- The issuer host must authenticate the card upon the load/unload request.
- The card must authenticate the issuer host upon the response to the request.
- A proof must be sent to the load acquirer that a load or unload occurred to avoid repudiation.

Script Messaging

An update key must be used for script messaging where the parameters of a card are changed.

Key Management

The system must be protected against unauthorized transfer of electronic value or modification of data. This protection will be enforced through the use of secrets in the form of symmetric and asymmetric keys using dynamic data authentication, i.e., challenge and response. The management of these keys is critical to system security.

- The management of keys must be accomplished in a secure, certified environment.
- There may be multiple certification authorities that manage keys for the system, including the possibility of one overall highest level certification authority (perhaps on an international level), and domestic certification authorities for each country or region.

Load/Unload Security

Those who deploy new payment technologies, such as the Common Specifications for an Electronic Purse System, must be energetic in the pursuit and deployment of new security measures to accommodate these new technologies and to protect their users. Deployers of the Common Electronic Purse Specifications must actively pursue new, more demanding security measures and methods with all entities who affect scheme participants.

Electronic purse system participants must be assured that load/unload devices must not link to the system without security that protects all participants from fraud. Ideally, the same security measures and methods should be employed for all load and unload devices. The basic requirements are as follows:

- There must be adequate security for load and unload transactions which ensures that the issuer is guaranteed payment of funds.
- The common specifications must be architected in such a way as to accommodate more rigorous security measures and methods as they become available.

- Loads/unloads from devices must only be through a card issuer-cardholder banking mechanism which the card issuer controls and safeguards. Loads performed where funds movement is not under the direct control of the electronic purse card issuer may require different security measures. Such a mechanism is typically the following:
  - The card issuer financial institution provides the customer with the ability to use his or her PC to access his or her bank account(s) through the issuer financial institution's home banking page on the Internet. Access may be to an account which is either linked or not linked to the electronic purse card.
  - Secure firewalls, encryption, certification and other security is in place at the issuer to ensure the integrity of the transaction.
  - Although the PC banking mechanism allows access to any of the cardholder's accounts at a particular financial institution, it does not provide the cardholder with the ability to load/unload electronic value from any other accounts which he or she may hold at other financial institutions.
  - Other types of load/unload devices that may develop in the future must be certified by the scheme as secure prior to being allowed to link to the system. Certification guidelines must be developed to accommodate this requirement.

Transactions

- Load and unload transactions are processed on-line.
- Load transactions require a form of cardholder authentication for funds requests except when cash is the funds source.
- Load and unload transactions must be authenticated and authorized by the card issuer or the issuer's agent.
- Unload must be supported at devices that display the acceptance mark of a scheme which supports unload. Besides the domestic currency, other currencies supported are at the issuer's and acquirer's option.

Personalization

Personalization of electronic purse cards must be done under secure conditions involving four entities and processes: the certification authorities, the issuer, the card supplier and the card personalizer.

Certification Authorities

- Must generate public and private key pairs.
- Must be able to receive the issuer's and acquirer's public keys and use them to generate issuer and acquirer certificates.
- Must send the issuer certificate to the issuer and the acquirer certificate to the acquirer.

Issuer

The issuer is responsible for the initialization and personalization of its electronic purse public key cards.

Fraud Detection

- The system must support a fraud detection and reporting capability sufficient enough to aid in the detection of counterfeit and fraud.
- Fault handling and exception processing capabilities must be robust enough to ensure transaction integrity and to facilitate the isolation of unrecoverable activity.
- Schemes must provide a centralized reporting function for risk analysis.
- The system must protect the integrity of key transaction data including transaction identification, currency code and amount. If tampering is suspected, the system must cause the transaction to fail.

V. Card Requirements

General Principles

The Common Electronic Purse Specifications will enable cardholders to use the electronic purse card domestically and internationally in a similar manner. However, an Issuer may choose to limit the use of a CEPS based product, or the use of a function, to a given country or region. The following are the card requirements:

- Must use contact-based integrated circuit technology.
- Must include an integrated circuit serial number that may or may not be linked to a cardholder's account.
- Must support system-specific card numbering standards.

The following are the card application requirements:

- Must be able to be authenticated at a load device by the Issuer and point-of-sale terminal by the PSAM.
- Must require a form of cardholder identification for electronic value load from accounts in both a proprietary environment and a shared network environment unless loading from cash.
- Must support on-line PIN verification.
- Must support at least one type of off-line PIN verification (encrypted or plain text), as defined by the issuer.
- Must support purchase reversal transactions.
- May support cancel last purchase transaction capability.
- May be unloaded electronically to an account at an unattended load device.
- May be updated electronically on-line in a proprietary environment.
- Must not dictate a card operating system, but only an electronic purse application.
- Must be able to support off-line locking and unlocking, enabled at issuer option.
- Must have the capability for the issuer to identify a maximum value that can be stored on a per currency basis.

Types of Cards

- The Common Electronic Purse Specifications must be supported on single application cards and on multi-application cards.
- The Common Electronic Purse Specifications will not be supported on disposable cards.

Co-existing Applications

Compatible Applications

The electronic purse application must be capable of co-existing with other applications on the same card. Examples of applications include, but are not limited to:

- Financial payment applications
  - Debit
  - Credit
  - Domestic electronic purse programs
- Non-financial payment applications
  - Loyalty programs
  - Programs using contactless technology
  - Security identification programs
  - Cellular phone applications

General Requirements

- Financial applications, such as electronic purse, debit and credit, may be able to transfer electronic value to another application, such as telephone, loyalty or transit.
- Non-financial applications, such as telephone, loyalty or transit, may not transfer electronic value to financial applications, such as electronic purse, debit and credit.
- All applications must be protected from corrupting each other.

Locking

The architecture for the electronic purse application must include the lock/unlock capability. Lock/unlock may be deployed at the issuer's option.

Consumer Locking

The locking capability allows the consumer to lock the electronic purse application on his or her card, thus preventing any electronic value from being decremented from the card until it is subsequently unlocked.

Card Issuer Locking

Card issuers must be able to lock the electronic purse application on a consumer's card for reasons at its discretion. Card issuer locking must be performed on-line.

Multi-currency Service

- The electronic purse application must have the capability to support multiple currencies, but an issuer may choose whether to enable this function for its cardholders.
- The issuer must decide how many slots are supported.
- A slot must be loaded with only one currency at a time.

- The currency of the slot is defined when the slot is personalized, loaded or upon currency conversion.
- Value may be loaded into whichever slot is empty if the currencies already loaded are different from the one to be loaded.
- A currency may be loaded in the slot that is being converted or to a slot which already holds the target currency.
- If no slot is empty, the currency in the slot of the cardholder's choosing may be converted to the one to be loaded.

Script Messages

The electronic purse card issuer may wish to send a message to the electronic purse card application for various reasons. For example, the electronic purse card issuer may wish to update a card parameter such as the expiration date.

- Script messaging is enabled at the option of the electronic purse card issuer.
- Script messaging is performed on applications which already reside on the card.

Logs

- Purchase, purchase reversal, cancel last purchase, load and unload transactions must be recorded in log(s) on the card.
- Standard log fields and discretionary fields should be specified.
- Log(s) must provide meaningful information to cardholders when displayed or printed.
- The size of the log is at the discretion of the issuer.

Manufacturing

Issuers must use scheme-approved entities in manufacturing cards. This includes:

- Plastic manufacturers
- Silicon manufacturers
- Chip imbedders
- Personalizers

Personalization

Cards must be personalized with the appropriate keys.

Expiration Dates

- The application must have an expiration date which is checked by the device when the card is either loaded, unloaded, or used for currency exchange, purchase, or cancel last purchase transactions.
- Expired cards must not be used for loading electronic value.

- The time period during which a cardholder can unload electronic value, perform a purchase or a currency exchange from an expired card may be determined by each issuer.

Card Security

Please see the Security Section for card security requirements.

VI. Load Requirements

A load transaction is when electronic value is incremented to a reloadable card from a financial institution account or from cash. Support of the load function is required for Common Electronic Purse Specifications participants.

General Requirements

- Consumers must be able to load electronic value to their cards at any participating load device, regardless of the location, provided that the currency that is requested is supported by the acquirer and the card issuer.
- Funds issuers must accept funds authorization requests, regardless of the load currency type, as permitted.
- All participating load devices must adhere to the Common Electronic Purse Specifications.
- Support of loading from cash is optional.
- Home, or venue-based, loading must be from an account located at a financial institution.
- Electronic purse load transactions must be uniquely identified as such.
- The funds pool must be incremented to increase the card issuer's liability.

Funds

- The source of funds for a load may be independent from the issuer of the electronic purse card.
- Load devices that are available to the general public should support multiple sources of funding and support both linked and unlinked loads.
- The source of funds may be cash.

Cardholder Authentication

- Authorizations for load transactions require a form of cardholder authentication for funds requests.
- The load device must support on-line PIN encryption or off-line PIN verification.
- The load device which supports only off-line PIN verification must support both the off-line PIN encryption method and the off-line PIN plain text verification method as defined in EMV.
- Load devices must be equipped with a secure PIN pad.

Types of Load Devices

The architecture for the electronic purse service should not preclude the eventual deployment of a variety of devices to meet the needs of many card acceptance environments. (While today ATMs and cashless ATMs provide most of the loading capability for electronic purse cards, in the future, load devices may be attended, unattended, public venue, home devices, and other devices not mentioned here and/or yet to be developed.) There must be an agreed upon approval process for new devices.

Receipts

Load transactions require the load acquirer to provide consumers with the option of a receipt, as appropriate and subject to local regulations.

Card Capture

Card capture, where the card is pulled into the interior of a load device so that it may not be retrieved by the cardholder, may be supported at the issuer's option and if the device is capable.

Database/Archive

- The electronic purse card issuer must reflect all changes in the value of a loaded card and the aggregate funds pool on their card databases and funds pool accounting systems (where separate).
- The load acquirer must keep records by card number of all loads that take place at its load devices.

Load Security

Please see the Security Section for load security requirements.

