EUROPEAN PAYMENTS COUNCIL
Towards our Single Payment Area

Doc: EPC 020/08 (Version 1.02)	18 May 2008 NBI/FGE

SEPA CARDS FRAMEWORK STANDARDISATION "VOLUME"

Payments and Withdrawals with Cards in SEPA: Applicable Standards and Certification Process

DRAFT

Abstract	This document defines the EPC SCF Standardisation
Document Reference	EPC 020/08
File	epc 020 08 scf standardisation volume 1 02
Date of Issue	18 May 2008
Reason for Issue	For public consultation **until 18 August 2008** (close of business)
Reviewed by	Cards Standardisation Task Force
Produced by	Norbert Bielefeld and Francis Geets
Authorised by	Cl. Brun, EPC Cards WG chair
Circulation	Restricted

Table of Contents

1 DISCLAIMER

This document is a working document of the European Payments Council, made available for consultation.

It does not reflect at this stage, and may not be purported to reflect, any official policy stance of the European Payments Council.

2 GENERAL

2.1 Introduction

This document builds on the SEPA Cards Framework that has been available since March 2006 and has contributed through the formulation of policy guidelines to setting the foundations for the SEPA for payments and cash withdrawals with cards. The ambition of the present document is again to set foundations, this time for interoperability and gradually convergence of the technical standards which underpin the end-to-end card value chain.

Achieving greater standardisation in the European card world is a necessity going forward, yet a formidable challenge. When undertaking this task a number of at times conflicting dimensions have to be reconciled:

- The often-excellent service experienced by both cardholders and merchants may not be disrupted. As far as notably cardholders are concerned, greater standardisation must remain almost transparent to them.

- Retailers have significantly invested in and deployed terminal equipment and related software applications. Of course the depreciation deadlines of these equipments up to now reflect more individual decisions than any grand European vision. In addition, in a number of countries, retailers have just completed a migration to EMV.

- Equally retailers are not one. The different requirements of their multiple professions and sectors result in specificities, which must be translated into the products, they deploy.

- Manufacturers appreciate a dose of standardisation, yet want also to be able to differentiate their ware from each other, and take advantage of innovation, in order to compete in the marketplace.

- Policy makers and regulators harbour significant expectations from standardisation: economies of scale achieved thanks to standard equipment certified and deployable at European level should decrease costs and make payments with cards an even more attractive proposition.

- Finally Europe is not an island. Standards for cards are not only decided in Europe, and stakeholders in Europe are concerned about the compatibility beyond Europe's borders of the solutions they propose and/or implement.

This document is the attempt to reconcile these challenges, by offering to all stakeholders a pragmatic path:

1. A set of business and functional core requirements for the card-to-terminal, terminal-to-acquirer, and acquirer-to-issuer domains. These core requirements are complemented by principles for certification with the objective to first achieving mutual recognition of certificates, and later single, Europe-wide certification. It will up to each market participant to decide whether to make use of these core requirements, yet those who do

will be able - as a result of a self-assessment process - to claim themselves to be SEPA-compliant.

2. These core requirements will represent foundation stones on which market participants will be able to develop further technical specifications to meet the specific needs of the various market segments, and to allow for competition. These further technical specifications will be called “proposed specifications” – it will be the responsibility of each provider to ensure that they are effectively compatible with the core requirements above. This document includes several illustrations of such technical specifications – provided here solely for information purpose.

The distinction proposed in this document between business and functional core requirements, and “proposed specifications”, builds on the work performed by several market initiatives (listed at the end of this document). Part of their work had already been the object of individual consultations by the one or the other initiative.

This document is now available for public consultation until 18 August 2008. Responses received during the public consultation process will be incorporated into a further version of this document, for approval by the Plenary of the European Payments Council at the end of this year, and subsequent general publication for adoption and implementation by the market.

In parallel to the present consultation further research will be initiated by the European Payments Council in order to identify the principles for the possible adoption and implementation paths and timelines throughout Europe. This research should be expected to be concluded only in 2009 a finalised standardisation document has been issued.

We expect this document to significantly contribute to shaping the future of payments cards in SEPA. Whether manufacturer, retailer, processor, card scheme or bank, or a representative association, this is your opportunity to express your requirements and influence this future. We invite you to take advantage of it.

2.2 Scope, objectives of EPC work on Cards standardisation

2.2.1 Scope

The objective of the SEPA Cards Framework (SCF)[1] is to establish high level principles and rules which when implemented by banks, schemes, processors and other stakeholders such as merchants and retailers, will enable European customers to use general purpose cards to make payments and cash withdrawals in euro throughout the SEPA area with the same ease and convenience than they do in their home country.

[1] In case of any doubt or conflict, the terminology and meaning of the SCF prevails on any terminology or meaning of the present document.

The SCF acknowledges that a further piece of work is required so that the commitment to cardholders that there are “no differences whether they use their card(s) in their home country or somewhere else within SEPA” is delivered in the most efficient manner by banks and schemes. The necessity for deeper standardization has also been highlighted by European policy makers.

The scope of EPC’s work on cards standardisation in general, and of the present Volume in particular, is the definition and description of core requirements to be implemented throughout the card payment and cash withdrawal value chain (including certification) in order to enable SCF compliance.

2.2.2 Objectives

The **"SEPA Cards Framework Core Requirements"** are the functional and security specifications needed to deliver consistent cardholders experience, functional interoperability and security for SCF Compliant Card Schemes.

In line with the SEPA Cards Framework, these core requirements represent a commitment from the banking payment industry for adoption and implementation. The banking payment industry calls upon all other relevant parties throughout the card payment value chain (merchants, vendors, processors, card schemes, etc.) also to adopt and implement these core requirements.

The core requirements consist of data definitions, supported technologies, descriptions of processes and messages, needed data elements and security requirements.

The core requirements will be a subset of optional detailed implementation specifications which will allow full technical interoperability. The latter will be called **"SEPA Cards Framework Proposed specifications".**

2.2.2.1 Implementation of the Core Requirements

After a date to be set in the implementation plan (to be agreed with the merchants, vendors and other important stakeholders), any service or function included in the scope of Core Requirements should comply with the specified requirements to be considered as consistent with the SCF.

In the Acquirer-to-Issuer domain (authorisations and clearing messages),

- all the acquirer-to-issuer protocols specified or used by SEPA compliant schemes and corresponding infrastructures should be compliant with the Core Requirements for the services and functions they support.

In the Terminal-to-Acquirer domain (authorisation and data collect messages),

- all the terminal-to-acquirer protocols specified or used by SEPA Compliant schemes or SEPA Compliant acquirers should be compliant with the Core Requirements for the services and functions they support.

In the Card-to-Terminal domain,

- Services and functions in the Core Requirement scope should be implemented according to the Core Requirement within the payment terminal, but will of course depend on the environment & terminal usage profile, and also on the services that a merchant wants to support.

Other functions (not in the scope of Core Requirements) are those functions for which no core requirement is defined. Merchants, banks or schemes might require this function based on their own proprietary requirements.

2.2.2.2 Implementation of the Proposed specifications

The use or support of the Proposed specifications will be optional.

2.2.2.3 Impact on the different stakeholders

- In a scheme wishing to be SEPA compliant, any of that scheme's functionality covered by the scope of Core Requirements should comply with the Core Requirements. It is however that scheme's decision which functionalities it implements.

- For a terminal wishing to be SEPA compliant, any of that terminal's functionality covered by the scope of Core Requirements should comply with the Core Requirements. It is however that terminal manufacturer's decision which functionalities it implements.

- For a merchant wishing to be SEPA compliant, any of that merchant's payment service covered by the scope of Core Requirements should comply with the Core Requirements. It is however that merchant's decision which service it implements.

- For an acquirer or processor wishing to be SEPA compliant, any of that acquirer or processor's payment service covered by the scope of Core Requirements should comply with the Core Requirements. It is however that acquirer or processor's decision which service it implements.

- For an infrastructure (authorisation switching network or clearing network) wishing to be SEPA compliant, any of that infrastructure's payment service covered by the scope of Core Requirements should comply with the Core Requirements. It is however that infrastructure's decision which service it implements.

2.3 Governance and standards maintenance aspects

2.3.1 Governance

This SEPA Cards Framework Standardisation Volume is being created and will be maintained under the responsibility of the EPC Cards Working Group or its successor.

A version of the SEPA Cards Framework Standardisation Volume is deemed final once approved by a Resolution of the EPC Plenary and published on the EPC Website.

EPC may from time to time publish notably for consultation draft versions of this SEPA Cards Framework Standardisation Volume. These will always be clearly marked as drafts.

EPC could at a time of its choosing hand over the maintenance of this SEPA Cards Framework Standardisation Volume to an internationally recognised standardization and maintenance body (e.g. CEN, ISO). EPC would clearly communicate about such a decision 3 months before it became effective.

2.3.2 Maintenance

The key principles underpinning maintenance of the SEPA Cards Framework Standardisation Volume are the following:

- Innovation: SEPA Cards Framework Standardisation

- Transparency: the maintenance process shall be transparent and open so that changes to be implemented from a standardization perspective are carefully considered and scrutinized. Establishing open channels for in particular retailers, vendors, and banks and schemes is a key aim of the maintenance process.

- Cost-benefit analysis: maintenance proposals shall be supported by careful analysis weighting up the cost and benefits to ensure that changes that may result from the maintenance of the SEPA Cards Framework Standardisation Volume are viable for all concerned.

- Development of SEPA: standardisation in cards is seen as a critical component of further developments towards achieving SEPA. Not only payment industry participants but also public authorities will continue to monitor the level of effective and desirable standardization, and may make proposals that could result in maintenance of the SEPA Cards Framework Standardisation Volume.
- In order to avoid to the greatest extent possible disruption through numerous changes over a short period of time this Volume will not be updated more than once a year.

2.4 Consultation and validation process

EPC will consult in particular banks, card schemes, retailers, vendors, directly or indirectly though national communities of through associations, when developing and maintaining this SEPA Cards Framework Standardisation Volume. However draft versions of this Volume will always be published on the EPC Website when a period of public consultation will be opened, so that any interested party can submit comments and proposals. In submitting comments and proposals any party will accept that these will be published on the EPC Website (provided their content is not of nature to jeopardize EPC's responsibility as publisher).

The EPC Cards Working Group shall collect and analyse the comments received from the public consultation process. The EPC Cards Working Group shall prepare a formal report on the consultation and make this report available on the EPC Website.

A consultation process may be initiated by the EPC Cards Working Group for 1 of the following, or both reasons:

2.4.1 Receipt of a (or several) Suggestion(s)

A Suggestion is an idea for making any change to the SEPA Cards Framework Standardisation Volume. A Suggestion may be devised by any person and is to be submitted to the EPC Secretariat in accordance with the rules set out in this section. Suggestions can then be sent by the EPC Secretariat to EPC Cards Working Group for consideration.

The latter shall look to receive suggestions from the following sources:

- Banks,
- Card schemes,
- Retailers,
- Vendors.

The EPC Secretariat may also accept suggestions made by EPC Members and bodies within the EPC that have insight into the operation of the SEPA Cards Framework and the usage of the SEPA Cards Framework Standardisation Volume.

The EPC Secretariat shall acknowledge receipt of the Suggestion to the originator within 21 Calendar Days of receiving the Suggestion. An acknowledgement of receipt does not mean that a Suggestion has been accepted, but only that the Suggestion has been received for consideration by the EPC Cards Working Group.

2.4.2 Identification by the EPC Cards Working Group of 1 (or several) Item(s) requiring maintenance

From time to time the EPC Cards Working Group itself may in the course of its work identify items requiring maintenance. Except as regards communication with originators of suggestions (see hereafter) these will be treated as suggestions.

2.4.3 Consideration of a Suggestion and/or Item requiring maintenance

The EPC Cards Working Group shall be responsible for deciding (a) whether the suggested change shall be accepted into the maintenance process or rejected, and (b) whether the change proposed by the Suggestion is a Minor Change or a Major Change.

In respect of (a) the EPC Cards Working Group will only accept suggestions into the maintenance process that propose ideas that fall within the scope of the SEPA Cards Framework. As part of this analysis the EPC Cards Working Group shall consider the change proposed by a Suggestion in accordance with the following broad criteria:

- The change presents a case for wide SEPA market acceptance;
- The change is underpinned by cost-benefit analysis;
- The change is aligned with the strategic objectives of the EPC;
- The change is feasible to implement;
- The change must not impede the integrity and coherence of the SEPA Cards Framework.

Suggestions that are not within the scope of the SEPA Cards Framework, or ones that fail to meet these criteria will generally not be accepted into the maintenance process.

In respect of (b), the EPC Cards Working Group will decide whether a Suggestion proposing a change can be defined as a Minor Change or a Major Change.

A Minor Change is a change of an uncontroversial and usually strictly technical nature that facilitates that the comprehension and implementation of the SEPA Cards Framework Standardisation Volume. Clarifications of the Volume shall not be deemed to affect the substance of the Volume and will therefore be a Minor Change. Examples of such changes include corrections of spelling mistakes, grammatical corrections, or minor adjustments to strictly technical standards to account for upgrades. If a change is classified as a Minor Change it can be approved via a simplified process, as set out below.

A Major change by contrast is a change that affects or proposes to affect the substance of the Volume. Examples of such changes include the addition or development of new technical standards, changes affecting policy, or innovations. Changes that are classified as Major Changes are approved through detailed consultation as presented above.

2.4.4 Acknowledgement of Acceptance or Rejection of Suggestion to originator

After considering the Suggestion the EPC Cards Working Group will decide whether or not to formulate a Change Request on the basis of the Suggestion made and whether the Suggestion should accepted into the maintenance process.

After arriving at a conclusion the EPC Cards Working Group shall notify the originator of its decision in a timely manner. The EPC Cards Working Group may notify an originator directly or indirectly through the EPC Website.

All Suggestions, irrespective of whether they have been accepted into the maintenance process, shall be published on the EPC Website with a view to permitting such a list to be openly viewed.

2.4.5 Preparation and development of a maintenance request

Once a Suggestion has been accepted and the change proposed by the Suggestion classified as a Major Change by the EPC Cards Working Group, the EPC Cards Working Group is responsible for carrying out detailed work to prepare and develop a maintenance request on the basis of the Suggestion made.

The EPC Cards Working Group shall conduct research and carry out a cost-benefit analysis on the Suggestion. This work will involve developing a business case for making a maintenance request and eventually a maintenance proposal. The analysis of the EPC Cards Working Group should also show how the Suggestion meets the criteria set out above.

Where the change proposes to modify the Volume (and any related documentation), a maintenance request shall also show the likely amendments to be made to the Volume (and related documentation) as a result of implementing the change proposed in the Suggestion.

The EPC Cards Working Group shall make all reasonable efforts to develop the maintenance request in a timely manner. The EPC Cards Working Group shall publish a regular update on the EPC Website to indicate the stage of development of maintenance requests.

In the course of developing the maintenance request the EPC Cards Working Group shall consult with the originator so that, as far as reasonably possible, the maintenance request is in line with the Suggestion submitted by the originator.

2.4.6 Consultation on maintenance requests

Once the EPC Cards Working Group has developed a maintenance request, the EPC Cards Working Group shall begin the process of consulting notably banks, card schemes, retailers and vendors.

Banks shall be consulted through established channels (European and national banking communities).

Card schemes, retailers and vendors identified by the EPC Cards Working Group shall receive an invitation to respond to the consultation.

In addition the consultation will be posted on the EPC Website with an invitation to comment.

On the occasion of a consultation the EPC Cards Working Group could organize a cards stakeholder forum at European or national level.

The EPC Cards Working Group shall aim to conclude consultation within 90 calendar days of first calling for consultation. However, in cases where the maintenance request requires further consideration or clarification, the EPC Cards Working Group shall be free to extend any deadline for completing the consultation.

2.4.7 Preparation of maintenance proposal and maintenance proposal submission document

If the EPC Cards Working Group decides to proceed with the change following consultation, the EPC Cards Working Group shall prepare a maintenance proposal, taking into account comments received during the consultation process. The maintenance proposal shall set out details of the change proposed and the likely costs and benefits involved in implementing the change. The maintenance proposal shall detail non-confidential comments received from the different respondents to the consultation. Where the change proposes to modify the Volume (and any related documentation), the maintenance proposal shall include a mark-up of the Volume (and any related documentation) to show the amendments to be made to the Volume and related documentation as a result of implementing the change.

A maintenance proposal may bring together more than one change, as developed from one or more Suggestions.

The EPC Cards Working Group shall complete a maintenance proposal submission document for submission to the EPC Plenary alongside the maintenance proposal. The maintenance proposal submission document shall certify that each stage of the maintenance process, from origination to consultation, has been properly completed in respect of the change proposed.

2.4.8 Submission of maintenance proposal to the EPC Plenary

Following its consideration by the Co-ordination Committee in accordance with the EPC Charter, the maintenance proposal and the maintenance proposal submission document shall be submitted to the EPC Plenary for determination. The EPC Plenary shall determine whether or not to accept the maintenance proposal by Resolution.

2.4.9 Publication

A maintenance proposal that has been considered by the EPC plenary shall be published on the EPC Website together with the maintenance proposal submission document and the decision of the EPC Plenary. The EPC Cards Working Group shall use reasonable efforts to publish all maintenance proposals, irrespective of whether the change has been accepted or rejected by the EPC Plenary, as soon as reasonably practicable after the relevant decision of the EPC Plenary.

2.4.10 Maintenance release process and cycle

2.4.11 Process for submitting Minor Changes

2.4.11.1 Preparation of list of Minor Changes

The EPC Cards Working Group shall prepare a list of Minor Changes not more than twice each year. This list shall take into account Suggestions received by the EPC Cards Working Group as well as any Minor Changes that the EPC Cards Working Group considers as required.

2.4.11.2 Publication of list of Minor Changes

The EPC Cards Working Group shall publish a list of Minor Changes on the EPC Website. Any person may submit comments to the list of Minor Changes through the EPC Website to the EPC Cards Working Group. The EPC Cards Working Group shall permit comments to be sent to it for a period of 90 calendar days starting from the date of publication of the list of Minor Changes on the EPC Website. However the EPC Cards Working Group shall be free to extend this period, if appropriate.

2.4.11.3 Re-classification of a Minor Change

In the event the EPC Cards Working Group receives extensive comments on the list of Minor Changes, where some items on the list are identified by contributors as potentially Major Changes, the EPC Cards Working Group may remove the item from the list and consider re-classifying this item.

The EPC Cards Working Group may consult with relevant contributors on the status of the item with a view to determining whether a change is a Minor or a Major Change. Following such a consideration, the change may be re-classified as a Major Change and redirected for approval through the approval process for Major Changes (see above).

2.4.11.4 Submission of list of Minor Changes to the EPC Plenary

The list of Minor Changes shall be submitted to the EPC Plenary for determination. The EPC Plenary shall determine whether or not to accept the changes proposed in the list of Minor Changes by Resolution.

2.4.11.5 Publication of approved Minor Changes

A list of Minor Changes that has been considered by the EPC Plenary shall be published on the EPC Website together with the decision of the EPC Plenary on the items listed. The EPC Cards Working Group shall use reasonable efforts to publish the list of Minor Changes, irrespective of whether the changes proposed have been accepted or rejected by the EPC Plenary, as soon as reasonably practicable after the relevant decision of the EPC Plenary.

2.4.11.6 Maintenance release process and cycle

In order to prevent potential disruptions by a rapid succession of numerous maintenance proposals, the EPC Plenary shall only approve 2 lists of Minor Changes (or less) in any calendar year, except in exceptional circumstances. The EPC Plenary may only approve a further list when for example failure to maintain the Volume may result in disruption for stakeholders.

2.5 Intellectual property, copyright aspects

Readers including potential and actual users of this SEPA Cards Framework Standardisation Volume acknowledge that any copyright to the Volume belongs to the EPC. Neither readers nor potential and actual users of this SEPA Cards Framework Standardisation Volume shall assert contrary claims, or deal with the SEPA Cards Framework Standardisation Volume in a manner that infringes or is likely to infringe the copyright held by the EPC in the SEPA Cards Framework Standardisation Volume.

Part of the documents included in this SEPA Cards Framework Standardisation Volume may have been originally produced – and may be published – in whole or part by one or another of the “initiatives” – or individual participants thereto - listed in the acknowledgment section to this Volume.

When invited to participate in the EPC Cards Standardisation Process, participants in the said initiatives were jointly and repeatedly informed that one of the primary objective of the work undertaken is to ensure that European banks and other stakeholders, including the schemes in which they participate, have open and free access to, and free usage of, standardization work performed. In order to maximize efficiency all also acknowledged that the work to be undertaken would capitalize to the greatest extent possible on existing initiatives, with the additional objective to recognize the needs of all relevant stakeholders, coordinate work underway, agree deadlines and monitor deliverables.

Whilst acknowledging the provenance of such material as originating with the said initiatives and/or participants thereto, the intellectual property rights, copyright and rights of development and disposal now reside exclusively with EPC. EPC gratefully acknowledges the work of the said initiatives and/or participants thereto in creating part of the original documentation and supporting work.

EPC and all parties including the said initiatives may make use of this material other than for commercial gain, provided that its source, now being EPC, is duly recognised.

2.6 Definitions

The definitions hereafter are limited to the ones necessary to understand the functional requirements listed in the EPC Cards Matrix file.

2.6.1 Services - debit and credit when applicable -

A service is the process to support financial and non financial events in the card payment or withdrawal environment.

ATM Cash withdrawal	ATM Cash withdrawal takes place at an unattended cash dispensing devices and allows cardholder to withdraw money.
Balance inquiry	Solicited card balance inquiry (e.g. for account checking or prepaid cards).
Cancellation at Point of Sale	This service occurs when a previously performed Payment is cancelled by the merchant after processing. Cancellation should only occur before the transaction is cleared to the issuer. It is sometimes called “Manual reversal”.
Card funds transfer	A service • which allows to transfer funds from ○ a card account (PAN) to another card account ○ a bank account (IBAN) to a card account ○ a card account to a bank account • where neither of these two entities acts as a card acceptor (or professional payee) • where the payment is not done for a commercial purpose
Card validity check	A service that allows the validity of the card to be checked. This transaction has no financial impact on the card account. Sometimes it is called “information request”.
Cash advance (attended)	A service that allows the cardholder to withdraw cash at merchant POS terminal or a bank counter.
Cash deposit	Cash deposit is a card operation where a cardholder deposits cash to his own card account. It takes place • either at a bank counter • or at an attended or unattended point of service.
e-purse - Loading/unloading	It is a card operation where a cardholder transfers/removes funds on an electronic purse.

Instalment payment	Spread out transmission of the payment by the merchant for a known amount and duration.
No-show	This service allows a merchant to transmit a payment when a cardholder who has made a booking and didn't' cancel it in a specified period. It is used e.g. for hotel trade.
Original credit	A service which allows to transfer funds from a card acceptor (or professional payee) account to a card account. Unlike refunds, an original credit is not preceded by another card payment.
Payment	The basic payment on a terminal capturing all the data required for the execution of payment transaction (authorisation, clearing and settlement) required to pay for the purchase of goods, services, etc.
Payment completion	The service of completing a payment following a pre-authorisation or update pre-authorisation request.
Payment with Cash back	Cash back is a service offered during a card payment whereby an extra cash amount is added to the total amount of a payment. The customer receives the extra cash amount in notes or coins along with the goods/services.
Pre-authorisation	A pre-authorisation is used to secure an amount for a specified period of time. During the authorisation, the amount is only secured since neither the final amount nor the final date and time of the actual payment are known (e.g. car rental, hotel, video rental, etc.). Pre-authorisation is also called "reservation".
Prepaid card - Loading	Operation where a cardholder transfer funds to a prepaid card account from another card account, a bank account or cash.
Prepaid card - Unloading	Operation where a cardholder debits a prepaid card account.
Quasi-Cash payment	A payment for items that are directly convertible to cash, such as gaming chips.
Recurring payment	A periodic payment transmitted by the merchant often without a fixed amount and with an unknown duration.

Refund (partial or total)	The Refund is the opposite of a payment transaction. As an example, the cardholder returns goods to a merchant and is credited with their value. This service allows the merchant to reimburse the cardholder.
Two steps payment	The two steps payment is a payment , for which an authorisation (offline or online) is required before the goods are delivered, when the final amount of the payment is unknown. The two steps payment starts with an unknown amount, and ends when the final amount is known. There is a “short” elapsed time between the start and the end of the two steps payment. The two steps payment is performed on one terminal, in two steps. Examples where two steps payment is used are unattended gasoline pumps and phone booths.
Update pre-authorisation	The update pre-authorisation service is used to update the estimated amount and/or update the validity period of the previous pre-authorisation or the previous update pre-authorisation.

2.6.2 Additional features

Additional features allow particular usage within a service.

Payment or cash withdrawal with dynamic currency conversion	A service which allows the customer to select the currency of the transaction. DCC is performed by the acceptor to dynamically convert the service currency of the acceptor to the currency of the cardholder.
Payment with purchasing or corporate card Level 2 data	Handling of data related to a specific activity (e.g. VAT, reference numbers, etc.).
Payment with purchasing or corporate card Level 3 data	Handling of data related to a specific activity (e.g. e-invoicing, sector specific additional data, etc.).
Payment with cumulative amount	A payment with cumulative amount is transmitted to cumulate more than one transaction carried out by the same cardholder.

Payment with deferred clearing	The characteristic of a deferred clearing is that the acquirer postponed the clearing of the transaction. It is used for example for the payment of health expenses.
Payment with increasing amount	A service that allows the customer to increase the amount of a payment , for example where a gratuity (tip) is added.
Payment with Loyalty information	A service that allows a merchant to accept payments with loyalty or reward his customers or other loyalty programmes.
Payment with purchasing or corporate card data	A service that allows the capture of data to be added to the payment transaction in support of the use of a company purchasing or corporate card.
Unsolicited available funds	The unsolicited available funds response will give Issuers the ability to use authorisation response to provide unsolicited account balance information.

2.6.3 Functions

A function is a part of the process supporting a service.

Advice	A function where the sender notify the receiver of an activity that has been taken.
Authorisation	Transactional Authorisation (or simply authorisation) is the function performed by the Acceptor to assess whether a card payment can take place or not.
Completion	Completion is the function performed to provide the acquirer with information on how the payment was completed.
Data capture	Data capture is a function to transfer exchange data captured at a POI System to the Acquirer for financial presentment.
Financial presentment	Clearing is the function which enables banks and financial institutions to exchange the amounts due for the processed payments transactions.
Information request	A function to request information.

Reconciliation	A function which enables two entities (merchant, acquirer, issuer or their agents) to exchange their views on financial totals (amounts, number of transactions).
Referral	A referral occurs when the initial authorisation request is first responded to with an appropriate Referral Authorisation Response Code and the transaction is completed with a voice conversation (out of scope) to seek an approval for the transaction to proceed.
Reversal	A reversal shall be used to partially or completely nullify the effects of a previous financial or authorisation transaction.

2.6.4 Environments

Attended	An attendant (an agent of the merchant or of the acquirer) is present at the point of transaction and participates in the transaction by entering transaction-related data. The transaction occurs 'face to face'.
e-payment – 3D-Secure	A payment where goods, services, etc. are purchased over electronic systems such as the Internet and other computer networks using 3D-Secure protocol. The cardholder can be authenticated by the issuer.
e-payment – card present (ICC)	A payment where goods, services, etc. are purchased over electronic systems such as the Internet and other computer networks. A card reader device which is not under the merchant responsibility is used to get ICC card data.
e-payment – other	A payment where goods, services, etc. are purchased over electronic systems such as the internet and other computer networks without using 3D secure protocol.
Mobile payment (remote)	e-Payment performed with a mobile phone.
MOTO	Payment performed by mail or telephone, following a mail order or telephone order.

Proximity/contactless payment	• Payment performed locally through a contactless communication between a Mobile NFC-enable device and a contactless reader. • Payment performed locally through a contactless communication between a contactless card and a contactless reader.
Semi-attended	The cardholder conducts the transaction at the point of transaction without the participation of an attendant (agent of the merchant or of the acquirer). However an attendant is present to provide assistance to the cardholder if necessary.
Unattended	The cardholder conducts the transaction at the point of transaction without the participation of an attendant (agent of the merchant or of the acquirer). The transaction does not occur face to face (e.g. vending machines, petrol pumps, parking meters, etc.).

2.6.5 Acceptance technologies

Chip contactless EMV based	IC Card compliant with EMV contactless specifications. EMV chip uses RFID for making secure payments. The embedded chip and antenna enable consumers to wave their card over a reader at the point of service.
Chip with contact EMV	IC Card compliant with EMV specifications.
Contactless non EMV	A non EMVco Contactless application which uses RFID for making secure payments (e.g. magstripe contactless or legacy application).
Imprint	Cardholder data are obtained from a card Imprint.
Magstripe	Cardholder data are obtained from magnetic track reading.
Manual entry	Cardholder data are obtained from manual key entry.

2.6.6 Authentication methods

3D-Secure authentication	The 3D-Secure technology enables the merchant's plug-in to check that the cardholder is registered with a secure payment system. It provides the internet details of the cardholder authentication entity (issuing bank or delegated entity).
Biometric	Biometric is a cardholder's identity verification method based upon one or more intrinsic physical or behavioral features.
Card security code	Card security code printed on the card (e.g.CVV2 or CVC2).
No CVM	No cardholder verification method is required.
Off-line Pin	The PIN entered to verify cardholder's identity is controlled by the chip-processor. The PIN may be verified by the card in encrypted form or in clear text.
On-line Pin	The PIN entered to verify cardholder's identity is controlled by sending an encrypted PIN to the Issuer or delegated entity for validation in an authorisation request.
Signature	The cardholders' handwritten signature is used to verify his identity.

2.6.7 Card management services

Card activation	Card activation is an operation to initialise a new card prior to any usage.
Card pick up	This Pick-up service purpose is to inform the acceptor that the card should be picked up.
Card pick up advice	This Pick-up advice service purpose is to inform the issuer that the card has been picked up.
Pin change	The PIN change service provides the cardholder the capability to change his PIN.

Return card advice	The Return card advice purpose is to inform the issuer that the card has been returned to cardholder.
Return card to cardholder request	The Return card to cardholder request purpose is to get authorisation to return card to cardholder.

2.6.8 Terminal management services

Acquirer parameters downloading	This service allows to download/update the parameters that the acquirer is responsible for (POI identification, exception file, floor limits, EMV parameters, etc.).
POI characteristics uploading	This service allows the entity in charge of the terminal management to get information on the POI.

2.6.9 Back office services

Back Office management	Operations beside presentment to ensure clearing (e.g. charge back, re-presentment, fee collection, request for copy of receipt, etc.).
Merchant management	Services offered to the merchant by its bank or other institution (financial report, etc.).

2.6.10 Exchange management

Application Layer Security	Definition of an application layer and cryptographic mechanisms that • Authenticate the parties involved in protocol exchanges • Keep data elements secret that require confidentiality • Ensure the integrity of the processes and data.

Error handling	Description of the error handling needed for the card payment processing and clearing (handling of data content and format errors, time-outs etc.).
Key management	Definition of a trust model, key management respectively key hierarchy for the protection of data and the exchange of cryptographic keys and other related security parameters.
Protocol syntax	Definition of the coding and semantics of the processed data exchanged by the involved parties (e.g. ISO 8583 Bitmap, ASN.1, XML, BER-TLV).
Transport Layer Security	Definition of a session/transport layer and cryptographic mechanisms that • Authenticate the parties involved in protocol exchanges • Keep messages secret • Ensure the integrity of the processed messages. (e.g. authentication, encryption and signatures implemented by SSL/TLS).
Transport Logic / Kinematics	The transport logic includes the definition of the application layer underlying communication respectively transport protocols including the rules (e.g. establishing a connection, force disconnection, etc).

2.7 Detailed description of the scope ("cross domain matrix")

The core requirements are globally described in Ch. 3. It is likely that future versions of the present document will describe individually each of these requirements.