VII. Unload Requirements

An unload transaction is when electronic value is decremented from a reloadable card into a cardholder's bank account. Support of the unload transaction is an issuer's option. However, if multiple currencies are supported, and currency exchange is not supported by the issuer, then unload must be supported by the issuer. (This is to allow the removal of value from a card of a currency which is no longer needed.)

General Requirements

- Cards should be unloaded to an account which is resident at the card issuer's financial institution. (Unlinked unloads are not precluded but are out of the scope of CEPS.)
- Unloads to cash (redemptions) are only permitted to resolve customer service issues, and must be performed at the issuer's location.
- Unload technical specifications should be very similar to those of the load technical specifications.
- Partial unloads are at the option of the card issuer.
- Unloads must conform to all relevant local regulations.
- Unload transactions must be uniquely identified as such.
- The funds pool must be decremented to reduce the issuer's liability.

Cardholder Authentication

Unload transactions do not require cardholder authentication. (However, an acquirer's devices may be configured such that authentication is required for access.)

Types of Unload Devices

The architecture for the electronic purse should not preclude the eventual deployment of a variety of devices to meet the needs of many card acceptance environments. Unload must not be precluded from being supported on any or all of these devices at the option of the acquirer.

Receipts

Unload transactions require the unload acquirer to provide consumers with the option of a receipt, as appropriate and subject to local regulations.

Card Capture

Card capture, where the card is pulled into the interior of a load device so that it may not be retrieved by the cardholder, may be supported at the issuer's option and if the device is capable.

Database/Archive

- The electronic purse card issuer must reflect all changes in electronic value on its card databases and funds pool accounting systems (where separate).
- The unload acquirer, or unload operator, must keep records by card number of all unloads that take place at its load devices.

Expired Cards

- Unload must allow the consumer to remove the electronic value from his or her card after the card has expired and can no longer be used to make purchases.
- Issuers and acquirers must support unload on expired cards for a minimum period of time as defined by the scheme or local regulations.

Unload Security

Please see the Security Section for unload security requirements.

VIII. Currency Exchange Requirements

Card issuers have the option of offering as many slots as they wish for their cardholders' use. Nevertheless, it is very possible that a cardholder will require a currency exchange at one time or another. This is because it is difficult to determine the exact number of slots for each individual cardholder such that a slot is always available and/or containing the desired currency. Further, a cardholder may wish to exchange the currency of a slot when returning to his or her country of residence.

Currency exchange is for the purpose of changing the currency of a slot so that another currency may be loaded or changed into the currency of choice. Support of the currency exchange transaction is an issuer's and acquirer's option. However, if multiple currencies are supported, and unload is not supported by the issuer, then currency exchange must be supported by the issuer. (This is to allow the removal of value from a card of a currency which is no longer needed.)

General Requirements

If currency exchange is supported by both the acquirer and the issuer, then:

- The cardholder must be allowed the option of exchanging the currency of a slot for a different currency.
- The cardholder must be allowed to identify which currency he or she will exchange for a different currency.
- Currency exchange may be performed into any currency of the cardholder's choosing that is supported by the issuer and the acquirer.
- Currency exchange may convert the currency of one slot into the currency that already exists in another slot.
- The load device must display the new currency amount in the slot to the cardholder subsequent to the currency exchange, and allow the cardholder the option of loading more electronic value in the slot. A subsequent load transaction is a separate transaction from that of the currency exchange.
- There must not be any slots that contain duplicate currencies.
- Currency exchange transactions must be uniquely identified as such.

Funds

- The source of funds for a currency conversion is that of the funds which already reside in the designated slot.
- The maximum slot balance as defined by the card issuer may not be exceeded when currency conversion is performed.

Currency Conversion

- The currency code of a slot is set at the time of initial load or currency conversion.

- Card issuers must manage and authorize currency exchanges.
- The currency of a slot may be either partially or fully converted to that of a different currency.

Card Issuer/Funds Pool Manager

The card issuer/funds pool manager must:

- Calculate the load amount of the new currency.
- Perform the currency exchange.
- Update the funds pool to reflect any change of electronic value.

Database/Archive

- The electronic purse card issuer must reflect all changes in electronic value on its card databases and funds pool accounting systems (where separate).
- The load acquirer or load operator must keep records by card number of all currency exchanges that take place at its load devices.

Receipts

As with load or unload transactions, currency exchange transactions require the load acquirer to provide consumers with the option of a receipt, as appropriate and subject to local regulations, or as provided as the normal course of business.

IX. Point-of-Sale Requirements

General Requirements

- Consumers must be able to use their cards in a similar manner at any purchase terminal.
- Acceptance of a variety of electronic purse schemes' cards supporting the Common Electronic Purse Specifications must cause only minimal impact to the merchant environment.
- Purchase transactions must not require a PIN, signature or other means of cardholder identification.
- Purchase and purchase reversal, incremental purchase, and cancel last purchase transactions must be processed off-line.

Terminal Requirements

- Terminals must have safe memory (non-volatile or battery-backed).
- Terminals must be EMV compatible.
- Terminals must contain a PSAM, which must support a unique PSAM identifier.
- Terminals must have the ability to know at least the date, time and sufficient information such that they may be identified in case of a problem. The information must be included in the transaction data and written to the card and terminal logs. (Certain merchant segments may be exempt from the time and location requirement.)
- Terminals must allow the cardholder to demonstrate intent to pay. This could be an accept button or some other means of demonstrated acceptance.
- Terminals must support an issuer certificate revocation list to protect an issuer whose private key was compromised.
- Terminals may support the capability to reject a purchase transaction based on an exception list.
- Terminals should process transactions and/or batches for all schemes supporting the Common Electronic Purse Specifications in a similar manner.
- The terminal must support the forwarding of single transactions and may support truncation and/or aggregation if the scheme and its issuers agree.

Terminal Display Requirements

- Purchase terminals should display card balances unless constrained by consumer protection regulation or operational issues.
- Purchase terminals should have the capability to display card balances at the request of the cardholder.

- Purchase terminals should display the purchase or cancel last purchase transaction amount before completing the transaction, and must allow the consumer to confirm or cancel the transaction if desired.
- Purchase terminals should display the new card balance when a transaction is complete unless constrained by consumer protection regulation or operational issues.
- Terminals must be able to recognize when a card is locked and display an appropriate message that advises the cardholder and merchant of that fact.

Split Transactions

Purchase terminals may support transactions that allow the consumer to complete a electronic purse purchase with a combination of payment means such as two or more electronic purse cards, an electronic purse card and cash, or an electronic purse card and a traditional bank card, i.e., debit and credit.

The combination of payment methods will depend upon the specific merchant environment involved. For example, a merchant may accept only electronic purse and cash as a means of payment. Therefore, those payment methods would be the only ones available to the consumer for completing a transaction at that merchant location. In this case, the consumer could only pay with more than one electronic purse card, or with an electronic purse card and cash.

Purchase Reversal Transactions

A purchase transaction may occasionally not be fully completed. One cause might be a communications interruption. Another example is that of a vending machine which accepts an amount for purchase and decrements the purse, but then determines that the requested item is out of stock. The vending machine would use a purchase reversal transaction to restore value to the card. Support of the purchase reversal transaction capability is optional for merchants.

- A purchase reversal transaction is considered to be one and the same transaction with the original purchase transaction that it is reversing.
- A purchase reversal transaction must be accomplished prior to the card being removed from the terminal.
- A purchase reversal transaction must be uniquely identified.

Cancel Last Purchase Transaction

A customer or merchant may notice that the amount of sale was incorrectly keyed after the customer has removed his or her card from the terminal. Or, the customer may wish to return merchandise to the merchant. A cancel last purchase transaction increments the card's balance to accommodate this. A cancel last purchase transaction is separate from the original purchase transaction. Support of cancel last purchase is optional for merchants and issuers. Cancel last purchase transactions may be used only within the limits listed below:

- Cancel last purchase must be performed at the same terminal on which the purchase transaction was performed.
- Cards that support cancel last purchase transactions must allow only the last transaction on the card's log to be reversed.
- No successive cancellations may occur in the same card.
- Cancel last purchase transactions must be for the same amount as the last transaction logged on the card.
- Cancel last purchase transactions may only be performed if the transaction to be canceled is part of the same transaction batch as the original transaction.
- Cancel last purchase transactions must be performed prior to sending purchase transactions in for settlement.
- A cancel last purchase transaction for an incremental purchase must be for the last increment only.
- A transaction which has been aggregated may be canceled.
- Cancel Last Purchase transaction details must not be aggregated.

Incremental Purchase Transactions

Incremental purchase transactions are transactions which occur as a series of very small-value purchases. The purchase amount is based on a predetermined value depending upon the venue. For example, in a telephone venue, the value would likely be based upon time (seconds, minutes). On the Internet, the increment might be based upon pages of a document or the number of times a game is played. Copiers would likely base value upon number of pages copied. Increments may be for different amounts.

- The terminal must send a command to the card that decrements the card balance for the initial increment in advance of the service being performed.
- The terminal must send the command to the card for a subsequent debit when the value of the initial increment has expired, or just before, depending upon the venue.
- The terminal must send the subsequent debit request for funds such that the command may be recognized as different from, but part of, the prior transaction.

- The card must recognize the subsequent debit request for funds command as part of the prior transaction, increment the total amount of the transaction, debit the purse for the incremental amount, and update the log record with the new information.
- The card must keep only a single log record for the entire transaction.
- A purchase reversal transaction for an incremental purchase must be for the last increment only.

Receipts

Purchase and cancel last purchase transactions must not require a receipt from the terminal unless required by local regulations or provided as the normal course of business for the merchant.

Acquirers

Acquirers must support the capability to report transaction activity and settlement advice to the merchant.