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to definition section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
PAYMENT SERVICES								
Payment	Y	Y	Y	Y	Y	Y	Y	1
Refund (partial or total)	Y	Y	Y	Y	Y	Y	Y	1
Cancellation at Point of Sale	Y	Y	Y	Y	Y	Y	Y	1
Two Steps Payment	Y	Y	Y	Y	Y	Y	Y	1
Pre-authorisation	Y	Y	Y	Y	Y	Y	Y	1
Update pre-authorisation	Y	Y	Y	Y	Y	Y	Y	1
Payment completion	Y	Y	Y	Y	Y	Y	Y	1
No-show	Y	Y	Y	Y	Y	Y	Y	1/2
Instalment payment	Y	Y	Y	Y	Y	Y	Y	2/3
Recurring payment	Y	Y	Y	Y	Y	Y	Y	2/3
Quasi-Cash payment	Y	Y	Y	Y	Y	Y	Y	1
Payment with Cash Back	Y	N	Y	N	Y	N	Y	3

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to definition section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
CASH SERVICES								
ATM Cash Withdrawal	Y	Y	Y	N	N	Y	Y	1
Cash advance (attended)	N	N	Y	N	Y	N	Y	3
Cash deposit	N	N	N	N	N	N	N	N/A
CARD INQUIRY SERVICES								
Card Validity Check	Y	Y	Y	Y	Y	Y	Y	2
Balance Inquiry	N	N	N	N	N	N	Y	3
Unsolicited available funds	N	N	N	N	Y	N	Y	3
CARD ELECTRONIC TRANSFER								
Card Funds Transfer	Y	N/A	N/A	N/A	N/A	Y	Y	3
Original credit	Y	Y	Y	Y	Y	Y	Y	3
e-purse - Loading/unloading	N	N	N	N	N	N	N	N/A
Pre-paid card - Loading	Y	Y	Y	Y	Y	Y	Y	3
Pre-paid card - Unloading	N	N	N	N	N	N	N	N/A

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to definition section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
CARD ADDITIONAL SPECIAL TRANSACTIONS								
Payment with Increasing amount	Y	Y	Y	Y	Y	Y	Y	2
Payment or cash withdrawal with dynamic currency conversion	Y	N	Y	N	Y	N	Y	3
Payment with cumulative amount	N	N	N	N	Y	N	Y	3 / 2
Payment with deferred clearing	N	N	Y	N	Y	N	Y	3 / 2
Payment with purchasing or corporate card Level 2 data	Y	Y	Y	Y	Y	Y	Y	1
Payment with purchasing or corporate card Level 3 data	Y	N	Y	N	Y	N	Y	3
Payment with Loyalty information	N	N	N	N	N	N	N	N/A

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
CARD MANAGEMENT SERVICES								
Pin change	N	N	N	N	N	N	N	N/A
Pin/card unlock	N	N	N	N	N	N	N	N/A
Card activation	N	N	N	N	N	N	N	N/A
Return card to cardholder request	N	N	N	N	N	N	N	N/A
Card pick up advice	N	N	N	N	N	N	N	N/A
Return card advice	N	N	N	N	N	N	N	N/A
TERMINAL MANAGEMENT SERVICES								
POI characteristics uploading	N	N	N	N	Y	N/A	N/A	3
Acquirer parameters downloading	Y	Y	Y	Y	Y	N/A	N/A	2
BACK OFFICE SERVICES								
Back Office management	Y	N/A	N/A	N	N	Y	Y	1
Merchant Management	N	N/A	N/A	N	N	N/A	N/A	3

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
EXCHANGES MANAGEMENT								
Transport Logic / Kinematics	Y	N	N	N	Y	N	Y	N/A
Transport Layer Security	Y	N	N/A	N	Y	N	N	N/A
Application Layer Security	Y	N	N/A	N	Y	N	N	N/A
Key management	Y	N	Y	N	Y	N	N	N/A
Error handling	Y	N	Y	N	Y	N	Y	N/A
Protocol syntax	Y	N	N/A	N	Y	N	Y	N/A
FUNCTIONS (implementation dependend - therefore no need to define the core requirements scope)								
Authorisation (partial & total)	Y	-	Y	-	Y	-	Y	1
Data capture	Y	-	Y	-	Y	-	N/A	1
Financial presentment	Y	-	N/A	-	N/A	-	Y	1
Referral	Y	-	Y	-	Y	-	Y	1
Reversal	Y	-	Y	-	Y	-	Y	1
Completion	Y	-	Y	-	Y	-	Y	2
Information Request	Y	-	Y	-	Y	-	Y	3
Advice	Y	-	Y	-	Y	-	Y	2
Reconciliation	Y	-	Y	-	Y	-	Y	2

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
SUPPORTED ENVIRONNMENT								
Attended	Y	Y	Y	Y	Y	Y	Y	1
Unattended	Y	Y	Y	Y	Y	Y	Y	1
Semi-attended	Y	Y	Y	Y	Y	Y	Y	1
MOTO	Y	Y	Y	Y	Y	Y	Y	1
e-payment – 3D-Secure	Y	Y	Y	Y	Y	Y	Y	1
e-payment – other	N	N	N	N	N	N	N	N/A
e-payment card present (ICC)	Y	Y	Y	Y	Y	Y	Y	3
Proximity/contactless payment	Y	Y	Y	Y	Y	Y	Y	3
Mobile payment (remote)	Y	Y	Y	Y	Y	Y	Y	3
SUPPORTED ACCEPTANCE TECHNOLOGIES								
Chip with contact EMV	Y	Y	Y	Y	Y	Y	Y	1
Chip contactless EMV based	Y	Y	Y	Y	Y	Y	Y	2
Contactless non EMV	N	N	Y	N	Y	N	Y	3
Magstripe	Y	Y	Y	Y	Y	Y	Y	1
Manual entry	Y	Y	Y	Y	Y	Y	Y	1
Imprint	N	N	N	N	N	N	N	N/A

	EPC interest	CARD TO TERMINAL DOMAIN		TERMINAL TO ACQUIRER DOMAIN		ACQUIRER TO ISSUER DOMAIN		Priority level
(hyperlinks to section heads)		Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	Core req. scope	Proposed specs.	1 = highest 2 = medium 3 = lowest
SUPPORTED AUTHENTICATION METHODS								
Off-line Pin	Y	Y	Y	Y	Y	Y	Y	1
On-line Pin	Y	Y	Y	Y	Y	Y	Y	1
3D-Secure authentication	Y	?	?	Y	Y	Y	Y	1
Card security code	Y	Y	Y	Y	Y	Y	Y	1
Signature	Y	Y	Y	Y	Y	Y	Y	1
No CVM	Y	Y	Y	Y	Y	Y	Y	1
Biometric	N	N	N	N	N	N	N	N/A

3 CORE REQUIREMENTS

3.1 Chapter "Card To Terminal space" Core Requirements

3.1.1 Reference

SEPA FAST
Financial Application Specification for SCF Compliant EMV Terminals Part 1: Attended POS Environment - Version 2.10 28.04.2008 - Business and Functional Requirements

3.1.2 Introduction

3.1.2.1 Terms and Definitions

Throughout this document the following terms will be used and should be interpreted according to their accompanied definition.

Activated	Indicates that a financial service or function has been configured as turned on.
Configurable	Indicates that the operation of a financial service or function may be adjusted by means of parameters, e.g. to turn the financial service or function on or off, to set the value of a data element to be used in the financial service or function, etc.
Configuration	The act and setting of the configurable financial services and functions within a terminal.
Currently selected financial service	The financial service used during the current transaction.
Currently selected language	The language used for displaying cardholder messages during the current transaction.
Financial service	Denotes the business process performed between a cardholder and a merchant (or acceptor) that results in a transaction, i.e. purchase, purchase with cashback, refund, cancellation, reservation, deferred sale, cash withdrawal, cash advance and cash deposit.
Function	Denotes a processing step or a sub-element of a financial service
Payment Profile	A Payment Profile in the terminal determines the processing parameters with which a terminal performs a transaction. The terminal chooses the Payment Profile based on the selected AID and optionally some data present in the FCI Discretionary data.
Supported	Indicates that a financial service or function is implemented in the terminal application
Terminal	Denotes all types of implementations of Point of Interaction (POI)systems: card acceptance devices including stand-alone terminals, connected terminals, distributed systems, and clustered systems
Terminal application	POI software supporting an implementation of SEPA-FAST

3.1.2.2 Abbreviations

AAC	Application Authentication Cryptogram
AC	Application Cryptogram
ARQC	Authorisation Request Cryptogram
AID	Application Identifier
ATM	Automated Teller Machine
CVM	Cardholder Verification Method
ECB	European Central Bank
EU	European Union
EPC	European Payments Council
FCI	File Control Information
ICC	Integrated Circuit Card.
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
POI	Point of Interaction
POS	Point of Sale.
PSE	Payment System Environment.
SCF	SEPA Cards Framework
SEPA	Single Euro Payment Area
VAT	Value-Added Tax

3.1.2.3 Reference

No references are made to relevant ISO/IEC standards, since they are already referenced to in the EMV standard.

[EMV] EMV Integrated Circuit Card Specifications for Payment Systems, Version 4.1, May 2004, and in addition all specification updates and any future versions as published on the EMVCo website.

[SCF] SEPA Cards Framework, Version 2.0, 8 March 2006, EPC

3.1.3 Business Requirements

This section describes the business requirements for SEPA-FAST. They are consistent with [SCF] and take into account additional requirements of the Payment Schemes.

3.1.3.1 Standardisation

SEPA-FAST shall comply with the requirements in the EMVCo specifications (see [EMV]), and shall be consistent with the SEPA objectives stated in [SCF] and in

- ECB: Towards a Single Euro Payments Area – Objectives and Deadlines (4th Progress Report) 17 February 2006
- European Commission: Consultative paper on SEPA Incentives, 13 February 2006

In addition, and as far as possible, SEPA-FAST shall take into account specific requirements of the Payment Schemes as described in the following sections.

SEPA-FAST shall harmonise these requirements and detail them as far as is needed. In order to protect existing investments in the deployment of EMV, and to ensure the stability of the standard, SEPA-FAST is not meant to change but rather to be complementary to the EMV specification, in particular to resolve the "grey areas" in that specification.

This harmonisation shall include the specification of the generic transaction flow at the terminal. This is required to facilitate the acceptance of any SCF compliant scheme at any terminal.

3.1.3.2 Adaptability and Configurability

In order to comply with the requirement of [SCF] that "The basic transaction flow will be defined by each scheme", the generic transaction flow in SEPA-FAST shall allow variations which are necessary to support requirements of different payment products. In addition, the support of the financial services described in SEPA-FAST depends on the sector of activity of the business and the terminal type used. Consequently, transaction flows shall be defined in such a way that the flow can be easily configured to include or omit specific functionalities.

However, a terminal may implement a subset of the described functionality, provided it is described by an implementation option.

3.1.3.3 Selection of the Payment Application

The Selection of the Payment Application must be in line with [SCF]:

> *"Where several payment applications are contained in the same card and supported by the same terminal, cardholders will have the choice of which payment application they will use. Prevalence at POS for a particular payment application may not be mandated by a card scheme."*

SEPA-FAST shall support Payment Application Selection based on standard EMV Application Selection but will also allow for the selection of non-EMV based products.

3.1.3.4 Cardholder Display Language – Language Selection

SEPA-FAST shall require cardholder messages to be displayable in at least a local language and English in every terminal.

SEPA-FAST shall describe language selection based on the assumption that all SCF compliant cards include the cardholder's preferred language and English. SEPA-FAST aims to minimise cardholder interaction and therefore SEPA-FAST shall not include manual language selection by the cardholder during financial services.

SEPA-FAST shall define all cardholder messages unambiguously and for all European languages.

3.1.3.5 Cardholder Authentication

In accordance with section 1.3.2 of [SCF], SEPA-FAST shall require every terminal to be able to support PIN as CVM. Other CVMs as defined by [EMV] may also be supported.

Offline-only terminals shall support both plaintext PIN verification performed by the ICC and enciphered PIN verification performed by the ICC.

Offline with online capability terminals shall support both plaintext PIN verification performed by the ICC and enciphered PIN verification performed by the ICC and may support, in addition, enciphered PIN verified online.

Online-only terminals shall support one of the following options:

a) Plaintext PIN verification performed by the ICC and enciphered PIN verification performed by the ICC,

b) or enciphered PIN verified online,

c) or the combination of options a) and b).

SEPA-FAST shall not support PIN Bypass.

3.1.3.6 Card Authentication

With the exception of online-only terminals, the terminal application shall support all offline card authentication methods as defined in [EMV].

3.1.3.7 Transaction Currency

SEPA-FAST shall cover a single-currency terminal application.

3.1.3.8 Multiple Payment Profiles and Acquirers

SEPA-FAST shall require terminals to allow the support of multiple Payment Profiles, as well as multiple Acquirers.

The terminal shall apply a specific set of processing parameters per Payment Profile, selected during Payment Profile Selection. Examples are floor limit and terminal action codes.

It shall be possible to define a specific Acquirer for each accepted payment profile.

3.1.3.9 Terminal-to-Acquirer Protocol and Data Storage

The terminal-to-Acquirer protocol shall support the transmission of full-chip data.

The use of the EPAS protocol shall not be proscribed and the use of other protocols shall not be excluded. The SEPA-FAST data dictionary and message flows will, however, be coordinated with the EPAS data dictionary and message flows.

Since SEPA-FAST implementations will be used in different environments it is necessary to specify different methods of capturing the transactions to be cleared.

The following methods, or combinations thereof, of transferring the transactions to an Acquirer will be described:

- Online capture through the authorisation message.
- Online capture through advice messages sent after each transaction.
- Batch capture through file transfer or transaction by transaction.

3.1.3.10 Performance

In order to limit transaction times, SEPA-FAST shall describe an optimised set of cardholder interactions and shall allow the possibility of parallel processing of tasks.

3.1.4 Functional Requirements

The following sections describe the functional requirements to be met by the terminal application for the processing of financial services, i.e. Purchase, Cancellation and Refund, Hotel and Rental, and Cash Advance on POS for an attended terminal.

3.1.4.1 Transaction Initialisation

Req 12: If the default financial service is not the required service, the attendant shall be able to select the required financial service from the list of financial services that are activated.

Req 13: For transaction initialisation the cardholder display shall always display a message to the cardholder, which will relate to the default service.

Req 14: This message shall be shown only in the currently selected language if the default language was manually overridden. Otherwise it shall be shown in the default language and English (or in the default language only if it is English). If the display is not capable of showing the message in two different languages at the same time, it shall alternate between the two.

Req 15: The transaction shall be initiated either by card reading or by attendant action.

The attendant may initiate the transaction by, for example:

- Entering the amount, if this is allowed for the currently selected financial service,
- Entering the PAN, if this is allowed for the currently selected financial service (e.g. Refund).

3.1.4.2 Payment Service

3.1.4.2.1 Technology Selection for Payment

Technology Selection is the process used to select one of the processing modes supported for the selected financial service.

Req 16: For Payment, chip processing shall be supported and shall have the highest priority. The remaining two processing modes described in section 2.1 may be supported by the terminal application. It shall be possible to configure which of the processing modes supported by the terminal application are allowed for the Payment Service.

Req 17: If a card is inserted in the chip reader of a terminal with separate readers or in a hybrid reader, the terminal application shall recognise this and shall initiate reset processing according to [EMV].

Req 18: If a card is inserted in the chip reader of a terminal with separate readers or in a hybrid reader, and if the reset processing is successful according to [EMV], the selection of the Payment Profile for a chip transaction shall be performed observing the requirements described in section 4.3.2.

Req 19: If a card is inserted in the chip reader of a terminal with separate readers or in a hybrid reader, and if the reset processing is unsuccessful according to [EMV], the terminal application shall terminate EMV processing and may accept the card based on the chip but as a non EMV card, which is out of scope of this document.

Req 20: If a card is inserted in the chip reader of a terminal with separate readers or in the hybrid reader, and if the reset processing is unsuccessful according to [EMV], and if the terminal configuration allows for additional re-reading of the chip, the counter of re-reads for the current transaction shall be increased by one and an error message shall be displayed to retry the chip (for a terminal with separate readers) or the card (for a terminal with a hybrid reader).

Req 21: If a card is inserted in the chip reader of a terminal with separate readers or in the hybrid reader, and if the chip technology does not work[2], and if the magnetic stripe processing mode is supported for Payment, and if fallback to magnetic stripe is allowed[3], the terminal application shall attempt to initiate magnetic stripe processing. In this case the following requirements shall be observed:

- For a terminal with separate readers, the terminal application shall record that there has been an attempt to read the chip during the current transaction, and shall display an error message to use the magnetic stripe.
- For a terminal with a hybrid reader, magnetic stripe processing shall be initiated without cardholder interaction if Track 2 of the magnetic stripe has been pre-read successfully.
- For a terminal with a hybrid reader, a message for the cardholder to retrieve the card shall be displayed if Track 2 of the magnetic stripe has not been pre-read successfully.
- For a terminal with a hybrid reader, transaction processing shall be terminated with an error message if neither pre-read nor post-read of Track 2 of the magnetic stripe is successful.

Req 22: If the terminal supports Magnetic Stripe processing for fallback, then the terminal application shall support reading and processing of the full Track 2.

Req 23: If a card is inserted in the magnetic stripe reader of a terminal with separate readers, and if the Service Code within Track 2 indicates that chip processing is supported by the card, and if there has not been an attempt to read the chip during the current transaction, the terminal application shall display a message to use the chip.

Req 24: If a card is inserted in the magnetic stripe reader of a terminal with separate readers, and if either the Service Code within Track 2 does not indicate that chip processing is supported by the card or there has already been an attempt to read the chip, the terminal application shall initiate magnetic stripe processing. Magnetic stripe processing shall be regarded as fallback if Track 2 indicates that chip processing is supported by the card[4].

Req 25: Irrespective of the type of reader, the terminal application shall only use magnetic stripe data from the last card reading attempt. In particular, if no magnetic stripe data was read during the last card reading attempt, no magnetic stripe data shall be used by, or be present in, the application.

3.1.4.2.2 Application Selection

Req 26: Application selection must follow EMV rules.

Req 27: The terminal application shall only support cardholder selection as defined in [EMV] Book 1 Section 12.4 Step 4.

[2] Chip technology does not work if the reset processing is unsuccessful and the terminal configuration does not allow for additional re-reading of the chip, or if no commonly supported chip application is present on the chip, or if chip processing has to be aborted because of an error.

[3] Magnetic stripe processing is not allowed for the current transaction if the chip on the card is blocked, or if all commonly supported chip applications are blocked, or if chip processing is aborted after an online request has been initiated by the card.

[4] Magstripe based transactions will not be SCF compliant after 2010

3.1.4.2.3 Initialisation of the Payment Profile

Req 28: The terminal application shall maintain a list of Payment Profiles, based on the AID and optionally some data present in the FCI Discretionary data. The processing parameters assigned to the Payment Profile that is finally selected shall be used for further processing.

3.1.4.2.4 Language Selection

Req 29: If the card's Language Preference is read during Payment Profile selection, selection of the cardholder display language shall be performed according to [EMV] and the terminal application shall use from that moment on the cardholder display language with the highest preference that it supports.

Req 30: If the card's Language Preference is not read, or if the terminal application does not support any of the languages in the card's Language Preference, the terminal application shall continue to use the currently selected language.

Req 31: If the terminal application offers the option to the attendant or the cardholder to override the default language and to select one of the languages supported by the terminal for the cardholder display, then this shall only be possible prior to the start of the transaction. In this case, the chosen language shall become the only language supported (and therefore become the currently selected language) by the terminal for the duration of this transaction.

3.1.4.2.5 Chip Transaction

3.1.4.2.5.1 Application Initialisation

Application Initialisation is performed compliant with [EMV]. This includes the support of Proprietary Tags.

Unless the amount is requested in the PDOL, the initialisation of the application (i.e. sending Get Processing Options command and reading application data) is possible before the amount is known.

3.1.4.2.5.2 Additional Processing Requirements

Req 32: It shall be possible to configure per Payment Profile the following additional functions:

- Checking Payment amount (min-max amounts allowed in the terminal),
- Entering of VAT amount,
- Adding a gratuity,
- Entering a Cashback amount,
- Entering variable numeric data, for example car mileage.

Req 33: With the exception of online-only terminals, the terminal application shall support all offline card authentication methods as defined in [EMV].

Req 34: It shall be possible to configure the supported CVMs per Payment Profile.

Req 35: The terminal application shall not support PIN Bypass.

Req 36: It shall be possible to configure the terminal application as online-only or online with offline capability or offline-only.

3.1.4.2.5.3 Authorisation Exchange (for Online Transactions)

Req 37: Online processing shall be described based on the necessary mandatory data elements.

3.1.4.2.5.3.1 Online Authorisation

Req 38: If it is not possible to perform an authorisation exchange, the processing shall meet the requirements described in section 4.3.5.3.2.

Req 39: The terminal application shall support Issuer initiated referrals for EMV processing.

Req 40: If the Authorisation Response Code indicates that the online-PIN entered did not verify correctly ("Wrong PIN"), the transaction shall proceed as described in section 4.3.5.4 and there shall be no online PIN re-entry allowed within this transaction.

3.1.4.2.5.3.2 Unable-To-Go-Online Processing

Req 41: Unable-to-go-online processing shall be performed according to [EMV] with the following extension. If the terminal requests an approval, and the card approves the transaction, and the amount exceeds the terminal floor limit, the terminal application shall be configured to either approve the transaction or perform a voice authorisation. This can be set per Payment Profile.

3.1.4.2.5.3.3 Call Referral Process

Req 42: If an Issuer initiated referral is received the transaction shall be completed by requesting an AAC in the second generate AC. The terminal application shall display a message requesting the removal of the card and display the phone number to be called for a voice authorisation. It shall then request an approval code to be manually entered. If an approval code is entered, the transaction shall be approved with the ARQC from the authorisation request used as Application Cryptogram in the transaction record. If an approval code is not entered, the transaction shall be declined, with the AAC from the second Generate AC used as Application Cryptogram in the transaction record.

3.1.4.2.5.4 EMV Completion Actions

The EMV completion actions shall be performed according to [EMV] including generation of the second AC and script processing (if a script is present in the authorisation response).

3.1.4.2.5.5 Transaction Completion Actions

Transaction completion includes logging, receipt printing, capturing and possible reversals.

Req 43: The terminal shall print a transaction receipt for the cardholder if configured in the Payment Profile. The transaction receipt can be combined with the sales receipt.

Req 44: If the transaction (approved, declined or aborted) is not immediately online-captured, it shall be logged in the terminal.

Req 45: At least the minimum set of data elements specified by SEPA-FAST shall be captured or logged.

Req 46: The types of transactions which are to be captured or logged (only approved, declined or aborted) shall be configurable in the Payment Profile.

Req 47: A reversal of an online approved authorisation shall be performed if the transaction is declined or aborted.

Req 48: If the terminal supports more than one method to capture transactions (see section 3.9), then the method of data capture to be used shall be configurable per Payment Profile.

3.1.4.2.5.6 Error-Handing

Req 49: A SCF Standard Terminal Application core requirement shall describe in detailed flows the error handling needed for EMV processing.

3.1.4.2.6 Other Requirements

Req 50: If the terminal is offline with online capability, it shall be possible to configure the terminal application to allow/not allow the attendant to force a transaction online.

Req 51: If the terminal is offline with online capability or online-only, it shall be possible to configure the terminal application to allow/not allow the attendant to force a transaction to be approved.

Req 52: It shall be possible to configure the terminal application to provide alternative CVMs

3.1.4.3 Refund Service

Refund transactions are made when a merchant credits the cardholder, for example when the cardholder returns an item that was purchased previously.

Req 53: The allowed maximum amount of the Refund Service shall be configurable.

3.1.4.3.1 Technology Selection for Refund

Technology Selection is the process of selecting one of the processing modes supported for the current financial service.

Req 54: It shall be possible to configure which of the processing modes supported by the terminal application are allowed for the Refund.

Req 55: It shall be possible to configure the priority of the processing modes.

3.1.4.3.2 Processing

Req 56: Where not explicitly stated otherwise, the Refund shall follow the same process as the Payment Service, but using its own configuration. It is recommended that the Transaction Amount given to the chip during the Refund is zero.

Req 57: The Refund service performed with the chip shall follow EMV processing until 'the read application data' function has obtained either the Track 2 equivalent data or the PAN and expiry date. The chip process shall be terminated by requesting an AAC from the card in the 1st GENERATE AC, i.e. no CVM processing, no Data Authentication, etc are performed.

Req 58: Whether the Refund shall be performed online with the Acquirer or not shall be configurable.

Req 59: The transaction receipt shall show that this is a refund and show the refund amount.

3.1.4.4 Cancellation Service

The Cancellation Service, sometimes called the Manual Reversal Service, is a service which cancels a previously completed transaction, e.g. when the attendant entered a wrong transaction amount, or e.g. when signature is incorrect.

Req 60: It shall be configurable which of the financial services are cancellable.

Req 61: A Cancellation is always performed for the full amount of the original transaction.

Req 62: It shall be possible to configure if Cancellations shall be restricted to the last transaction processed at the terminal or may be extended to any transaction not yet cleared by the Acquirer.

Req 63: A set of data elements uniquely referencing the original transaction shall be defined to be included in every cancellation transaction.

3.1.4.4.1 Technology Selection for Cancellation

Req 64: The same rules as Technology Selection for the Refund Service shall apply to the Cancellation Service.

3.1.4.4.2 Processing

Req 65: Where not explicitly stated otherwise, the Cancellation shall follow the same process as the Refund Service, but using its own configuration.

Req 66: If the original transaction cannot be recognised by the terminal or has been captured, the cancellation transaction shall either be declined or be performed online according to the configuration.

Req 67: The transaction receipt shall show that this is a Cancellation and show the cancelled amount.

3.1.4.5 Hotel and Rental Service

3.1.4.5.1 Pre-Authorisation

Req 68: Where not explicitly stated otherwise, pre-authorisation shall follow the same process as the Payment Service, but using its own configuration.

Req 69: The merchant shall enter an estimated amount which is based on known or expected expenses.

Req 70: The cardholder display shall clearly indicate that the amount is an estimated amount.

Req 71: The terminal shall be configurable to allow the merchant to enter the number of days that this pre-authorisation shall remain valid. If this function is activated, and the merchant skips this entry then a configurable default number of days shall be used.

Req 72: The transaction receipt shall show that this is a pre-authorisation performed and show the estimated amount.

Req 73: A Pre-authorisation shall be online to the issuer in order to reserve the funds.

Req 74: Pre-authorisations approved by the issuer shall not be cleared.

Req 75: Approved pre-authorisations shall be stored for performing subsequent steps (i.e. Update Pre-Authorisation, sale completion), either in the terminal or in a system external to the terminal.

Req 76: It shall be possible to cancel approved pre-authorisations with the Cancellation Service. Approved pre-authorisations shall be cancelled online.

3.1.4.5.2 Update Pre-Authorisation

The Update Pre-Authorisation is used to update the estimated amount and/or update the number of days of the previous pre-authorisation or Update Pre-Authorisation.

Req 77: Where not explicitly stated otherwise, Update Pre-Authorisation shall follow the same process as the pre-authorisation.

Req 78: An Update Pre-Authorisation shall be uniquely linked to the previous preauthorisation (or Update Pre-Authorisation) to which it relates.

Req 79: Update Pre-Authorisations shall only be allowed while the previous preauthorisation (or Update Pre-Authorisation) is still valid.

Req 80: An Update Pre-Authorisation shall include a new estimated amount and/or number of days.

Req 81: The cardholder display shall clearly indicate that the amount is a new estimated amount.

Req 82: The transaction receipt shall show that this is a pre-authorisation performed and show the new estimated amount.

Req 83: If the Update Pre-Authorisation is approved by the issuer, then it shall be stored to replace the previous pre-authorisation (or Update Pre-Authorisation).

Req 84: If the Update Pre-Authorisation is declined by the issuer, then the previous pre-authorisation (or Update Pre-Authorisation) shall remain unchanged.

Req 85: It shall be possible to cancel approved Update Pre-Authorisations with the Cancellation Service. Approved Update Pre-Authorisations shall be cancelled online.

3.1.4.5.3 Payment Completion

Payment Completion uses the previously performed pre-authorisation (or Update Pre-Authorisation) to confirm and complete a payment with the final amount of the sale.

Req 86: Where not explicitly stated otherwise, Payment Completion shall follow the same process as the Payment Service.

Req 87: A Payment Completion shall be uniquely linked to the previous pre-authorisation (or Update Pre-Authorisation) to which it relates.

Req 88: A Payment Completion shall only be allowed while the previous pre-authorisation (or Update Pre-Authorisation) is still valid.

Req 89: A Payment Completion shall include the final amount of the sale.

Req 90: If the final amount of the sale is equal to or below the estimated amount of the previous Pre-Authorisation (or Update Pre-Authorisation), including a configurable overspend percentage, then the chip process shall be terminated by requesting an AAC to the card. The Payment Completion process shall be performed with the chip data from the previous Pre-Authorisation (or Update Pre-Authorisation).

Req 91: If the final amount of the sale is above the estimated amount of the previous Pre-Authorisation (or Update Pre-Authorisation), including a configurable overspend percentage, then the Payment Completion shall follow the same process as the Update Pre-Authorisation. The Payment Completion process shall be performed with the chip data of this Update Pre-Authorisation.

Req 92: The cardholder display shall clearly indicate that the amount is the final sale amount.

Req 93: The transaction receipt shall show that this is a sale and show the final sale amount.

Req 94: It shall be possible to cancel a Payment Completion with the Cancellation Service.

3.1.4.6 Cash Advance on POS Service

Req 95: Where not explicitly stated otherwise, Cash Advance shall follow the same process as the Payment Service, but using its own configuration.

Req 96: The cardholder display shall clearly indicate that this is a cash advance transaction with the cash advance amount.

Req 97: The transaction receipt shall show that this is a cash advance transaction and show the cash advance amount.

3.2 Chapter "Terminal To Acquirer space" Core Requirements

3.2.1 Introduction

This chapter outlines a list of core data requirements for the exchange of information between a Terminal (or a Card Acceptor) and an Acquirer to ensure the proper end-to-end processing of authorisation, financial and management of card related data. Those core requirements are to be viewed as the necessary elements of information to be taken into account in the transposition process towards actual data elements and messages to be further implemented by any interested stakeholder into an Acceptor-to-Acquirer relationship.

The purpose of the proposed material is therefore to address data and messages in terms of core requirements rather than to define those data and messages and their related attributes. The latter process should remain in the hands of the entities in charge of the design and drafting of data and messages which should comply to those requirements.

3.2.2 Definitions of key terms used in this chapter

3.2.2.1 Message Types

The following types of messages should be considered in the design and drafting of messages belonging to the Terminal-to-Acquirer domain:

Request

a message where the sender informs the receiver that a transaction is in progress and an immediate response is required to complete the activity.

Response

a message where the sender informs the receiver that a request or advice message was received

Advice

a message where the sender notifies the receiver of an activity that has been taken, requiring no approval but requiring a response.

Notification

a message where the sender notifies the receiver of an activity taken, not requiring an approval or any response message.

3.2.2.2 Message Classes

Messages used in the Terminal to Acquirer domain can also be classified in the following message classes. The first three message classes (authorisation, financial presentment, reversal) are termed Primary messages throughout this document.

Authorisation

an approval or guarantee of funds given by acquirer to the acceptor

Financial presentment

permits the application of the approved transaction amount to the acceptor and the cardholder's accounts for billing or posting. Includes First Financial Presentment and Second Financial Presentment as well as on-line Financial Presentment Request or Advice in Single Message applications

Reversal

the partial or complete nullification of the effects of a previous financial presentment, financial accumulation presentment or authorisation that cannot be processed as instructed. Includes Authorisation Reversal and Financial Reversal (reversal of Financial Presentments).

Reconciliation

the exchange of totals between two institutions (acceptor, acquirer or their agents) to reach agreement on financial totals.