X. Public/Open Network Requirements

Background

The explosive growth of the Internet, and the rapid increase in the number of consumers with access to the World Wide Web, has caused interest in the development of Internet electronic commerce. A variety of service providers have introduced payment schemes to support the purchase of goods or services on-line in a virtual merchant environment

Market Drivers

Estimates on the evolution and growth of the electronic commerce marketplace are speculative due to the uncertainty of consumer and merchant adoption of new technologies. However, a base case estimate of the worldwide electronic commerce market in the year 2000 prepared for Visa by The Boston Consulting Group is US $39 billion. This estimate includes both business-to-business and consumer electronic commerce, as well as transactions both over and under US $10.

It is expected that US $2 billion in transactions under US $10 will be "micropayments" which are individual, extremely low-value transactions. Key markets for micropayments include music clips, video games, and publishing.

A significant issue for electronic commerce is consumer privacy and concern over business use of information. Strong consumer interest in electronic commerce is still in its infancy. Merchant interviews show that electronic commerce is in the early stages of development. The deployment of electronic purse in both real and virtual malls will increase consumer demand, drive merchant acceptance, and provide a competitive advantage over other micropayment solutions which are limited to Internet use only.

Strategic Objectives

An electronic purse product with Internet capability provides several benefits for financial institutions, cardholders and merchants.

Financial Institutions

- Expands the functionality of electronic purse.
- Potentially increases revenue opportunities from cardholders and merchants.
- Provides new merchant marketing opportunities for acquirers.
- Offers a micropayment solution for electronic commerce.

- Enables financial institutions' role in a micropayment solution.
- Provides added value to card programs and strengthens customer relationships.
- Leverages the strength of the brand, building awareness and usage of a new technology.
- Acts as a cornerstone application for electronic purse products.

Cardholders

- Enhances the value and convenience of electronic purse cards.
- Enables single card access to both real and virtual merchant environments.
- In combination with other symbols on cards, provides single card payment solutions for both low- and high-value transactions.
- Removes concerns about misuse of account numbers, since value is actually stored on the card itself.

Merchants

- Provides a payment solution for microtransactions, enabling merchants to offer a wider range of digital merchandise.
- Provides a method to recover costs of services and generate incremental profits.
- Leverages the strength of the brand to generate consumer acceptance.
- Provides access to an existing, and rapidly growing, card base.
- Integrates into existing settlement procedures for electronic purse transactions.
- Guarantees payment if the transaction is completed.
- Provides the ability to reach a global consumer market.

General Requirements

Following are key business requirements for developing an Internet-based electronic purse product.

- The Internet and the World Wide Web eliminate domestic borders. Since consumers will have access to merchant home pages around the world and will make purchases in currencies accepted by the merchant, electronic purse on the Internet must have multi-currency capability.
- Electronic purse on the Internet must be supported on single application and multi-application reloadable cards.
- Electronic purse on the Internet must integrate with major browser software and/or operating systems.
- Electronic purse on the Internet must support the following transaction set:
    - Load
    - Unload

    - Currency Exchange
    - Incremental Purchase
    - Purchase/Purchase Reversal
- Cancel last transaction should be analyzed for potential implementation subject to a review of:
    - Security requirements, and
    - The business requirements of the scheme provider, and
    - The business requirements of the card issuer
    - Other
- Electronic purse on the Internet should be targeted to micropayments under $10, but the maximum transaction amount is limited only by the balance on the card.
- Electronic purse on the Internet must have a flexible architecture so that it may be accommodated within or integrated into future standards governing electronic wallets or e-commerce trading protocols.

Security

- Electronic purse on the Internet must provide confidentiality of payment, purchase and other information transmitted across open networks. It must ensure that the consumer is not deceived by the amount of a purchase or by the merchant. A way to achieve this security goal is with the use of a separate display which cannot be influenced by the PC software.
- Loading over the Internet must ensure information confidentiality If a PIN is involved, it must be kept secure. A way of achieving this is through the use of a separate, trusted PIN pad.
- Security features must protect the integrity of transactions over the public/open networks and must not permit the determination of encryption keys or other security data through attack methods over the network.
- System security must provide for authentication of the card and terminal/payment server and authentication of the merchant by the cardholder.

Card Reader Device

- Must provide an interface and message transmission between the card and the cardholder's client device.
- Must be capable of supporting all cards conforming to the Common Electronic Purse Specifications.

Cardholder Client Device

- The cardholder client device must control the interface to the card and select the purse slot that corresponds to the currency code of the purchase.

- The cardholder client device must display the current card balance, amount of purchase and new card balance at completion of the transaction and provide an accept capability.
- The cardholder client device must provide options for doing a balance check (displaying all slots, not just those with value) and display of the card's transaction log.

Merchant Application

- The merchant device(s) must log all transactions.

XI. Transaction Processing Requirements

Purchase, Incremental Purchase, Cancel Last Transaction

General Requirements

- Differences in transaction processing must be as transparent as possible to merchants.
- Acquirers must ensure that a unique terminal identifier and/or PSAM identifier is sent in each transaction.
- Purchase, incremental purchase and cancel last purchase transactions must be processed off-line.
- The value of the initial and subsequent segments of incremental transactions must be aggregated into a total transaction amount such that only a single log record is forwarded for processing.
- The acquirer must ensure that the transactions have been secured using the MAC key.
- The acquirer must ensure that the PSAM contains the MAC key, certifying authority public key, the scheme provider's certificate, and terminal private key.

Transaction Processing

- The system operator which is acquiring transactions from the merchant acquirer must:
  - Provide a function that collects, validates, clears and settles purchases and cancel last purchase transactions.
  - Pass the transactions to the appropriate system operator(s).
  - Receive responses from the system operator(s).
  - Forward the responses back to the merchant acquirer.
- Transaction data must be capable of being routed to the appropriate card issuers for updating of the fund pools. This includes funds pools at the card issuer or correspondent bank and funds pools at a funds pool administrator.
- Transaction detail should be available either on-line or via reporting for a specified period of time (to be determined by each scheme).

Flow

See Appendix A for flows and flow diagrams.

Load Transactions

General Requirements

- Load transactions must be processed on-line and require cardholder authentication for funds requests except when cash is the funds source.
- Load acquirers and card issuers must be able to process load transactions for all cards using the Common Electronic Purse Specifications.
- Load acquirers and card issuers must process the following transactions:
  - Authentication of electronic purse card data and the response.
  - Authorization of funds and the response.
  - Increment card electronic value in any supported currency selected by the cardholder.
  - Settlement of funds and transfer to electronic purse card issuers.

Flow

See Appendix A for flows and flow diagrams.

Unload

General Requirements

- Unload acquirers are not precluded from processing unload transactions of cardholders from another financial institution if there is a bilateral agreement in place, but this is out of the scope of CEPS.
- Unload transactions must be processed on-line.
- Unload acquirers must be able to process unload transactions supported in devices which are operated by the card issuer of the cardholder requesting the unload.
- Unload acquirers must process the following transactions:
  - Authentication of electronic purse card data and the response.
  - Authorization to unload and the response.
  - Decrement card electronic value in the currency selected by the cardholder.
  - Settlement and funds transfer from electronic purse card issuers.

Flow

See Appendix A for flows and flow diagrams

Currency Exchange

- Currency exchange transactions must be processed on-line.
- All currency exchange transactions must be routed to the appropriate card issuer for authentication.
- Load acquirers and card issuers must be able to process currency exchange transactions for all cards using the Common Electronic Purse Specifications if they support the currency exchange capability.

Customer Service

The appropriate system operator(s) may store the data and make transaction information available to the electronic purse card issuer for customer service purposes for a specific period of time (to be determined by the scheme).

Script Messaging

- System operators must be able to pass script messages from the card issuer to the load acquirer.
- Load acquirers must be able to receive script messages.
- Load acquirers must be able to pass script messages to load devices and on to the card application.
- Script messaging must not affect system performance such that the customer's experience at the load device is adversely impacted.

Fault Handling, Exception Processing, Failed Transactions

Fault handling and exception processing capabilities must be robust enough to ensure system integrity and recovery. Potential exception conditions and rules for system and product responses include the following:

- The consumer alleges an incorrect amount was deducted from or incremented to the card.
  The merchant should check the terminal log and, if supported, perform a cancel last purchase transaction.
- Negative completion messages are received from the card.
- A purchase transaction fails one or more edits in the validation cycle.
  If the transaction cannot be settled, it will be rejected, and the acquirer and merchant will be notified in the reconciliation reporting. The notification must include the reason for the reject and must have the ability to re-send the transaction.
- A transaction is lost before reaching the appropriate system.
  At the issuer's discretion, an adjustment to system balances will be made if necessary.

Chargebacks

Purchases

There are no automatic chargebacks supported for purchase transactions which fail validation of the transaction signature. However, each scheme may decide to implement a dispute resolution process to deal with this situation.

Loads/Unloads

Limited chargeback processing must be supported for load/unload transactions in the event of claims of services not rendered or value not received.

Transaction Identification

Transactions must be uniquely identified by the card number, date and time stamp, PSAM number, amount, currency code, transaction counters, BINs, and batch number.

Collection

Time Limits

- Merchant transactions must be collected regularly and in a timely manner.
- Settled and acknowledged transactions must be deleted from the datastore, subject to local laws and regulations.

XII. Settlement and Reconciliation Responsibilities

Settlement and reconciliation requirements include the capability to pass, settle and reconcile transactions between system operators.

System(s) Operator(s)

The Common Electronic Purse Specifications for settlement and reconciliation require support of a distributed, portable processing capability. This allows there to be one or more than one system operator within a given country or territory. System operators may be as small as a single financial institution and/or as large as a single system operator running the system for all the participants in several countries.

A system operator can play several roles for electronic purse card issuers and merchant acquirers. Depending on the products supported, and the relationships, a system operator can support everything from card ordering and personalization, to terminal management and purchase settlement. There can be many options and arrangements.

- If acting as a load/unload/currency exchange acquirer's or electronic purse card issuer's processor/agent, the system operator must forward all load/unload transactions to and from the appropriate networks or financial institution for authorization, authentication, settlement, currency change requests and transfer to the appropriate funds pool.
- A system operator must provide detailed reconciliation reporting to its members.
- A system operator must provide settlement to its members if acting as a settlement entity. Settlement of purchase transactions may be based on transaction detail as well as batch headers, so purchase settlement must include reporting to acquirers at the transaction level.