3.2.2.3 Single and Dual Message Systems

Messages required in the Terminal to Acquirer domain can also be classified as belonging to one of the following message systems:

Single Message System

When the Authorisation and the Financial Presentment are combined in the same message. Such combined (or single) messages are typically exchanged individually (i.e., one message per transaction) and online.

Dual Message System

When the Authorisation and the Financial Presentment are conducted using separate messages. Authorisation messages are typically exchanged individually (i.e., one message per transaction) and online. Financial Presentment messages are typically exchanged in batch covering multiple transactions (batch data capture presentment).

In certain cases, System used in the Terminal to Acquirer domain might be different from the one used in the Acquirer to Issuer domain (e.g. single message system in Terminal to Acquirer domain whilst Dual Message System used in Acquirer to Issuer Domain

3.2.2.4 Online and Batch transmission

Online transmission

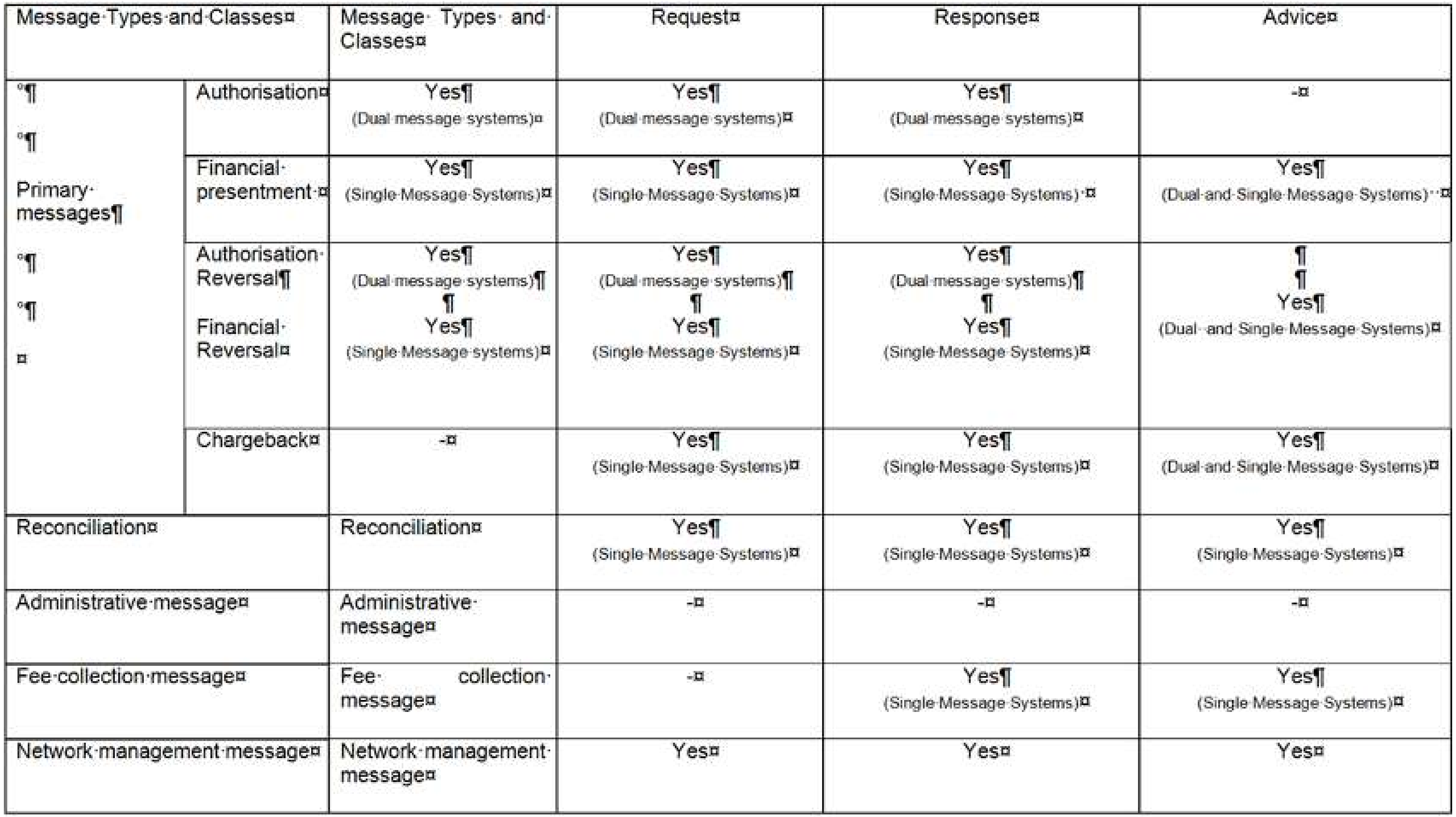
When a transaction is sent individually,

Batch transmission

When multiple transactions are combined in one transmission.

3.2.2.5 *Combined Type and Message Class table*

Messages required in the Terminal to Acquirer domain can belong to a given Message Class as well as to a given Message type. The table below, shows the cases where this is applicable and notes when certain types of messages are typically only used in either Single Message Systems or Dual Message Systems.



Message Types and Classes		Message Types and Classes	Request	Response	Advice
Primary messages	Authorisation	Yes (Dual message systems)	Yes (Dual message systems)	Yes (Dual message systems)	-
	Financial presentment	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
	Authorisation Reversal Financial Reversal	Yes (Dual message systems) Yes (Single Message systems)	Yes (Dual message systems) Yes (Single Message Systems)	Yes (Dual message systems) Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
	Chargeback	-	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
Reconciliation		Reconciliation	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Single Message Systems)
Administrative message		Administrative message	-	-	-
Fee collection message		Fee collection message	-	Yes (Single Message Systems)	Yes (Single Message Systems)
Network management message		Network management message	Yes	Yes	Yes

3.2.3 Core data elements requirements

The table below lists the basic core data elements required in any implementation, in terms of presence, format , usage and values for the Terminal to Acquirer domain. The column Purpose provides additional information about the data element. Cells left blank indicate that no requirements is applicable.

Any additional data elements and messages (types, classes) may be adopted insofar the resulting messages or data definition still take into consideration the necessary core data elements of information defined in the present document.

Specific data elements for specific Payments/Cash/inquiry/… Services not listed as core may also be used.

Data Element Name	Presence	Purpose	Format	Usage and values
Message ID	Mandatory	Identifies the message (type and class)		
Primary account number	Mandatory for Authorisations and Financial Presentments	Identifies Cardholder accounts and allows the issuer to post a transaction	Must be LLvar n…19	
Processing code	Mandatory	Differentiates cash withdrawal, payments, balance inquiry, refunds, debit, credit, source and destination account for transfers etc...	Must be n6	
Amount transaction	Mandatory for all Messages except for inquiry services (Balance inquiry, verification service, etc..)	Identifies the amount of the message in the transaction currency minor unit	Must be n12	Must include the minor unit without decimal point or comma.
Currency code amount transaction	Mandatory when Amount transaction is present	Identifies the currency used at the POI	Must be n3	Must comply with ISO 4217. Can be any value for authorisations not relating to payment or cash services.

Data Element Name	Presence	Purpose	Format	Usage and values
Amount reconciliation	Mandatory in Financial Presentments, Financial Reversals when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the amount of the message in the reconciliation currency minor unit	Must be n12	Must include the minor unit without decimal point or comma.
Currency code amount reconciliation	Mandatory in Financial Presentments, Financial Reversals when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the currency used for reconciliation.	Must be n3	Must comply with ISO 4217
Conversion Rate reconciliation	Mandatory in Financial Presentments, Financial Reversals when reconciliation currency differs from transaction currency. Note: Can be populated either by the Acquirer or a switching network	Permits to convert from transaction to reconciliation amount	Must be n8	The leftmost digit denotes the number of positions the decimal separator shall be moved from the right. Digits 2-8 define the conversion rate without decimal separator.
Systems trace audit number	Mandatory in Requests, Advices and their Responses. Also mandatory for Notifications if these are sent online.	Identifies the transaction at the Acquirer level	Must be n6	Note: Schemes may have specific requirements for values. For example this value must be unique when combined with Acquirer ID per day (UTC)]

Data Element Name	Presence	Purpose	Format	Usage and values
Date and time local transaction	Mandatory for all message types except for Authorisation Reversals	Shows the local date and time at the POI	For Authorisations must include MMDDHHmm as minimum.	
Expiration Date	Mandatory in Requests and Advices for manual entry transactions	Shows the expiration date when track data is not available	Must be n4 (YYMM)	
Point of service capability	Mandatory for all Messages with the exception of Authorisation Responses and Reversals. Note: Can be populated either by the Terminal or by the acquirer.	Permits to identify the terminal capability and then which operational rules apply		
Point of service data code	Mandatory for all Messages with the exception of Authorisation Responses and Reversals.	Permits to know the way the transaction was performed and then which operational rules apply		
Card sequence number	Mandatory in EMV-compliant ICC Requests and Advices when this information is available.	Gives the Issuer information about the specific plastic card in use	Must be n3	
Function code	Mandatory for Financial Presentments, Financial Reversals.	Differentiates first and second presentment. When used in Authorisation, differentiates authorisation, preauthorisation and full or partial reversal.		

Data Element Name	Presence	Purpose	Format	Usage and values
Message reason code	Mandatory for Advices and Notifications. except for first presentments.	Shows the reason for sending the message.		Depending on implementations this data may be derived implicitly from several data fields on the message
Merchant category code (or Card Acceptor Business Code)	Mandatory for Requests, Advices and Notifications, except for Reversals.	Identifies the sector in which the merchant/card acceptor operates and then which operational rules apply	Must be n4	
Amounts original	Mandatory for Authorisation Responses when the amount differs from the original one. The Original reconciliation amount is mandatory only in Single Message Systems and when a reconciliation amount was used in the original message.	Permits to keep the original amount.	Original amount transaction: n12 Original reconciliation amount: n12	
Acquiring institution identification code	Mandatory	Identifies the Acquirer Institution	Must be numeric with maximum 11 digits	Note: The value can be scheme dependent
Electronic payment data	Mandatory for Authorisations and Financial Presentments Requests of e-payment transactions.	Shows the issuer the cardholder authentication data and e-payment specific data		Note: The value can be scheme dependent
Track 2 data	Mandatory for Requests, when available, from magnetic stripe or ICC	Identifies Cardholder accounts and some security or operational information	Must be LLVAR z..37	

Data Element Name	Presence	Purpose	Format	Usage and values
Approval code	Mandatory in Authorisation and Financial Presentment Responses when approved and in Financial Presentment advices and notifications when the transaction has an approved online Authorisation.		Must be 6 characters and must allow at least "an" (alphanumeric)	
Action / Response code	Mandatory in Responses and Advices excluding reversal advices	Shows the transaction result		
Card acceptor terminal identification	Mandatory in Requests, Advices and Notifications. except for key entry and Card Not Present transactions. Not mandatory for reversals.	Identifies the terminal within the merchant/card acceptor	Must be Ans8	
Card acceptor identification code	Mandatory in Requests, Advices and Notifications. Not mandatory for reversals.	Identifies the merchant/card acceptor within the acquirer.	Must be Ans15	
Card acceptor name/location	Mandatory in Requests, Advices and Notifications. Not mandatory for reversals	Permits the issuer to include this information in the cardholder statement	Must include Country code and card acceptor name.	
Personal identification number (PIN) data	Mandatory in Authorisation Requests and Financial Presentment Requests when PIN online is used	Permits the Issuer or its agent to validate PIN	Must be b8	

Data Element Name	Presence	Purpose	Format	Usage and values
Security related control information	Mandatory in Authorisation Requests and Financial Presentment Requests when PIN online or MAC is used	Shows security parameters to be used for cryptographic purposes		
Integrated circuit card (ICC) related data	Mandatory in Requests and Advices when EMV information is used to populate the card data in the message.	Permits the Issuer or its agent and the card to deal with specific EMV data	Must be b…255 (LLLVAR)	
Security Code	Mandatory in Requests in a card-not -present transactions	Issuer generated Security Code typically from back or front of the card	Scheme dependent	
Original Data Elements	Mandatory for Authorisation Reversals	Helps to match the original related transaction	Scheme dependant	Note: Schemes may have specific requirements for usage and values
POI component	Mandatory in authorisation request and financial presentment	Gives information about the POI such as manufacturer ID, version number, model,…		
Forcing indicator	Mandatory in financial presentment for an online transaction	Indicates if the merchant has forced the transaction to be accepted without the approval of the issuer or the acquirer		

3.3 Chapter "Acquirer To Issuer space" Core Requirements

3.3.1 Introduction

This document lists the Core Data Elements for the Acquirer to Issuer domain.

The interface between the acquirer and the issuer has traditionally been based on the ISO 8583 standard. This standard allows fields to be used for national and proprietary purposes. National and international schemes have defined their own specific, mandatory requirements for the authorisation and settlement domains, for which some schemes also claim intellectual property rights.

The absence of a single standard does not limit interoperability, nor constrains the implementation of the SCF for merchants and cardholders. However, in order to assess future convergence, the EPC Acquirer to Issuer Expert Group is proposing a set of core data elements that should be used in every implementation interface between the acquirer and the issuer.

3.3.2 Definitions of key terms used in this chapter

3.3.2.1.1 Message Types

Messages used in the Acquirer to Issuer domain can be classified in the following message types:

Request

a message where the sender informs the receiver that a transaction is in progress and an immediate response is required to complete the activity.

Response

a message where the sender informs the receiver that a request or advice message was received

Advice

a message where the sender notifies the receiver of an activity that has been taken, requiring no approval but requiring a response.

Notification

a message where the sender notifies the receiver of an activity taken, not requiring an approval or any response message.

3.3.2.1.2 Message Classes

Messages used in the Acquirer to Issuer domain can also be classified in the following message classes. The first four message classes (authorisation, financial presentment, reversal, and charge-backs) are termed **Primary Messages** throughout this document.

Authorisation

an approval or guarantee of funds given by the card issuer to the acquirer

Financial presentment

permits the application of the approved transaction amount to the cardholder's account for billing or posting. Includes First Financial Presentment and Second Financial Presentment as well as on-line Financial Presentment Request or Advice in Single Message applications

Reversal

the partial or complete nullification of the effects of a previous financial presentment, financial accumulation presentment or authorisation that cannot be processed as instructed. Includes Authorisation Reversal and Financial Reversal (reversal of Financial Presentments).

Chargeback

the partial or complete nullification of a previous financial presentment or financial accumulation presentment when the card issuer determines that a customer dispute exists, or that an error or a violation of rules has been committed.

Reconciliation

the exchange of totals between two institutions (acquirer, card issuer or their agents) to reach agreement on financial totals.

Administrative message

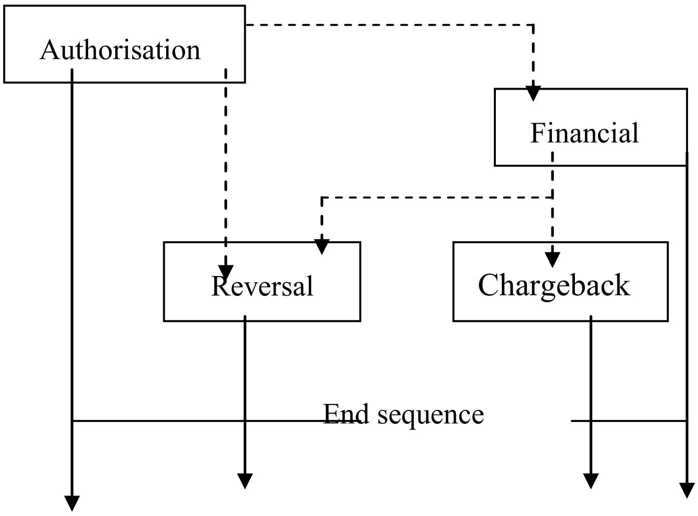
Administrative activity is anything that supports the business and technical infrastructure between financial institutions and their agents. For example Retrieval and Retrieval Fulfilment, rejection messages, etc…

Fee collection message

Fee collection is the activity which supports the collection and disburse of miscellaneous service fees between financial institutions.

Network management message

Network management is the range of activities carried out to control the system security and operating condition of the interchange network and may be initiated by any interchanging party.



EXAMPLES PRIMARY MESSAGE TRANSACTION FLOWS

3.3.2.1.3 Single and Dual Message Systems

Messages used in the Acquirer to Issuer domain can also be classified as belonging to one of the following message systems:

Single Message System

When the Authorisation and the Financial Presentment are combined in the same message. Such combined (or single) messages are typically exchanged individually (i.e., one message per transaction) and online.

Dual Message System

When the Authorisation and the Financial Presentment are conducted using separate messages. Authorisation messages are typically exchanged individually (i.e., one message per transaction) and online. Financial Presentment messages are typically exchanged in batch covering multiple transactions.

3.3.2.1.4 Online and Batch transmission

Online transmission

When a transaction is sent individually,

Batch transmission

When multiple transactions are combined in one transmission.

3.3.2.1.5 Combined Type and Message Class table

Message Types and Classes		Request	Response	Advice	Notification
Primary messages	Authorisation	Yes (Dual message systems)	Yes (Dual message systems)	Yes (Dual message systems)	-
	Financial presentment	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
	Authorisation Reversal	Yes (Dual message systems)	Yes (Dual message systems)	Yes (Dual message systems)	Yes (Dual and Single Message Systems)
	Financial Reversal	Yes (Single Message systems)	Yes (Single Message Systems)	Yes (Single Message Systems)	
	Chargeback	-	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
Reconciliation		Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
Administrative message		-	-	-	Yes
Fee collection message		-	Yes (Single Message Systems)	Yes (Single Message Systems)	Yes (Dual and Single Message Systems)
Network management message		Yes	Yes	Yes	Yes

3.3.3 Core data elements requirements

The table below lists the core data elements in terms of presence, format and usage and values for the Acquirer to Issuer domain. The column Purpose provides additional information about the data element. Cells left blank indicate that no requirement is applicable.

Data elements not listed as core data elements may also be used and those core data elements listed may also be used in additional message classes/types.

3.3.3.1 Core data elements requirements for Primary Messages

Data Element Name	Presence	Purpose	Format	Usage and values
Message ID	Mandatory	Identifies the message (type and class)		
Primary account number	Mandatory for Authorisations and Financial Presentments	Identifies Cardholder accounts and allows the issuer to post a transaction	Must be LLvar n…19	
Processing code	Mandatory	Differentiates cash withdrawal, payments, balance inquiry, refunds, debit, credit, source and destination account for transfers etc...	Must be n6	
Amount transaction	Mandatory for all Messages except for inquiry services (Balance inquiry, verification service, etc..)	Identifies the amount of the message in the transaction currency minor unit	Must be n12	Must include the minor unit without decimal point or comma.
Currency code amount transaction	Mandatory when Amount transaction is present	Identifies the currency used at the POI	Must be n3	Must comply with ISO 4217. Can be any value for authorisations not relating to payment or cash services.

Data Element Name	Presence	Purpose	Format	Usage and values
Amount reconciliation	Mandatory in Financial Presentments, Financial Reversals and Chargebacks when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the amount of the message in the reconciliation currency minor unit	Must be n12	Must include the minor unit without decimal point or comma.
Currency code amount reconciliation	Mandatory in Financial Presentments, Financial Reversals and Chargebacks when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the currency used for reconciliation.	Must be n3	Must comply with ISO 4217
Amount Cardholder Billing	Mandatory in Authorisations and Authorisation Reversals when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the amount of the message in the reconciliation currency minor unit	Must be n12	Includes the minor unit without decimal point or comma.

Data Element Name	Presence	Purpose	Format	Usage and values
Currency code Cardholder Billing	Mandatory in Authorisations and Authorisation Reversals when reconciliation currency differs from transaction currency. Note: Can be populated either by the switching network or the acquirer.	Identifies the currency used for reconciliation.	Must be n3	Must comply with ISO 4217
Date and time transmission	Mandatory in Requests, Advices and their Responses. Also mandatory for online notifications in Single Messages Systems	Permits to differentiate from Date and time local transaction	Must be n10 (MMDDhhmmss)	Time zone must be in UTC/GMT
Conversion Rate reconciliation	Mandatory in Financial Presentments, Financial Reversals and Chargebacks when reconciliation currency differs from transaction currency. Note: Can be populated either by the Acquirer or a switching network	Permits to convert from transaction to reconciliation amount	Must be n8	The leftmost digit denotes the number of positions the decimal separator shall be moved from the right. Digits 2-8 define the conversion rate without decimal separator.
Conversion Rate Cardholder billing	Mandatory in Authorisations and Authorisation Reversals when reconciliation currency differs from transaction currency. Note: can be populated either by the switching network or the acquirer.	Permits to convert from transaction currency to reconciliation currency	Must be n8	The leftmost digit denotes the number of positions the decimal separator shall be moved from the right. Digits 2-8 define the conversion rate without decimal separator.

Data Element Name	Presence	Purpose	Format	Usage and values
Systems trace audit number	Mandatory in Requests, Advices and their Responses. Also mandatory for Notifications if these are sent online.	Identifies the transaction at the Acquirer level	Must be n6	Note: Schemes may have specific requirements for values. For example this value must be unique when combined with Acquirer ID per day (UTC)]
Date and time local transaction	Mandatory for all message types except for key entry and Card Not Present Authorisations and Authorisation Reversals	Shows the local date and time at the POI	For Authorisations must include MMDDHHmm as minimum.	
Expiration Date	Mandatory in Requests and Advices for manual entry transactions	Shows the expiration date when track data is not available	Must be n4 (YYMM)	
Point of service capability	Mandatory for all Messages with the exception of Authorisation Responses and Reversals.	Permits to identify the terminal capability and then which operational rules apply		
Point of service data code	Mandatory for all Messages with the exception of Authorisation Responses and Reversals.	Permits to know the way the transaction was performed and then which operational rules apply		
Card sequence number	Mandatory in EMV-compliant ICC Requests and Advices when this information is available.	Gives the Issuer information about the specific plastic card in use	Must be n3	
Function code	Mandatory for Financial Presentments, Financial Reversals and Chargebacks.	Differentiates first and second presentment, full or partial chargebacks . When used in Authorisation, differentiates authorisation, preauthorisation and full or partial reversal.		

Data Element Name	Presence	Purpose	Format	Usage and values
Message reason code	Mandatory for Advices and Notifications. except for first presentments.	Shows the reason for sending the message.		Depending on implementations this data may be derived implicitly from several data fields on the message
Merchant category code (or Card Acceptor Business Code)	Mandatory for Requests, Advices and Notifications, except for Reversals.	Identifies the sector in which the merchant/card acceptor operates and then which operational rules apply	Must be n4	
Date reconciliation	Mandatory in Financial Presentments, Financial Reversals, Chargebacks. Note: Can be populated either by the switching network or the acquirer.	Groups all the financial transactions for a reconciliation.	Must include MMDD as minimum	May be included only once for batch transmissions instead of every message
Reconciliation Indicator	Mandatory in Financial Presentments, Financial Reversals and Chargebacks when more than one reconciliation per day is performed. Note: Can be populated either by the switching network or the acquirer.	Groups all the financial transactions for a reconciliation within the same day.		May be included only once for batch transmissions instead of every message

Data Element Name	Presence	Purpose	Format	Usage and values
Amounts original	Mandatory for Authorisation Responses and Chargebacks when the amount differs from the original one. The Original reconciliation amount is mandatory only in Single Message Systems and when a reconciliation amount was used in the original message.	Permits to keep the original amount.	Original amount transaction: n12 Original reconciliation amount: n12	
Acquiring institution identification code	Mandatory	Identifies the Acquirer Institution	Must be numeric with maximum 11 digits	Note: The value can be scheme dependent
Forwarding institution identification code	Mandatory for all Messages when different from Acquirer Institution	Identifies the sender processor.	Must be numeric with maximum of 11 digits	Note: The value can be scheme dependent
Electronic commerce data	Mandatory for Authorisations and Financial Presentments Requests of e-commerce transactions.	Shows the issuer the cardholder authentication data and e-commerce specific data		Note: The value can be scheme dependent
Track 2 data	Mandatory for Requests, when available, from magnetic stripe or ICC	Identifies Cardholder accounts and some security or operational information	Must be LLVAR z..37	
Approval code	Mandatory in Authorisation and Financial Presentment Responses when approved and in Financial Presentment advices and notifications when the transaction has an approved online Authorisation.		Must be 6 characters and must allow at least "an" (alphanumeric)	

Data Element Name	Presence	Purpose	Format	Usage and values
Action / Response code	Mandatory in Responses and Advices excluding reversal advices	Shows the transaction result		
Card acceptor terminal identification	Mandatory in Requests, Advices and Notifications. except for key entry and Card Not Present transactions. Not mandatory for reversals nor for chargebacks.	Identifies the terminal within the merchant/card acceptor	Must be Ans8	
Card acceptor identification code	Mandatory in Requests, Advices and Notifications. Not mandatory for reversals nor for ATM Transactions.	Identifies the merchant/card acceptor within the acquirer.	Must be Ans15	
Card acceptor name/location	Mandatory in Requests, Advices and Notifications. Not mandatory for reversals	Permits the issuer to include this information in the cardholder statement	Must include Country code and card acceptor name.	
Personal identification number (PIN) data	Mandatory in Authorisation Requests and Financial Presentment Requests when PIN online is used	Permits the Issuer or its agent to validate PIN	Must be b8	
Security related control information	Mandatory in Authorisation Requests and Financial Presentment Requests when PIN online or MAC is used	Shows security parameters to be used for cryptographic purposes		

Data Element Name	Presence	Purpose	Format	Usage and values
Integrated circuit card (ICC) related data	Mandatory in Requests and Advices when EMV information is used to populate the card data in the message.	Permits the Issuer or its agent and the card to deal with specific EMV data	Must be b…255 (LLLVAR)	
Security Code	Mandatory in Requests in a card-not -present transactions	Issuer generated Security Code typically from back or front of the card	Scheme dependent	
Original Data Elements	Mandatory for Authorisation Reversals	Helps to match the original related transaction	Scheme dependant	Note: Schemes may have specific requirements for usage and values

3.3.3.2 Core data elements requirements for Reconciliation Messages

Data Element Name	Presence	Purpose	Format	Usage and values
Date and time transmission	Mandatory in Requests, Advices and their Responses. Also mandatory for online notifications in Single Messages Systems	This field indicates date and time that this message is transmitted.	Must be n10 (MMDDhhmmss)	Time zone in UTC/GMT
System Trace audit number	Mandatory in Requests, Advices and their Responses. Also mandatory for Notifications if these are sent online.	Identifies the transaction at the Acquirer level	Must be n6	
Function code	Mandatory for requests, advices and notifications.	Differentiates from final and check point Reconciliation		

Data Element Name	Presence	Purpose	Format	Usage and values
Date reconciliation	Mandatory	Date for which financial totals are reconciled between the sender and the receiver	Must include MMDD as minimum	May be included only once for batch transmissions instead of every message
Reconciliation Indicator	Mandatory when more than one reconciliation per day is performed.	Identify a period time for reconciliation within the same day.		May be included only once for batch transmissions instead of every message
Sending institution identification code	Mandatory except for messages generated by a switching network	Identifies the sender institution.	Must be numeric with maximum of 11 digits	The value can be scheme dependent
Action / Response code	Mandatory in responses	Shows the transaction result		
Amount net reconciliation	Mandatory.	The net reconciliation amount including fees when applicable.	X+n 16. The value must be the sign "C" (positive result) or "D", (negative result) followed by amount net reconciliation (16 digits)	
Currency code amount reconciliation	Mandatory	Identifies the currency used for reconciliation	Must be n3	Must comply with ISO 4217.
Receiving institution identification code	Mandatory	Identifies the receiver institution.	Must be numeric with maximum of 11 digits	The value can be scheme dependent

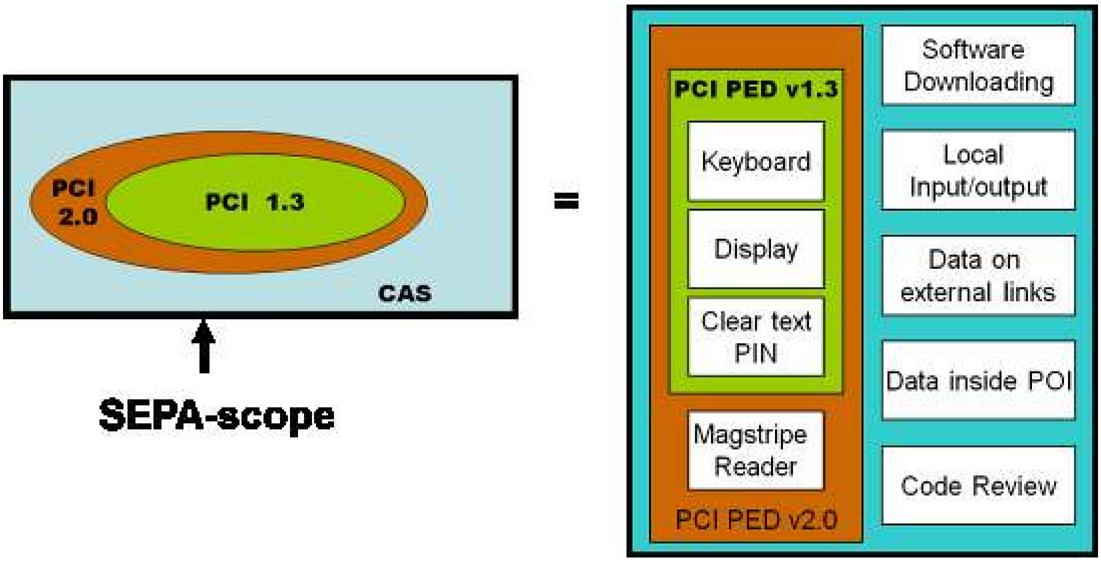
4 SECURITY REQUIREMENTS

In this area at least one European initiative has been providing input into standardisation work at global level. Going forward – beyond and above the direction of that work – decisions will have to be made concerning the governance of the input provided by European parties.

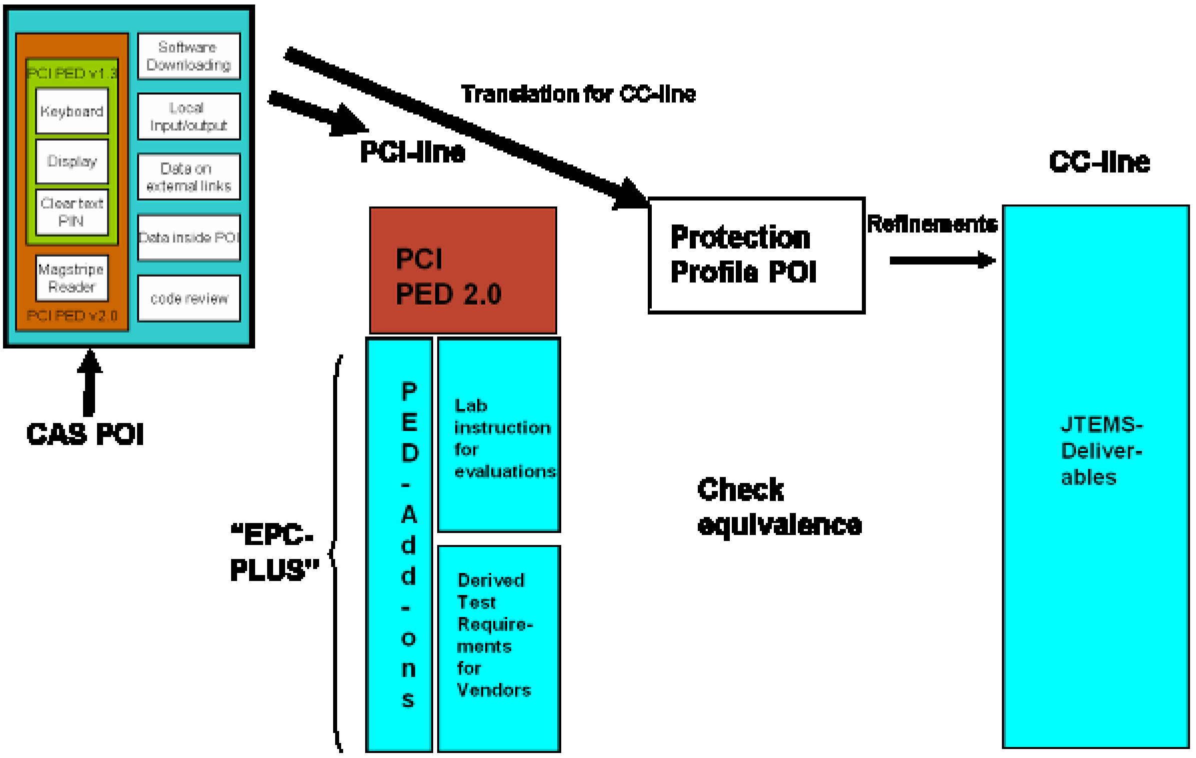
4.1 Terminal Security Requirements

SEPA for terminals has a broader scope than PCI-PED

- PCI PED 2.0 is endorsed by EPC CWG as baseline for SEPA requirements as input to the EPC Framework of Core requirements.
- EPC Additions to PCI PED - driven by CAS requirements - will be included in the Framework.