Purchase Transactions

Merchant

The merchant must reconcile settlement from the acquirer and contact the acquirer's merchant service center with any questions.

Merchant Acquirer

- Merchant acquirers must collect and forward all transactions within a given time period.
- Merchant acquirers must pass the merchant transactions to the appropriate system(s) operator and settle with the merchant.

- Merchant acquirers must receive settlement for purchase transactions, net of fees, which have occurred at their merchant sites.
- Merchant acquirers should be able to settle all electronic purse card transactions supporting the Common Electronic Purse Specifications in a similar manner.

Load Transactions

Load Acquirers/Operators

- The load acquirer must initiate and switch settlement transactions to the appropriate network or financial institution after receiving the settlement advice.
- Load acquirers should be able to settle all electronic purse card transactions in a similar manner.
- Load acquirers must settle all load transactions which have been completed at their load devices according to the scheme rules for the funding source.
- Load acquirers must keep a log of all load transactions switched through their systems, regardless of completion status.
- Load acquirers must ensure that their system balances on a regular basis, typically daily or more often.

Unload Acquirers/Operators - Linked Accounts

- Unload acquirers must be able to pass unload transactions to the host processing system of their financial institution, receive authorization messages and unload the cardholder's card.
- Unload acquirers must keep a log of all unload transactions regardless of completion status.
- Unload acquirers must ensure that their system balances on a regular basis, typically daily or more often.

Electronic Purse Card Issuer

- The electronic purse card issuer must be able to receive settlement from various system operators and processors.
- The electronic purse card issuer must be capable of receiving liability and activity reports for funds pools that it manages.

Funds Issuer

- The funds issuer must settle all load/unload transactions which have been authorized by their network.
- Settlement must include any appropriate interchange fees according to the scheme rules for the funding source.

- Funds issuers must ensure that their system balances on a regular basis, typically daily or more often.
- Funds issuers must authorize or decline all funds requests switched to them on their funds accounts.
- Funds issuers must not discriminate against funds requests from any particular load acquirer, nor for any particular currency except as required by law or regulation.

Funds Pools

The Common Electronic Purse Specifications will enable issuers to manage their own funds pools or delegate funds pool management to a third party, such as a correspondent bank or a funds pool administrator.

Issuer-Managed Funds Pools

- The card issuer must hold the liability for the funds.
- Unredeemed funds are the property of the card issuer.
- For purchase, cancel last purchase transactions and load/unload transactions, the electronic purse card issuer must reconcile with its system operator.
- Issuers who support multiple currencies may hold the funds pool in the currency in which the liability occurs, or in another currency of it choosing.
- In a distributed processing environment, system operators must reconcile with each other.
- Reconciliation between the funds pools must be automated and run daily.
- System operator(s) must support reconciliation-related inquiries from other system operators.

Third-Party Managed Funds Pools

- The third-party funds pool administrator must receive settlement for deposits of load transactions, and make payments for purchase transactions.
- The card issuer must hold the liability for the funds.
- For purchase, currency exchange and load/unload transactions, the electronic purse card issuer must reconcile with the third-party funds pool administrator.
- Reconciliation of the funds pools must be automated and run daily.
- Funds pool administrators must support reconciliation-related inquiries from other system operators.

XIII. Clearing and Administration

The Common Electronic Purse Specifications require support of a distributed, portable system for clearing and administration. This allows there to be one or more than one system operator within a given country or territory. System operators may be as small as a single financial institution and/or as large as a single system operator or processor running the system for all the participants in several countries. Clearing and administration requirements must include the capability to process electronic purse card purchases, incremental purchase transactions, cancel last purchase transactions, load and unload transactions, and currency exchange transactions, and to interface with other systems.

Data

- The clearing and administration system(s) must maintain a datastore for BINs, transaction detail, settlement options and keys.
- The clearing and administration system(s) must support purchase, load, unload, incremental purchase, cancel last purchase transactions and currency exchange transactions.

Transaction Collection and Posting

Collection

A specification must be published for how system operators must interface with each other for data collection and transmission.

- A cycle must be run regularly to collect, process and report product activity.
- The system must be able to process files of “on us” and “not on us” transactions and transmit the not on us transactions to the appropriate processor.

Validation and Update

The following functions are required:

Transaction Exceptions

- Transactions with errors will be reported back to acquirers, as appropriate.
- Errors will result from an unroutable BIN, an invalid MAC or if the transaction is found to be a duplicate.
- Transactions with errors will be recorded as not settled, and sent to the system operator/acquirer in the reconciliation report.

Transaction Validation

- The validations performed on transactions will depend on the record format defined in the design phase, but will include at a minimum:
  1. Duplicate transaction.
  2. MAC error.
  3. Invalid BIN.
  4. Date and numeric edits.

- The MAC used to validate transactions will not be the same for all issuers.

Load Advice

- Systems must process load/unload advices in the same manner as the other domestic products, such as debit and credit.

Currency Exchange

- Systems must be able to process currency exchange transactions through to the card issuer.
- Currency exchange transactions must be defined for settlement purposes.

Settlement

- New codes must be defined for electronic purse card settlement to replace those currently used.
- Purchases must be settled such that the funds are settled to the electronic purse issuer or third party funds pool administrator. The system must determine the appropriate funds pool end point.
- Purchase settlement/reporting must be supported for both single and dual message formats.
- The system must support settlement of transaction fees and charges.

Reconciliation

- An automated process must be provided to balance a daily database extract to a daily file.
- Report records must be generated with a unique electronic purse transaction identifier.
- An option for reporting and/or a raw data file containing the settlement status of each transaction must be provided to the acquirer.

Security and Key Management

Business Resumption Plan

The system must have a business resumption plan (BRP) so that critical processing of transactions can be resumed after a problem or disaster. This ensures reliable ongoing operation of the product. A BRP should include:

- Recovery of data.
- Re-processing of transactions.
- Re-routing of network data, as necessary.

Transaction Authentication

The product requires use of symmetric message authentication code (MAC) keys for transaction authentication.

Batch Security

Payment on detailed transactions or on batch header in case of exception conditions that result in transaction detail loss is a scheme and issuer decision.

Card Management

- All liability and activity reporting will be sent to the card issuer and/or appropriate third party funds pool administrator.
- As purchase, load, unload, and cancel last purchase transactions are processed, the system must store and report on card activity as needed.
- Functions such as card ordering, activation and status change must be supported.
- Optional card activity reporting must be offered to all card issuers for global card usage and program success evaluation.

Reporting

The following system participants will require reports of various types and at varying times:

- Merchants
- Merchant acquirers
- Issuers
- Funds pool administrators
- Risk managers
- System Operators
- Scheme Providers

XIV. Appendices

The following appendices are attached:

A. Flow Diagrams and Explanations
Purchase, load, currency exchange and unload transaction flows.

B. Glossary
The Glossary is attached to assist the reader in understanding the terms used in this document and in the smart card industry.

A. Flow Diagrams and Explanations

The flows that are depicted are based on logical transaction processing. The actual flows will be developed in the design phase of the product development process, and may bring modifications reflecting practical system design and messaging. Sequences depicted here may be altered during the design phase. There is no attempt to represent the flow of possible fees to any of the participants. Part of the processing of transactions may be delegated to other entities.

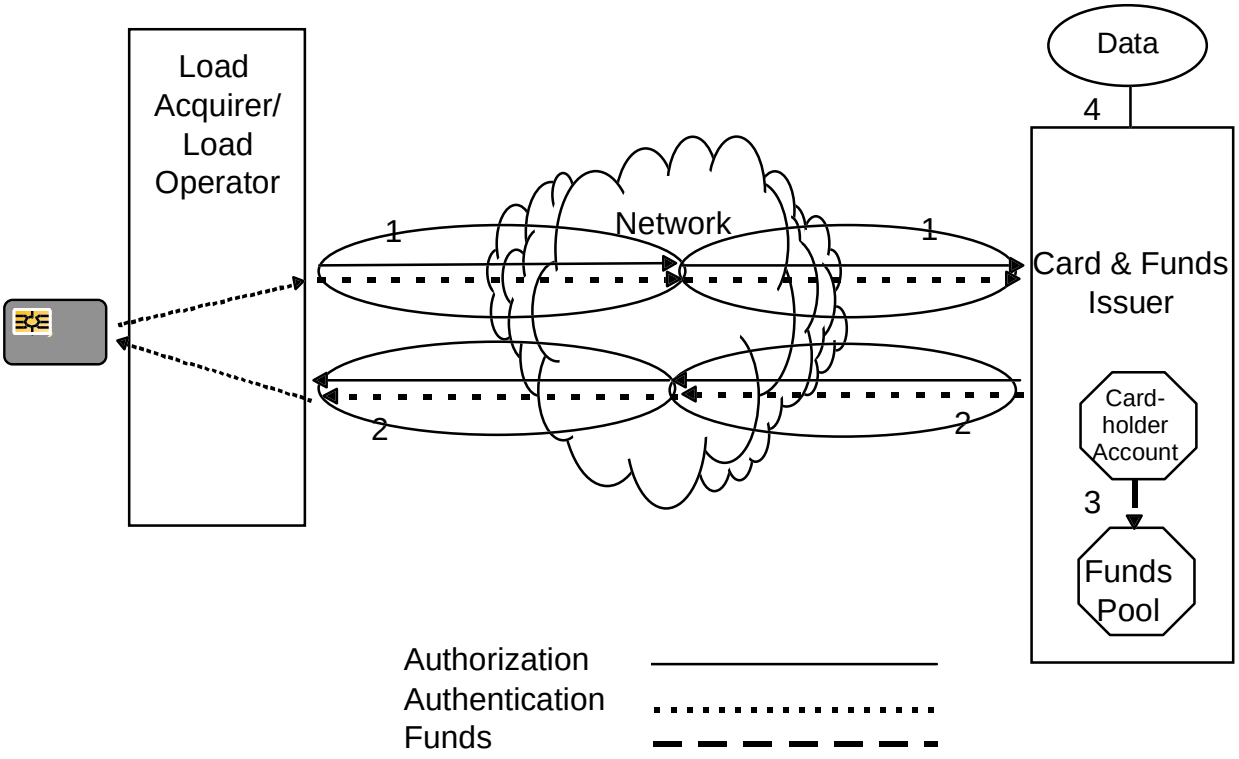
Generic Load Transaction Flow #1 - Linked Load

Scenario:

- The electronic purse card is linked to a specific funding account (cardholder account) from which it is loaded.

1. The Load Acquirer sends a combined authorization and authentication request to the Card and Funds Issuer via the Network.
2. The Card and Funds Issuer sends the positive combined authorization and authentication message to the Load Acquirer via the Network.
   The electronic purse card is loaded.
3. The Card and Funds Issuer debits the cardholder account and increments the funds pool of the currency loaded.
4. The Card and Funds Issuer updates the card data base.

Generic Load Transaction Flow #1



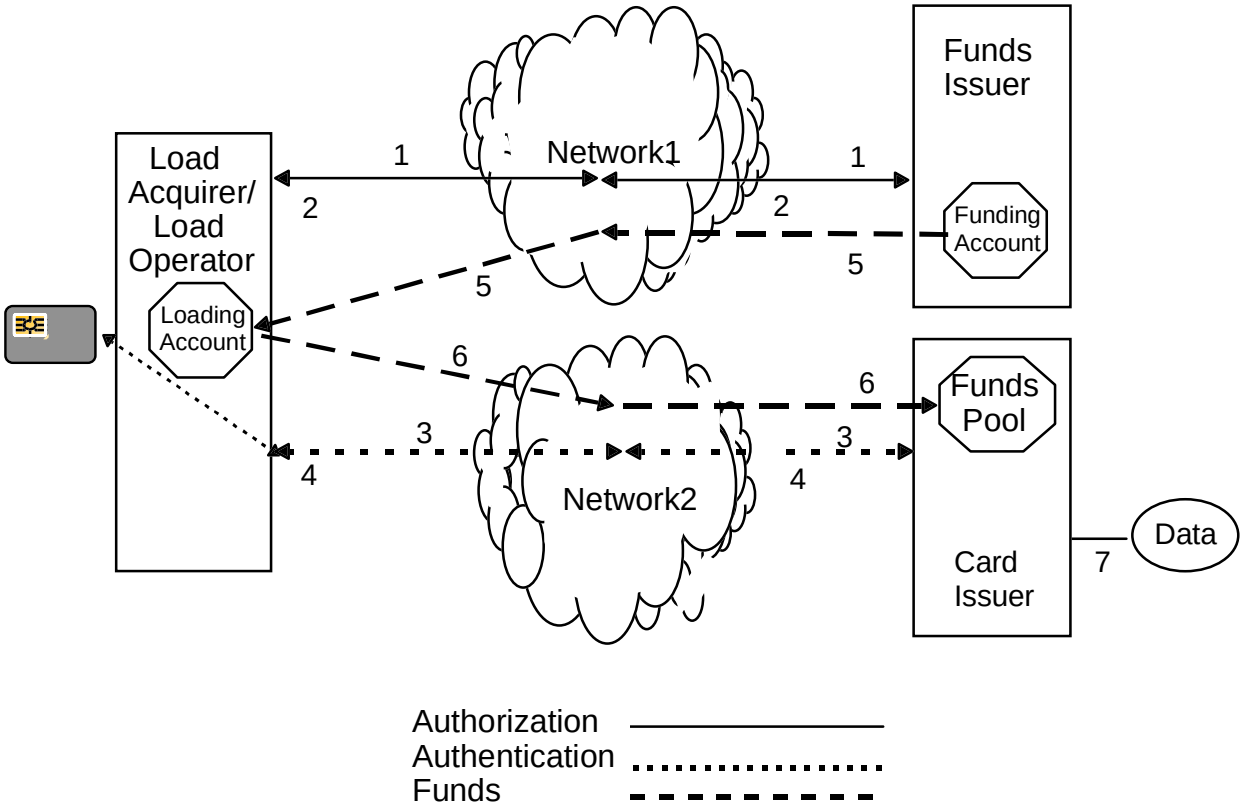
Generic Load Transaction Flow #2 - Unlinked Load

Scenario:

- The electronic purse card is not linked to the funding account.

1. The Load Acquirer sends an authorization request to the Funds Issuer via Network1.
2. The Funds Issuer sends the positive authorization response to the Load Acquirer via Network1.
3. The Load Acquirer sends an authentication request to the Card Issuer via Network2. This request is also a guarantee that the Load Acquirer will credit the Card Issuer.
4. The Card Issuer sends the positive authentication response to the Load Acquirer via Network2.
   The electronic purse card is loaded.
5. The Load Acquirer debits the Funds Issuer via Network1 and credits his loading account in the currency loaded.
6. The Card Issuer debits the Load Acquirer via Network2 and increments his funds pool in the currency loaded.
7. The Card Issuer updates the card data base.

Generic Load Transaction Flow #2



Generic Unload Transaction Flow

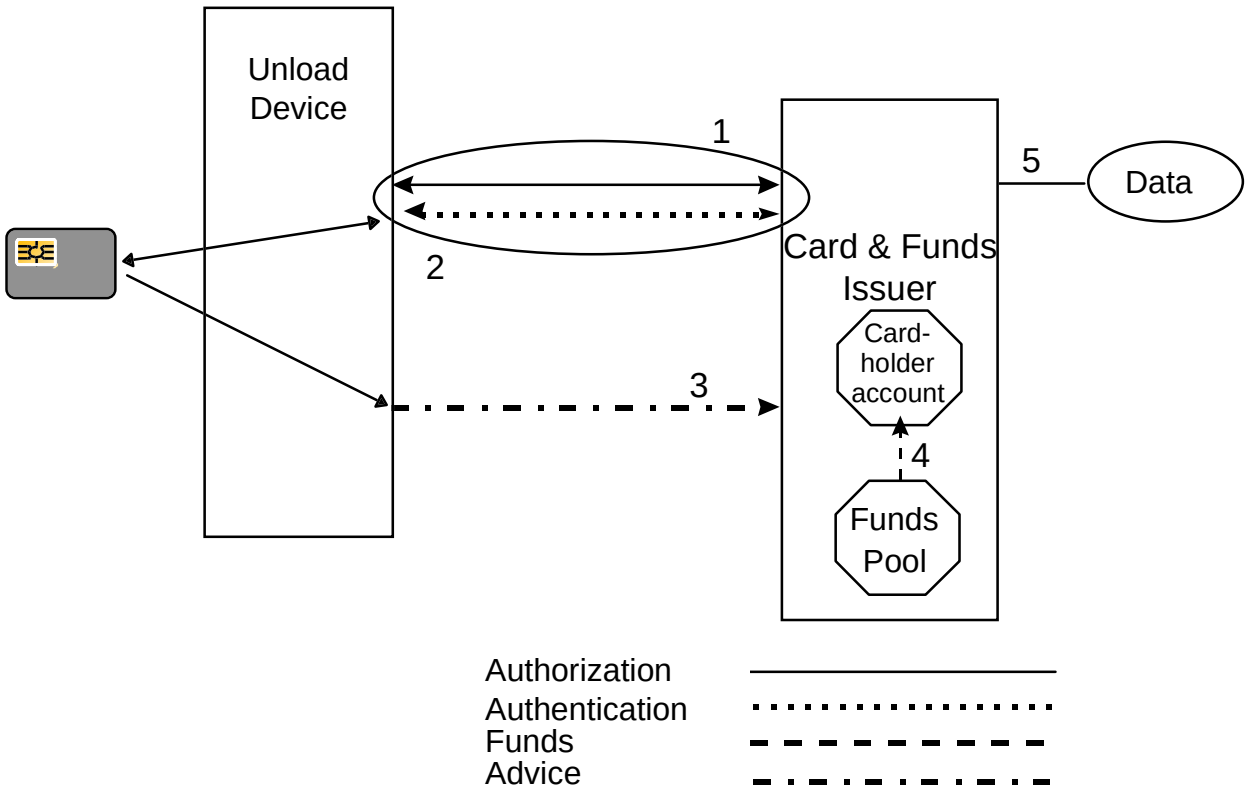
Scenario:

- The electronic purse card is linked to a specific funding account (cardholder account).

1. The unload device sends a combined authorization and authentication request to the Card and Funds Issuer.
2. The Card and Funds Issuer sends the positive authorization and authentication response to the unload device.

   The electronic purse card is unloaded.
3. The unload device sends the unload advice to the Card and Funds Issuer.
4. The Card and Funds Issuer decrements the funds pool of the currency unloaded and credits the cardholder account.
5. The Card and Funds Issuer updates the card data base.