Adjustment of SEPA requirements to PCI and CC methodology



4.1.1 Reference

CAS Common Approval Scheme - Version 0.1 28 April 2008

4.1.2 Introduction

CAS is a European initiative to harmonize security, certification and approval requirements, methods and a governance framework. At its founding workshop of 31 January, 2007, the EPC identified CAS as the initiative which can help to cover the standardization activities of certification principles and terminal certification targeting at a mutual recognition of type approval (chapter 3.6.3.2 and 3.6.3.3 of the SEPA Cards Framework, version 2.0).

Following CAS deliverables are identified:

- D1 Common SCF compliant security requirements for cards and terminals
- D2 Common SCF compliant evaluation methodology for cards and terminals,
- D3 Common SCF compliant certification and approval framework for cards and terminals.

In the following contents and targets of these D1 and D3 deliverables will be described.

4.1.3 Common SCF Compliant Security Requirements for Terminals (D1)

CAS' work is basically founded on the conviction, not to re-invent the wheel, but to let the stakeholders, e.g. the credit industry and the manufacturers, benefit from existing industry standards. As today numerous industry standards are mandated by different payment schemes, for security of terminals the PED Requirements of PCI SCC are relevant.

Following the EPC policy to build a list of "recommended core requirements" CAS had the task to find an harmonized approach for both:

- As the PCI PED requirements represent a very well defined set of security requirements for the protection of the PIN at PEDs CAS accepted the current version 2.0 as being the base part of the "recommended core requirements". For some of these requirements CAS defined some refinements for clarification.
- Beyond the PCI POS PED requirements on PIN protection further requirements were defined, which come as PLUS requirements of the European credit industry, building the second part to the "recommended core requirements"..

There are several reasons for the need of the PLUS requirements. First, CAS defined the POI as the object of evaluation. A POI is a system for accepting card transactions. At minimum the POI must have one payment application allowing cardholders to perform IC card based payment transactions with PIN as cardholder authentication method. In this context, the PED – covered by PCI POS PED - can be seen as a POI component. Second, CAS contributes value to the whole life cycle of the POI. Third, CAS' aim is to protect assets beyond PIN as been common practice in Europe until today and form the basis for the European credit industries' risk management. An example of such an asset is the integrity of transaction data (for example, transaction amount).

Thus CAS defined the PCI POS PED and the PLUS requirements as the "Recommended core requirements" of the EPC. This harmonized set of POI security requirements are proposed to be endorsed by the EPC as the recommended future SEPA Terminal security requirements. As a result, Europe will be provided with a harmonized set of POI security requirements for SEPA.

In next sub-paragraphs these requirements will be described in more detail.

4.1.3.1 Refinements of PCI POS PED requirements (PLUS requirements)

CAS accepted the PCI PED 2.0 version of requirements as one part of the Recommended CORE requirements. However, some amendments were made by CAS. These amendments can be seen as refinements, as PLUS requirements, stronger then the PCI PED requirements. So if a terminal will be evaluated against these CAS refinements, the terminal will pass PCI PED as well.

Following refinements (PLUS requirements) were agreed by CAS:

1 Regarding PED A9: The PED must provide privacy shield according to [EPC Shield]. The acquirer is the responsible party to assure, that the installation of the PED is according to the requirements defined by the EPC.

2. Regarding PED B3: The review must be performed by a testing laboratory.
3. Regarding PED B6: If the PIN (offline or online) needs to be encrypted, it shall be encrypted immediately.
4. Regarding PED B10: The PED has characteristics that prevent use of the device for exhaustive PIN determination.

Since the scope of CAS work is POI rather than PED and since life-cycle of POI is an explicit item within CAS, following refinements (PLUS requirements) were made.

1. Regarding the PED E and F requirements: in addition to all PED requirements, equivalent requirements are defined for POI security components. A POI security component is defined as any component that provides security protections needed to comply with the PCI POS PED and PLUS requirements.
2. Regarding PED E3: The vendor shall confirm compliance to PED E3 and the equivalent POI requirement by giving an integration statement.
3. The developer of the POI must document all physical, procedural, personnel and other security measures that are necessary to protect the integrity of the POI in its development environment. A site inspection by an independent auditor must confirm this.
4. Production of POI must take place in a secure environment. A site inspection must confirm this.
5. Each PED must be uniquely identifiable.
6. The manufacturer of the POI must provide guidelines for usage. Also means for recording the life-cycle of the POI must be provided.

4.1.3.2 Additional PLUS requirements

Due to protection of assets beyond PIN, CAS formulated additional PLUS requirements. Following PLUS requirements were defined, please note that the exact wording of these PLUS requirements is still under discussion.

- The POI shall provide means to protect all transaction/management data sent or received by the POI over external lines against modification and disclosure by cryptographic mechanisms.
- The POI shall provide means for authentication of its unique identifier by an external entity.
- If the POI implements software updates, the POI must verify the integrity and authenticity of the software. If not confirmed, the software update is rejected or all secret keys are erased.
- The transaction/accounting data shall be handled authentic and integer during processing and capture in the POI.
- The POI must be designed to protect the cardholder against deception about the normal sequence of transaction steps.
- The security of processing cards must not be influenced or affected by the processing of cards relating to other card schemes.

4.1.4 Common SCF compliant evaluation methodology for terminals (D2)

In this chapter it is described, which criteria are relevant from a CAS point of view for choosing an SCF compliant evaluation methodology and explains the status of CAS' work.

The methodology used to verify that the security requirements are implemented appropriately is as important as the requirements themselves. Proven methodology, transparency, accreditation of evaluation labs and cost efficiency are important aspects of an evaluation methodology. For years, cards are evaluated with the Common Criteria methodology. This is well and widely accepted by both the bankers and the chip manufacturers. For POI, there is no such agreement on a methodology. Thus, CAS has to choose an appropriate methodology or a set of methodologies for SEPA.

Two types of methodologies can be foreseen at this point.

- The PCI methodology: CAS would rely on the PCI POS PED evaluation methodology, developed and maintained by PCI SSC. In addition, CAS would have to provide test requirements and test procedures for the refined PCI POS PED requirements and the additional PLUS requirements, both identified as necessary to fulfil the SEPA needs.
- The CC methodology: CAS would use as much as possible the CC scheme including its evaluation methodology described as ISO 15 408. CAS could reuse the test methodology (CEM), the accreditation from CC bodies and the CC certification. CAS therefore cooperates with the European CC bodies to verify and evaluate whether the CC methodology can be implemented for terminals within SEPA. An important step is the establishment of the JIL Terminal Evaluation Methodology Subgroup JTEMS. JTEMS tasks are the definition of attack potential tables, of attack methods and of guidance for the application of CC to POI's. JTEMS directly reports to the JIL group of the CC bodies.

Currently, both methods are worked out. No decision is taken yet in favour of the PCI or the CC methodology as both will emerge over time.

CAS therefore works on an evolutionary process targeting at a harmonized future approach, which can be described as follows:

- Easy Entry solution step 1: The methodology used by PCI SSC is in place together with several appropriate methodologies used by European certification schemes and the first CC evaluations limited to the PED. Mutual recognition of certificates is already in place between these types of methodologies on a bilateral basis. All types of methodologies will emerge or converge due to the parallel CAS standardization process for SEPA.

- Easy Entry solution step 2: PCI SSC will be enhanced due to the PLUS requirements and the parallel harmonization process evolved by CAS; the CC evaluations start to benefit from JTEMS and thus are enhanced for an updated enhanced SEPA solution. Regional methodologies are migrated depending on the growing quality of "enhanced PCI" and "enhanced CC".

- Target solution: Due to the harmonization efforts of step 1 and 2 a SEPA methodology will be defined.

4.2 (Chip) Card certification

4.2.1 Reference

CAS Common Approval Scheme - Version: 0.9 - Management overview

Guidance on writing a Security Target for a Smartcard Embedded Payment Application

4.2.2 Introduction

This guidance document contains payment scheme's security requirements for a payment application embedded in a smartcard.

It is intended for use in a payment scheme's approval process whose purpose is to provide confidence in a smartcard product. In that process, the Security Target against which the Embedded Payment Application (EPA) is to be evaluated is checked by the payment scheme for conformance to the security requirements. The present document provides guidance for writing such a security target. Its format is similar to that of a security target according to Common Criteria (CC). It is intended to be used as part of a regular CC evaluation involving an evaluation laboratory accredited by a CC-recognised Certification Body. The Target of Evaluation (TOE) is the Embedded Payment Application, at cardholder use phase, including all hardware or software parts of the smartcard needed to perform functionality or enforce security.

4.2.3 Finance Industry needs addressed

This document addresses straightforward Finance Industry needs since it is aimed at smartcard embedded payment applications. EPA functionality targets (but is not restricted to) EMV specifications, which provide a basis for global development of highly secure payment systems, and are endorsed by more and more countries, including those already familiar with banking smartcard environment. CAS guidance is readily available for those seeking highly resistant cards, and as such is endorsed by major smartcard payment schemes in the SEPA.

4.2.4 CAS Guidance Overview

The purpose of this document is to identify minimum security requirements requested by CAS members for a Smartcard Embedded Payment Application (EPA).

Requirements are expressed under the formalism of Common Criteria as a product-independent Guidance document which is to be used by smartcard and application developers for writing product-dependent Security Targets compliant with CAS requirements. A primary goal for this document is that related evaluation reports are able to provide card issuers with the right level of information needed to assess the resulting risks for their schemes.

The Target Of Evaluation (TOE) is an on-card payment application at cardholder user phase, possibly with other co-embedded applications. All parts of the card needed to perform EPA functionality, from application level to IC hardware, fall within the scope of the TOE.

The set of assurance requirements is the widely used EAL4+ assurance package, namely EAL4 plus three augmentations (as per Common Criteria v2.3 final revision) :

-	ADV_IMP.2	*Implementation of the TSF*
-	ALC_DVS.2	*Sufficiency of security measures*
-	AVA_VLA.4	*Highly Resistant*

Assurance requirements are split in two packages, one for the TOE itself and one for its development environment, allowing for separate package assessment. However, both assessments must be combined in order to fulfil the whole set of CAS assurance requirements.

NB. The ongoing transposition of CAS Guidance to CC v3.1 seeks an equivalent EAL4+ level, when AVA_VLA.4 of CC v2.3 is accordingly replaced by AVA_VAN.5 of CC v3.1.

4.2.5 Security Problem Definition - A Scheme's Point of View

To perform his approval process, the Risk Management of a Payment Scheme requires that potential vulnerabilities brought up by the evaluation be expressed in terms of assets, threats and security objectives that are meaningful for the Payment Scheme. Therefore, all such items are connected with how the smartcard contributes to the security of the Scheme.

In a typical transaction, the EPA interacts with the Card Reader to:

- authenticate the cardholder ;
- perform internal risk management using transaction data provided by terminal (either off-line on behalf of the issuer, or on-line with access to issuer's authorisation server) ;
- certify transaction data through a Transaction Certificate.

In the example of a debit transaction, when the transaction is approved and certified, the merchant delivers the corresponding goods/services to the customer, then the merchant is credited and the cardholder account is debited. So in the highest sense, a smartcard payment transaction qualifies a merchant trading goods for a promise of payment, on the evidence of a transaction certificate.

In this respect, the main contribution of a smartcard to transaction security is its ability to *authenticate the transaction* by providing undisputed evidence of its terms, by means of the certified transaction data. Such evidence opposes possible fraud cases along the payment chain.

Two main categories of fraud are to be considered :

- *Transaction denial*, in which the fraudster denies either participation to a transaction or the terms of a transaction ;
- *Transaction forgery*, in which the fraudster introduces undue transaction data in the payment scheme.

⇨ Transaction denial may be further subdivided into:

- *Transaction repudiation*, when the fraudster denies participation to a transaction. Certified transaction data, accessible to all parties, act as evidence against such repudiation.
- *Transaction dispute*, when the fraudster denies the terms of the transaction. Certified transaction data, accessible to all parties, act as evidence for the transaction terms, provided they couldn't have been manipulated inside the card in the process of certificate issuance.

⇨ Transaction forgery may be further subdivided into:

- *Transaction replay,* when a genuine transaction is re-issued several times, with possible modification of non-certified transaction data such as merchant ID.

  To protect against transaction replay, the card ensures that different transactions result in different certificates by using transaction diversification data such as the Application Transaction Counter (ATC).
- *Transaction falsification*, when some of the data of one or several genuine transactions (e.g. authentication results, certificates) are re-used to fake a new, seemingly valid, one.

  The card provides protection through cohesion mechanisms ensuring that no transaction parts can be re-used as parts of other transactions. Typical cohesion mechanisms may include the binding of the sequence of commands within a transaction by use of a secured State Machine, or the binding of cryptograms for a given transaction (e.g. Combined DDA and Application Cryptograms in an EMV environment).
- *Transaction counterfeiting,* when the fraudster gains information about the secrets used by a card for its authentication and signature mechanisms (i.e. cryptographic keys), and then uses this information to emulate a genuine card.

  The card provides protection by defending its keys against disclosure, and by implementing algorithms that can't be defeated by observation of their results and their processing.
- *Identity usurpation*, when an attacker unduly gains the rights of a genuine actor (cardholder, merchant, acquirer, issuer...).

> The smartcard can provide protection against cardholder and issuer rights usurpation, through cardholder verification (e.g. PIN authentication), secure channel for card parameters update (script processing) and internal protection of issuer and cardholder data inside the card.

The technical sections of the CAS Guidance document elaborate on security features required for the EPA in order to perform its role in the security of a payment scheme as outlined above.

4.2.6 Intended Use

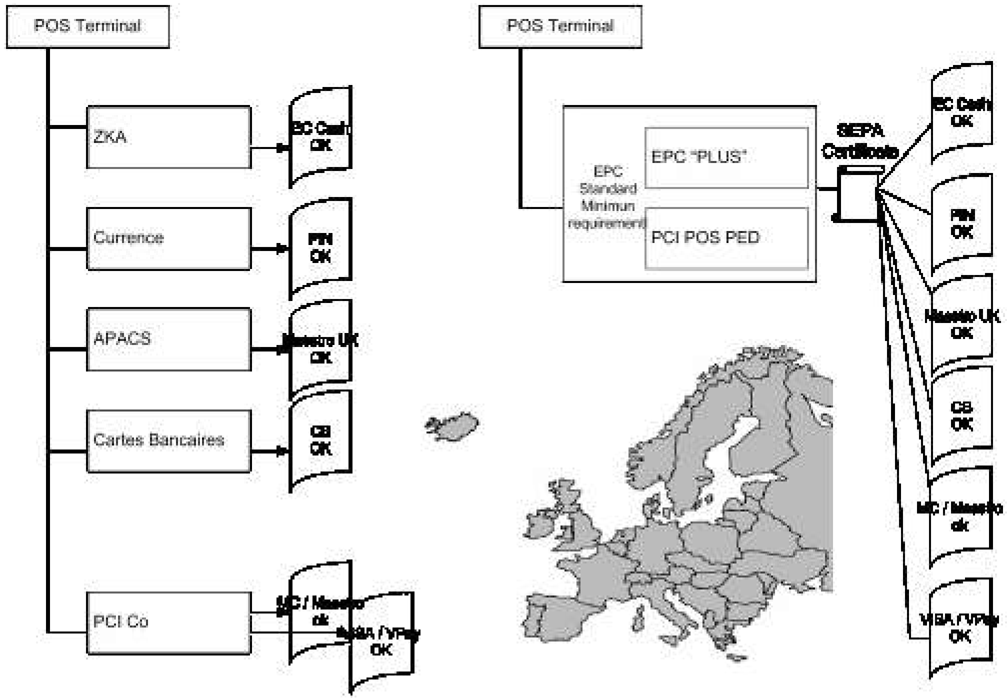
This document reflects a payment scheme's view of a smartcard. It does not assume any specific organisation of the supply chain, except where the supply chain interfaces with the payment scheme. The requirements expressed in this document apply globally to the TOE, never specifically to a part of the TOE, for example its hardware, basic software or middleware. There is no reference either to protection profiles that part of the TOE would comply with.