Generic Unload Transaction Flow



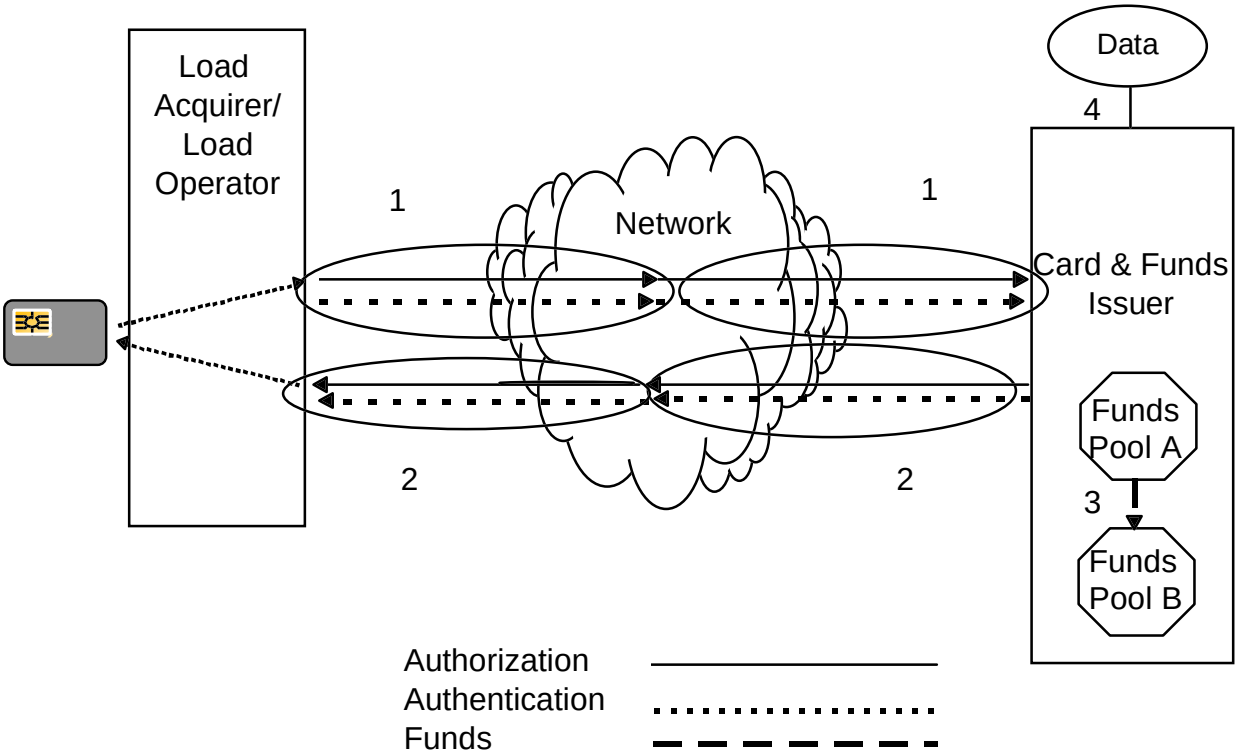
Generic Currency Exchange Flow

Scenario:

- Currency exchange from Currency A to currency B is performed by the Card Issuer. The funding source for the currency exchange is the funds already in a funds pool in currency A. Therefore, the Card Issuer is also the Funds Issuer.
- A slot may be emptied and reloaded with a new currency; or a slot may be partially emptied and electronic value loaded to a different slot which holds the currency of choice.

1. The Load Acquirer sends a combined authorization and authentication request including the amount of currency A to the Card and Funds Issuer via the Network.
2. The Card and Funds Issuer sends the positive combined authorization and authentication message including the amount in currency B to the Load Acquirer via the Network.
   The currency exchange is performed.
3. The Card and Funds Issuer debits the funds pool of currency A and increments the funds pool of currency B.
4. The Card and Funds Issuer updates the card data base.

Generic Currency Exchange Transaction Flow

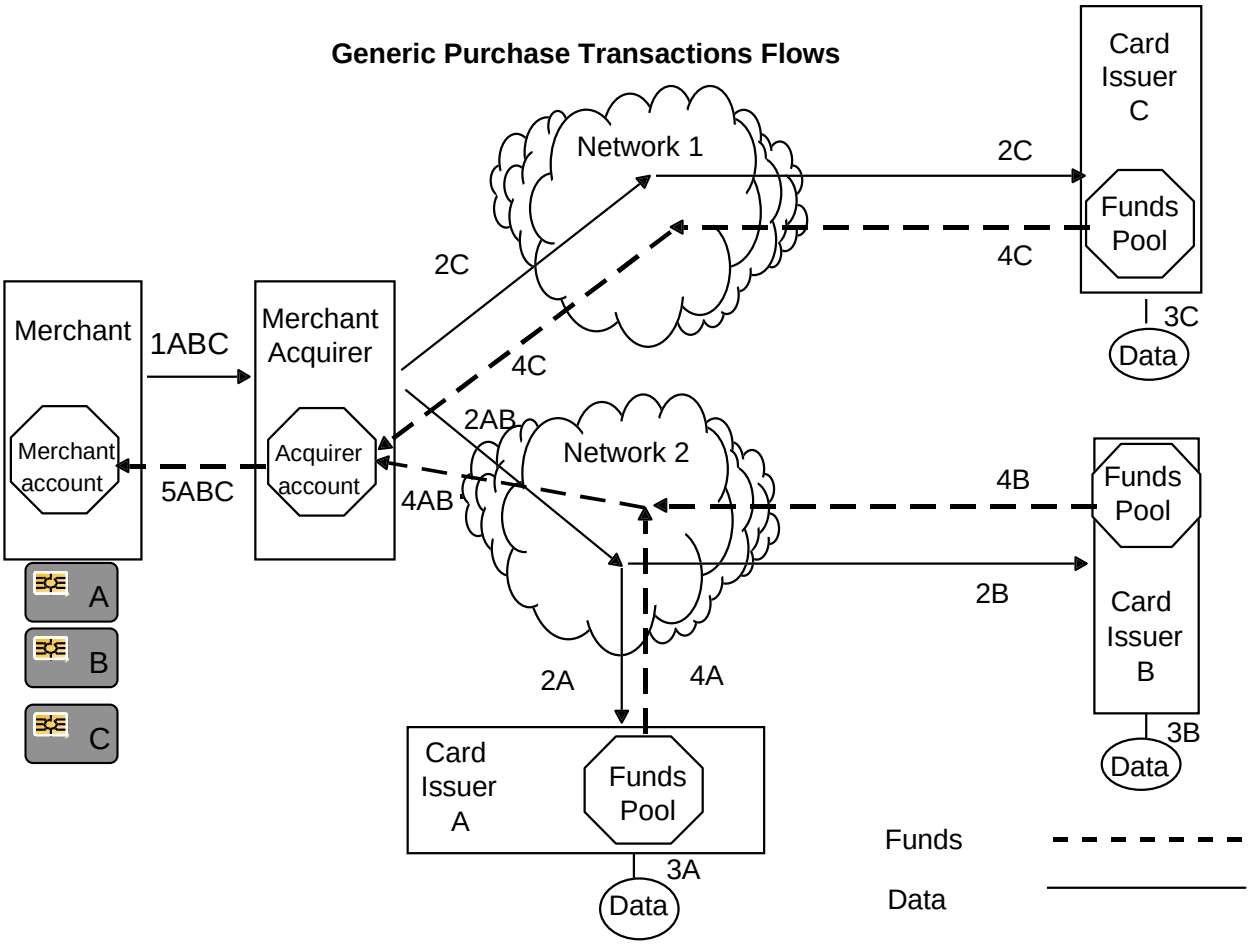


Generic Purchase Transaction Flows

Scenario:

- Transactions have occurred and been authenticated off-line.

1. The Merchant sends the transactions to the Merchant Acquirer.
2. The Merchant Acquirer sends the transactions to the Card Issuers via the respective Networks.
3. The Card Issuers update their card data bases.
4. The Card Issuers' funds pools of the transaction currency are decremented and the Merchant Acquirer's account is credited via the respective Networks.
5. The Merchant's account is credited and the Merchant Acquirer's account is debited.


Generic Purchase Transactions Flows
Card Issuer C
Network 1
2C
Funds Pool
4C
3C
Data
2C
Merchant
1ABC
Merchant Acquirer
4C
2AB
Merchant account
Acquirer account
5ABC
4AB
Network 2
4B
Funds Pool
2B
Card Issuer B
3B
Data
A
B
C
2A
4A
Card Issuer A
Funds Pool
3A
Data
Funds
Data

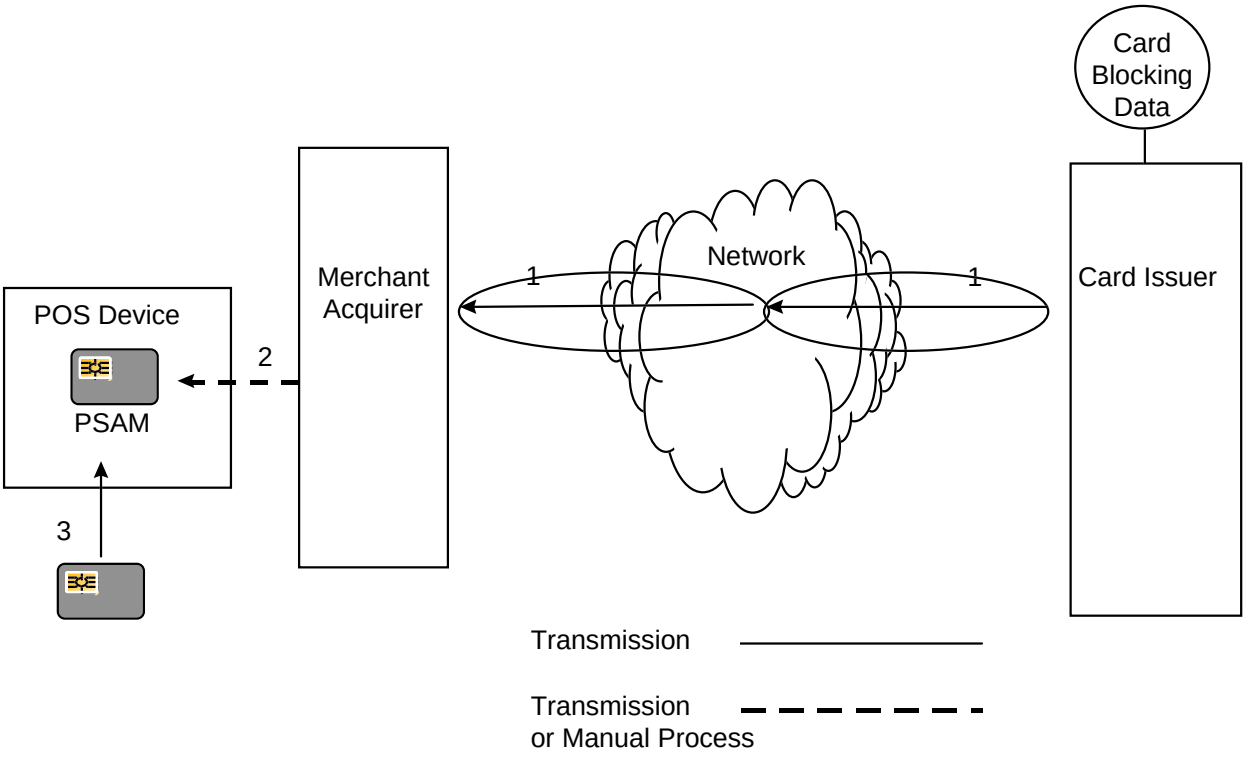
Generic Flow for Exception List Processing

Scenario:

- CEP cards are to be added to the scheme's card exception list.

1. After discussion with scheme issuers, the scheme provider adds a range of CEP cards to its list of cards and sends the exception list to all merchant acquirers for the scheme.
2. Merchant acquirers send all listed ranges to the POS devices. Storage may be in the POS device or in the PSAM.
3. A CEP card included in the listed range is inserted into the POS device and is rejected.

Generic Exception List Processing Flow



B. Glossary

A.

Access Control: Controlled access to premises, equipment (computers), services (toll roads, etc.).

Accountability: The ability to trace an electronic purse transaction from the point of origin to the issuer or issuer's agent for all transactions that change the balance of the electronic purse.

Activation: A secure procedure used to switch an electronic purse or a PSAM to its active life state for normal operation.

Aggregation: The total amount, consisting of the sum of all transactions in a given batch, provided to the issuer. No detail of the individual transactions that make up the total is provided, nor is it recoverable.

American National Standards Institute (ANSI): An American Standards organization. Standards are available from the ANSI Publication Sales Office, 1430 Broadway, New York, NY 10018 USA.

Anonymity: The condition which precludes the ability to be identified. Cash transactions are considered anonymous. Some electronic purse transactions, such as purchases made with disposable cards can be anonymous. Reloadable card transactions that use a funding source other than currency do not guarantee anonymity upon load/unload. However, anonymity of payment is still guaranteed at the point of sale.

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, stored value, loyalty, etc.

Application Specific Integrated Circuit (ASIC): A computer chip designed with special features to satisfy particular requirements. In the smart card context, an ASIC generally refers to chips with special "cells" for functions such as security (exponentiation used in public key) or communications (radio frequency). This is often used in contactless IC transit applications.

Asymmetric Key Cryptography: See Public Key Cryptography and Encryption.

Asynchronous Password Generation: A method of generating a unique one-time password for a computer user based on a challenge-response sequence between a host and a device possessed by the user. The device, generally referred to as a smart card or token, contains a secret ID or seed number, a cryptographic algorithm, and some method for the challenge issued by the host to be entered. This may be contacts on a traditional smart card or a keypad. When the user signs onto a system, the host issues a challenge in the form of a pseudo-random number. The user enters the number into the device, and a response is displayed on an LCD. This response is typed into the terminal by the user. The host computer, which knows the user's seed and the algorithm, compares the response to what it expects in order to authenticate the presence of the device. The method can be strengthened by requiring the user to enter a PIN.

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. Additionally it is an umbrella term for several risk management processes that can be performed during chip card transactions. See Static Data Authentication and Dynamic Data Authentication.

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.

Balance Reader: An off-line device that reads the balance of the slot(s) in an electronic purse. It may, optionally, provide other functionality.

Biometrics: A method of using a permanent human attribute for identification purposes. Examples include fingerprints, voiceprints, eye retina patterns, hand geometry and DNA.

C.

Cancel Last Purchase Transaction: The action that increments the balance on an electronic purse card. It is used to correct an amount which was keyed incorrectly at the time of purchase, or to reimburse a customer for the amount of a purchased item which the customer subsequently returned.

Card Acceptance Device (CAD): The mechanism, a key component of reader/writers, into which an integrated circuit card is inserted.

Card Authentication Method (CAM): A cryptographic means of validating a card's legitimacy.

Card Dispensing Machine (CDM): A machine that holds an inventory of electronic purse cards and dispenses them to consumers when appropriate payment is made.

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 Verification Value (CVV): A form of Card Authentication Method (CAM).

Cardholder Client Device: A device with intelligence, such as a personal computer. It is used as the interface between an Internet merchant's management computer (server) and the card reader attached to the cardholder's personal computer. The cardholder's client device provides access to the Internet and, through the Internet, to the merchant's merchandise offerings. The cardholder's client device provides access to various payment methods, including credit, debit and electronic purse.

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.
- 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.

Cash Card: A financial or other (e.g., telephone) payment card that has value stored on the chip; with each payment transaction the balance is reduced by the value of the transaction.

Certificate: Message authentication code for symmetric and signature for asymmetric cryptographic algorithms.

Certification Authority: An entity entrusted by one or more entities to create and assign certificates.

Challenge-Response: See Synchronous Password Generation.

Chargeback: The return initiated by a Card Issuer of all or a portion of a disputed transaction settled through a network.

Chip Card: A financial or other (e.g., identification) card that is embedded with an integrated circuit.

Chip-Reading Device/Terminal: A point-of-sale terminal, ATM, or other device capable of processing chip card-initiated commands.

Closed System: An electronic purse card system that includes a single issuer who is also the only participating merchant (e.g., telephone); or a single issuer and multiple service providers (e.g., university).

Collection: The process of transferring transaction data from point-of-sale terminals to the system operator by way of acquirers.

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.

Contact Technology: Technology which allows for the interchange of data between the card and the read/write device only when the integrated circuit on the card makes surface contact with the read/write device.

Contactless Technology: As the name implies, contactless integrated circuit cards contain no surface contacts and employ either RFID techniques (see Radio-Frequency ID), which incorporate an antennae in the card, or inductive techniques, where metallic plates inside the card are used to receive power and transmit data.

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.

Deactivation: A secure procedure, under control of the system operator, in which an electronic purse card or a PSAM is switched from its active life state to a permanently disabled state. Only reading of certain data is possible in the deactivated state.

Digital Signature: This is used to prevent 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 cryptographic algorithm and information that identifies the user, including a cryptographic key. The digital signature can be generated using either symmetric key cryptography or public key cryptography. In the public key version, the user signs the message using a secret key stored in a smart card or terminal hardware or software. The receiver employs the public key of the sender to authenticate their identity.

Digital Signature Algorithm (DSA): An algorithm used expressly for authentication. It cannot be used for encryption.

Digital Signature Standard (DSS): A standard for generating a non-reputable electronic code linking the user to a specific transaction. The standard specifies a government developed algorithm called the Digital Signature Algorithm (DSA), specifically designed to be easily implemented in smart cards without the need for special math co-processors. DSS also uses the Secure Hash Algorithm (SHA) for reducing message data to produce the digital signature.

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

Disruption Attack: An attempt to reduce the balance of a component without crediting the associated balance of another component.

Domestic Electronic Purse Card Issuer: The financial institution which issues the electronic purse card to the cardholder. It also authenticates load requests, provides its message authentication keys (MAC) to the international authentication and storage entity for transaction record authentication, and provides cardholder customer service.

Domestic Funds Pool Administrator: The financial institution which acts on behalf of an issuer and maintains liability for international purchase transactions, pays purchase settlements, receives funds from loads, reconciles with the international system operator, and invests the funds in the funds pool.

Dynamic Data Authentication (DDA): A process where the card is presented with a challenge which then generates a response using its secret key which is authenticated by the terminal or host computer. Dynamic Data Authentication (DDA) provides card authentication to protect against counterfeiting in an off-line environment. DDA provides security protection equivalent to Card Authentication Method (CAM) and Card Verification Value (CVV). DDA uses a unique signature containing dynamic application data from the transaction. This unique signature is created and encrypted using a secret key in the card. Since the secret key cannot be retrieved from the card, the card cannot be counterfeited. DDA using public key requires a crypto-engine in the card to create dynamic signatures which are verified by the terminal. DDA supports electronic commerce and electronic banking requirements for additional security and portability by storing certificates and keys and encryption algorithms on the chip card.

E.

EEPROM: Electronically Erasable Programmable Read-Only Memory is a non-volatile memory technology where data can be erased and rewritten. EEPROM is widely used in smart cards, usually in 1Kbyte to 8Kbyte quantities.

Electronic Purse: An electronic purse (also referred to as a stored value application) uses an integrated circuit or magnetic stripe 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 Purse Card Issuer: See Card Issuer.

Electronic Purse Payment Transaction: A retail purchase of goods or services; a point of sale transaction. This is an off-line transaction.

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.

Electronic Wallet: Software deployed by Internet merchants on their Web pages which provide the mechanisms for payment to the consumer.

Embedder: The organization that inserts IC assemblies into plastic cards and may also provide personalization services.

EMV Specifications: Technical specifications 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.

Encryption: The transformation of data into a form unreadable by anyone without a secret decryption key.

EPROM: Electronically Programmable Read-Only Memory is a non-volatile storage circuit that can be written to once. This memory can only be erased using ultraviolet light, which is not feasible for chips packaged in plastic. EPROM is widely used in smart cards, usually in 256-bit to 32K-byte quantities.

Error Recovery: A group of transactions used for correcting certain errors observed during processing of normal transactions.

F.

FRAM: Ferroelectric Random Access Memory contains a thin layer of ceramic material covering a traditional circuit to provide durable non-volatile memory. The technology, fairly new to the commercial market, is used in some chip and RFID cards.

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 and authorizes the disbursement of funds to be loaded to a reloadable electronic purse card in the event of an unlinked load.

G.

GSM: Global System Mobile is a communications standard for portable phones that employ smart cards for identification and security.

H.

Hybrid Contact/Contactless Card: A combination of a surface pad for contact applications and a dual/RF capability for contactless applications both, of which are connected to the same chip.

I.

Initialization: The process, executed by card suppliers, that sets data fields on the card.

Integrated Circuit Card (IC): A card that contains an integrated circuit and includes both memory-only and smart cards.

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.

Intelligent Card: A memory card with a processor.

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 which clear and settle transactions performed by cardholders and merchants, regardless of the card issuer, acquirer and/or system operator.

Issuer Revocation List: A list similar to a "hot card" list which identifies issuer public key certificates that are no longer valid. This allows an issuer to block certain cards, where the issuer private key been compromised, for use at purchase terminals.

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 can 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 Purse: An electronic purse application on a customer's card which is referenced to a specific funding account or financial institution.

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 cardholder's 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 Machine: See Load Device.

Load Value Transaction: Consumer initiated transaction that adds value to electronic purse cards at load devices.

Loyalty Program: A program that rewards customers for incremental card and/or product usage. Examples include airline frequent flier programs, rental card programs, frequent shopper programs and video store frequent renter programs.

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.

Memory Integrated Circuit Card (also Memory Card): A card that contains an integrated circuit chip (OTP ROM, Mask ROM, DRAM, FRAM, EPROM or EEPROM) capable of storing data. Memory cards sometimes require an on-board battery to maintain stored data. EPROM memory card has a chip that contains information that can be written into it only once. This type of card is generally used for consumer access to employee buildings, libraries, clubs, etc.; or, in the case of an electronic purse card, a value is stored on the card and used until the value is depleted, at which time the card is thrown away (disposable). EEPROM memory card has a chip that contains information that can be written and read many times.

Merchant: The organization delivering goods and/or services to the cardholder.

Merchant Acquirer: An organization which collects and possibly aggregates transactions from several purchase devices for delivery to one or more system operators.

Merchant Card: See Purchase Secure Application Module

Merchant Server: The computer which allows an Internet merchant to set up his or her merchandising layout ("storefront"), interface to merchant terminals, concentrators and terminals for data storage and collection, and perform other functions necessary to the processing of Internet transactions from the merchant site.

Message Authentication Code (MAC): A digital code generated using a cryptographic algorithm, which establishes that the contents of a message have not been changed. A MAC is generated by taking all or part of a message, such as the transaction amount and account number, and processing it through the algorithm, usually DES. 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.

Microcomputer Integrated Circuit Card: A memory card with a microprocessor and an operating system for security also referred to as a smart card.

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 with sufficient memory to support more than one application, e.g., electronic purse, debit, credit, loyalty.

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.

Negative File: A file designed to support card numbers and/or ranges of identifiers for cards that are not allowed to perform transactions.

Netting: The process of calculating the net settlement value that needs to be allocated to the issuers, acquirers and system operators.

Non-repudiation: Providing cryptographic proof that neither the originator nor the receiver can repudiate having sent/received a given message with its original contents.

Non-volatile Memory: The memory of an integrated circuit which is stable, non-erratic, non-variable and which retains its content when power is removed. This is usually accomplished through use of a battery back-up which provides an uninterrupted power source if the electric power supply is compromised or transitory.

O.

Off-line Authentication: Off-line is defined as a "Go/No Go" situation resulting from the card being recognized as legitimate by the reader or a terminal. In some cases the off-line reader or terminal may contain a downloaded file for checking eligibility of the cardholder.

Off-line Authorization: Chip technology makes it possible to authorize a transaction off-line, in a dialogue directly between the chip card and terminal. Off-line authorizations can reduce fraud and lower costs in markets where expensive or unreliable telecommunications make on-line authorizations costly or difficult. In addition, chips allow issuers to set policies on when off-line authorizations are acceptable or when on-line authorizations are required (see On-line Issuer Authorization).

Off-line PIN Verification: Cardholder verification whereby the chip card itself compares the PIN entered by the cardholder to the PIN securely stored on the chip by the issuer. If the two match, the card tells the terminal to proceed with the transaction. Off-line PIN verification enhances transaction security and can lower authorization costs.

Off-line Transaction: A transaction that does not require real-time connection to a card issuer.

On-line Issuer Authorization: The process whereby a sales transaction or cash advance for a specified amount is approved or declined on-line by the issuer or the issuer's designated processor.

On-line Transaction: A transaction that requires a 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.

Open System: A systems environment that has a common set of operating rules which permits the scheme to support multiple issuers, multiple acquirers and multiple merchants.

Optical Memory Cards: Also known as laser cards, because a low-intensity laser is used to burn holes of several microns in diameter into a reflective material, exposing a substrata of lower reflectivity. The presence, or absence, of a burned hole represents bits. Storage capacity of the cards is generally greater than two (2) megabytes.

P.

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).

Portable: Capable of being moved, transferred or migrated to another site. An example of portable refers to the capability of a back office system to be able to be deployed in several different locations.

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 can be made public. In the case of a digital signature scheme, the public key defines that verification function.

Public Key Certificate: Also known as digital signature. This allows the recipient to authenticate the message based on the sender's public key.

Public Key Cryptography and Encryption (PKE): An asymmetric cryptographic method using two different mathematically related keys for encryption and decryption. One key remains secret and is maintained by the user in a terminal or smart card. The other key, since it cannot be used to derive the secret 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 secret key can decrypt the message. Because of the sophisticated and extensive mathematics that allow this cipher system to work, public key 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 his own private key on part of the message, including identification information. Anyone receiving the message can authenticate the sender's identity by decrypting the digital signature using the sender's public key; message also may be scrambled to ensure the secrecy of the message contents. Also popular is the use of PKE techniques 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 an 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 security application module installed in connection with a point of sale device, within a hardware security module, providing the necessary security for purchase-related transactions and the collection process.

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.

Radio-Frequency ID: A class of methods for transmitting information from a card without physical contact between card and reader. A variety of techniques are used to accomplish this contactless, or proximity, reading and writing. There are two major RF ID approaches for cards containing integrated circuit chips. Active RF techniques require an on-board battery to power transmission, and passive techniques induce their power for radio fields generated by the reader/writer. There are three basic classes of RF technology: high, medium and low frequency. Each of these has unique performance and cost characteristics for both cards and reader/writers.

Random Access Memory (RAM): Random access memory is a volatile memory device that requires power to maintain data. In smart cards, RAM is an interim storage mechanism for registers and other by-products for processing functions. It is used only while the card is receiving power from a reader/writer. In memory-only cards that contain RAM, batteries in the card provide power to maintain data. Memory cards in general do not include RAM.

Read After Write: A data integrity check. Data is immediately read after it is written and compared to the file or tape record that drives the encoder.

Reader: A device that can read the encoding on a card or badge.

Read-Only Memory (ROM): Read-only memory is a non-volatile memory which is written once, usually during IC production. It is used to store operating systems and algorithms employed by the microprocessor in a smart card during transactions.

Read/Write: The capability to encode/re-encode data on integrated circuits.

Reader/Writer: A device that can encode (write) and read the encoding on a card or badge.

Reconciliation: The process of validating that appropriate credits and debits are processed for load and unload transactions. An audit process which ensures that data residing on more than one database is in balance.

Redemption: The process of returning the remaining value on an electronic purse card to the cardholder for reasons such as defective card, expired card, etc.

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.

Replay: To obtain messages from a real electronic purse card transaction and try to replay it later in order to duplicate a transaction.

Repudiate: The act of rejecting, renouncing or disclaiming a transaction which was previously accepted.

S.

Scheme: An electronic purse card system including the card and terminal application, central system, and security.

Scheme Provider: An 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.

Secure Hash Algorithm (SHA): A government developed algorithm that is used in Digital Signature Standard (DSS) to reduce the message data required to produce the digital signature.

Security Architecture: The utilization of detailed security mechanisms, including cryptographic algorithms and the key management necessary to implement security requirements.

Session Key: A temporary cryptography key computed in volatile memory and not valid after a session is ended.

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.

Shared Network: An ATM network that allows multiple financial institution access.

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 carrier 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.

Static Data Authentication (SDA): A methodology through which it can be determined whether data has been altered. Static Data Authentication (SDA) provides off-line data authentication to detect data alteration but not skimming. SDA is equivalent to Card Verification Value. SDA uses fixed certificates (a fixed set of data elements) that cannot be counterfeited but can be skimmed.

Subscriber Identity Module (SIM): A SIM is used to link a phone number to a specific person, instead of linking the number to a specific phone set. Smart cards, which can be inserted into any reader-equipped phone, are used to carry the customer's number. A pan-European standard has been established for SIMs, and several experimental programs are scheduled in the U.S. for personal communications networks (PCNs) using the technology.

Super Smart Card: The term given to cards that have on-board keypads, LCDs and batteries, as well as an integrated circuit capable of storing and processing data. Super smart cards usually contain specialized programming, stored in ROM, for specific applications such as banking transactions or password generation.

Switch: A system that routes transactions to the appropriate endpoints. Also known as a network.

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 can 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 also Data Encryption Standard.

Synchronous Password Generation: A method of generating a unique one-time password for computer users based on time or transaction synchronization between a host and a device at the point of transmission. The user's device, generally referred to as a token, contains a secret ID or new password every 30 or 60 seconds so the user never enters the same password twice. The host computer contains a synchronized clock, the same algorithm and a file of user seed numbers, so it knows what password to expect at any given time. The method can be strengthened by requiring the user to enter a PIN also.

System Operator: A system operator is a processing entity that supports load acquirers and merchant acquirers whose merchants have POS devices that accept Common Electronic Purse consumer cards, and Common Electronic Purse issuers. A system operator will process transactions for one or more Common Electronic Purse schemes.

T.

Third-party Sales Agents: An organization, other than the card issuer, which sells cards on behalf of the issuer.

Transaction Certificate: A set of encrypted data generated by the chip card to provide information about the actual steps and processes executed by the card, terminal, and merchant during a given transaction. The transaction certificate can be referred to after the transaction in case of a dispute or chargeback.

Transaction Response Time: The amount of time that passes between the moment that the ATR is complete until the card is ejected. Transaction response time requirements differ among the various service providers.

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.

Unload Transaction: The on-line process of unloading value from a electronic purse card to an account.

W.

Wallet: Generally refers to a calculator type or other portable device capable of executing a variety of financial transactions and identification functions. A wallet may include the ability to read and process data from debit, credit, electronic purse and other applications. I may function as a portable device with LCD display, keyboard and read/write capabilities managing a variety of applications and/or information, both financial and non-financial.