It is the responsibility of the smartcard suppliers, together with their own suppliers higher up the supply chain, to decide how the requirements in this generic ST are best met. They may choose to organise the evaluation of an EPA as a composition, using a previously evaluated IC or software platform (assuming that the TOE design includes one). They may choose to use protection profiles for ICs or software platforms.

Payment schemes recognise the efficiency of composition. They also appreciate that IC evaluation gives them advanced notice on the capacity of IC state-of-the-art technology to defeat attackers. Therefore they encourage smartcard suppliers to resort to it.

5 CERTIFICATION FRAMEWORK

Simplified Certification Procedures for the terminals



A similar procedure applies to cards.

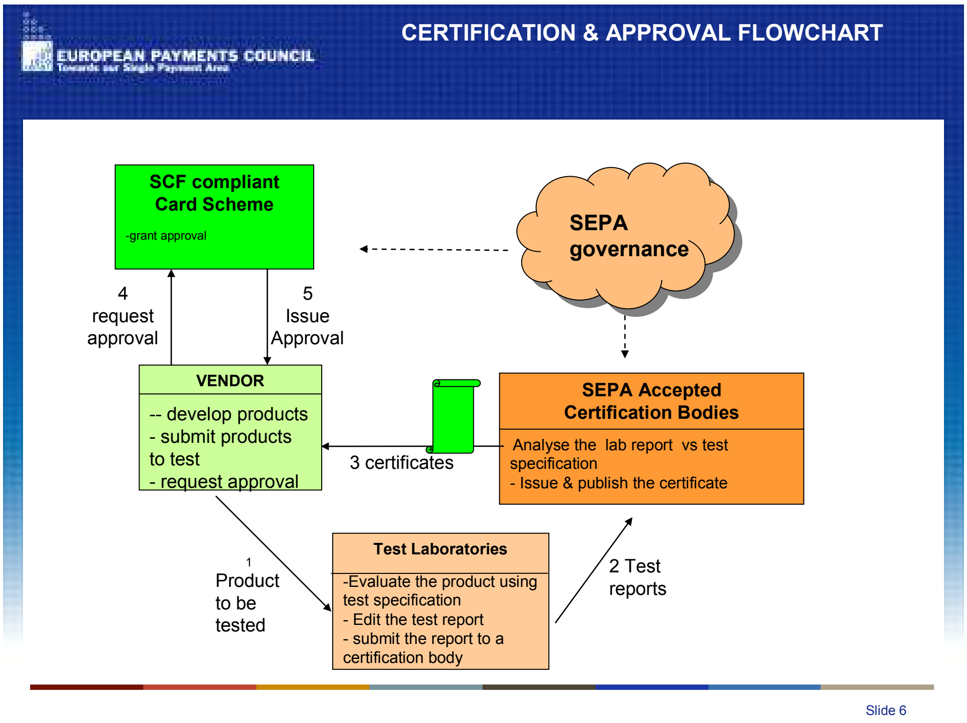
5.1 Common SCF compliant certification and approval framework for cards and terminals (D3)

One of the crucial aspects of the SEPA mutual recognition is the governance issue. CAS addresses this issue by defining a Certification Framework. This Framework describes the mutual recognition in SEPA for the interoperability part as well as for the security part. It is the common understanding within CAS, that it will focus on certification first considering, that approval takes risk assessment issues of the respective scheme into account.

The framework up to now relies on the following certification roles, which are well known within the European credit industry

- The role of a "certification body", which mainly assesses the evaluation reports, ensure comparability of the evaluation process towards the SEPA rules and issue certificates.
- The role of an "administration office", which mainly acts as an administration body for registering certification bodies, the evaluators and card schemes,
- The role of an "evaluator or test laboratory", which mainly perform the compliance testing on the basis of an interoperability test set and security requirements and issue a test report to the vendor.
- The role of vendors, which requests and in the end receives an interoperability and/or security certification.

Additional roles, which might be appropriate to implement mutual recognitions of certificates between certification bodies for a kind of SEPA governance are being discussed:



EUROPEAN PAYMENTS COUNCIL
Towards our Single Payment Area

CERTIFICATION & APPROVAL FLOWCHART

SCF compliant Card Scheme
-grant approval

SEPA governance

4 request approval

5 Issue Approval

VENDOR
-- develop products
- submit products to test
- request approval

3 certificates

SEPA Accepted Certification Bodies
Analyse the lab report vs test specification
- Issue & publish the certificate

1 Product to be tested

Test Laboratories
-Evaluate the product using test specification
- Edit the test report
- submit the report to a certification body

2 Test reports

Slide 6

5.2 Certification and type approval Work in progress (CAS)

5.3 The card-to-terminal space Work in progress (CAS)

5.4 The terminal-to-acquirer space Work in progress (CAS)

6 PROPOSED SPECIFICATIONS

This part introduces proposed specifications which make a reference to different identified initiatives with their own IPR.

6.1 Card To Terminal Domain – Proposed Specifications

SEPA-FAST - Context and SEPA FAST objectives

The Cards Working Group of the European Payments Council (EPC) has agreed on the SEPA Cards Framework (SCF see [SCF]), which "spells out high level principles and rules which when implemented by banks, schemes, and other stakeholders, will enable European customers to use general purpose cards to make payments and cash withdrawals in Euro throughout the SEPA area with the same ease and convenience than they do in their home country" (section 1.1 of [SCF]) and is "aimed at building an environment in which there are neither technical nor legal or commercial barriers which stand in the way of cardholders, banks and merchants choosing and using SCF compliant payment and ATM access card products" (section 1.2 of [SCF]).

The [SCF] "confirms the EMV chip and, on the acquiring side, PIN, as the supporting technology going forward" (section 1.3.2 of [SCF]).

EMV deployment has already started for many schemes, and in many countries inside and outside SEPA, based on the EMV specifications as published by EMVCo. Experience has shown that EMV terminals cannot be implemented on the basis of the EMVCo specifications alone, since they are functional specifications mainly describing how to process a standard, successful EMV transaction. Some processing details, e.g. error handling and the fallback process to magnetic stripe, are described only rudimentarily by the EMV specifications.

In addition, terminal implementations must also consider different card scheme requirements (which are not always aligned), regional requirements, and requirements with regard to Issuers, Acquirers, card acceptors/merchants and infrastructure.

This has led to:

- Interoperability problems, mainly due to problems in the implementation of the EMV specifications in terminals and Acquirer networks,
- Terminals that implement the specifications correctly, but which are not optimised in terms of processing time,
- A different "look and feel" of transactions to the cardholder depending on the terminal and the terminal implementation,
- Additional costs for terminals caused by:
- A high degree of customisation regarding the integration of the EMV specifications into a specific network,
- Multiple terminal testing due to different sets of requirements which have to be fulfilled by a single terminal in a specific acquiring environment.

In order to avoid these problems and to ensure SEPA level interoperability for the two domains (section 3.6.3.1 of [SCF]):

- Cardholder-to-terminal interface and
- Card-to-terminal interface

An unambiguous, detailed terminal specification, the "Financial Application Specification for SCF Compliant EMV Terminals" (SEPA-FAST) will be developed with the objective of:

- Harmonising EMV implementations on terminals supporting SEPA payments,
- Supporting a uniform "look and feel" of transactions from the cardholder's perspective,
- Reducing the risks of interoperability obstacles between applications,
- Enabling an open market for EMV-based components,
- Being the basis for "one-stop shopping" for terminal testing and mutual recognition of type approval.

The development of SEPA-FAST is to be performed in close cooperation with other European standardisation initiatives which cover the other SEPA-level interoperability domains, particularly the:

- Terminal-to-Acquirer interface and
- Acquirer-to-Issuer interface.

Based on those principles, SEPA specifications will be produced.

6.2 Terminal To Acquirer Domain – Pan-European Implementation Specifications

In addition to the basic needs of interoperability and security addressed in the previous sections, many acquirers and acceptors in Europe express today the need to use unique pan-European implementation specifications for the Terminal-to-Acquirer domain.

In order to ensure (or act as a catalyst for) the creation of at least one pan-European Terminal-to-Acquirer exchange protocol implementation specification, the EPC has initiated a cooperation with the pre-existing EPAS Consortium. EPAS is an ITEA[5] labelled project, including currently 21 full members and 12 associated members from 10 different countries coming from different sectors: banks, manufacturers, retailers, etc.

One of its objective is to create a new Terminal-to-Acquirer exchange protocol fulfilling the different needs of banks and merchants at European level. More details on the EPAS project is given in Annex 7.4.

In order to address the need of a pan-European interchangeability of the hardware components and interoperability of software components in card acceptance terminals and integrated solutions, the EPC has similarly initiated cooperation with the pre-existing ERIDANE Consortium, which is gathering 10 members from different European Countries. More details on the ERIDANE project is given in Annex 7.5.

[5] "Information Technology for European Advancement", European program for research and development

6.3 Acquirer To Issuer Domain – Proposed Specifications

Comparison of some ISO 8583 Implementations

6.3.1 Introduction and background

The Expert Group conducted an investigation into the possibility of achieving in the short term a reduction of the number of versions of ISO 8583 in Europe, in-line with the Terms of Reference for the standardization work in this domain.

This document describes the investigation that was conducted and presents the conclusions of the Expert Group.

6.3.2 Approach and methodology

Typically, most countries have one or more domestic implementations for both Authorisation and Clearing plus some international ones like Berlin Group, MasterCard, Visa, Eufiserv, etc. For the purpose of this investigation, the Expert Group selected a sample of representative international formats (those mentioned above) plus one domestic format: Cartes Bancaires.

For each of these formats, the Expert Group analyzed several relevant protocol-level aspects of the format, such as:

- ISO 8583 version's usage.
- Connectivity
- Character's usage
- Bit map's usage
- Advice's management
- Repeat's management
- Reversal's management
- How to proceed when an authorisation request times out.
- Partial reversal and partial approval allowance
- Refund's management
- Transaction fee's management.
- Transaction ID
- Transaction life cycle ID

The information used for the analysis was taken directly from the official specs (Berlin Group, MasterCard and Visa) and in some other cases was provided by the companies themselves (Cartes Bancaires and Eufiserv). In all cases they have been revised by technical experts of the respective companies and their comments and amendments were incorporated in the final analysis.

6.3.3 Analysis

The full analysis conducted is summarized in the table presented in appendix. It shows that functionally equivalent solutions display a number of substantial numbers of protocol-level differences.

6.3.4 Conclusion

The conclusion of the analysis is that, due the different ways of implementations, some even outside ISO 8583, the approach of reducing the number of implementations across Europe is foreseen unlikely to be justifiable in a short term if not complemented by other business drivers.

The Acquirer to Issuer Group will proceed by preparing and delivering Minimum Requirement, i.e. a list of Core Data Element to determine a target for convergence.

In addition Proposed specifications will be developed to allow full technical interoperability.

Appendix: Table showing summary of analysis conducted

	BERLIN GROUP		CARTES BANCAIRES		EUFISERV				MASTERCARD		VISA		
	AUTHORIZATION Dual message	CLEARING	AUTHORIZATION Dual message	CLEARING	Online (single and dual message)		Batch (differed clearing)		AUTHORIZATION	CLEARING	AUTHORIZATION		CLEARING
					V2	SIL	V2	SIL	CIS - BANKNET	IPM - GCMS	BASE I / VIP	SMS	BASE II
ISO 8583 VERSION	Ver. 1 (1993)	Ver. 1 (1993)	Ver. (1987)	NON ISO 8583	Ver. 0 (1987)				Ver. 0 (1987) File Action Ver. 1	Ver. 1 (1993)	Ver. 0 (1987)		NON ISO 8583
PROTOCOL TYPE	BILATERAL		Centralized	Centralized	Bilateral	Centralized	Bilateral	Centralized	CENTRALIZED		CENTRALIZED		
CONNECTIVITY/File transfer tool	IP - VPN	IP-VPN /C:D	IP	PeSIT Modèle OSI TCP/IP	IP-VPN or X25		IP-VPN or X25/ XFB or C:D		TCP/IP (FRONT-END EM)	XFB and C:D	TCP/IP (FRONT-END VAP)		BATCH TRANSFER FTP IBM STANDARD / XFB
MESSAGE / BATCH STRUCTURE	Message type id + Bitmap(s) + Data Fields	Record header + Detailed Records + Reconciliation Record + Message Trailer	Message type id + Bitmap(s) + Data Fields	Record header + Detailed Records + Reconciliation Record	Non ISO Message header + Message type id + Bitmap(s) + Data Fields		Record header + Detailed Records + Reconciliation Record		Message type id + Bitmaps(s) + Data Fields	Record header + Detailed Records + Reconciliation Record + Message Trailer	NON ISO Message header + Message type id + Bitmap(s) + Data Fields		Record header + Detailed Records + Reconciliation Record + Message Trailer
CHARACTERS USAGE	ASCII		ASCII	ASCII	EBCDIC				ASCII OR EBCDIC	EBCDIC	EBCDIC Field lengths in Binary, Numeric fields in BCD		EBCDIC
BIT MAPS	PRIMARY AND SECONDARY Variable length	PRIMARY AND SECONDARY Variable length	PRIMARY AND SECONDARY Variable length	NO	PRIMARY AND SECONDARY Variable length				PRIMARY AND SECONDARY Variable length	PRIMARY AND SECONDARY Variable length	PRIMARY AND SECONDARY Variable length THIRD BM been replaced by F55 for Acquirers. Issuers may still use it (Visanet will convert)		N/A Fixed length
MAC	YES	ONLY TRAILER INCLUDES MAC	NO	Integrity with SIT/CB algorithm	Yes		NO but SLL encryption at file transfer level is used		No (secured at network level)	No (secured at network level plus optional encryption)	IT IS DEFINED BUT NOT USED	NO	HASH OPTIONAL IN ALL RECORDS
MESSAGE COMPLETION AFTER AUTHORIZATION TIMES-OUT	TO SEND A 1420 REVERSAL	N/A	N/A	N/A	Send a 0420 Reversal		N/A		TO SEND A 0420 REVERSAL	N/A	TO SEND A 0101 REPEAT OR REVERSAL	TO SEND A 0420 REVERSAL	N/A
ADVICES	NOT PERMITTED	N/A	Yes	N/A	Yes, from stand-in service		N/A		Yes	N/A	YES, BUT ONLY FROM VISA UNDER REQUEST		N/A
REPEATS	421 Maximum 10	N/A	MTI 0101, 0121,0401	N/A	0121, 0421 Minimum 5		N/A		0120, 0420 Maximum 49	N/A	0101 / 0401 REPEATS UNTIL ACCEPTED	0420/0200	N/A
REVERSALS	VIA 1420 / 1421 COMUNICATIONS	VIA NON ISO REVERSAL INDICATOR WHITIN 1240	Via MT0400 / MT0410	YES	Via MT0420 / MT0421		Via MT0420		VIA 0400 COMUNICATIONS	VIA NON ISO REVERSAL INDICATOR WHITIN 1240	VIA 0400 / 0401 request	VIA 0420	VIA VISA PROPIETARY RECORDS TC2X
PARTIAL REVERSAL	YES VIA P30	N/A	BMP095	NO	Yes via BMP 120		Yes via BMP 120		YES, VIA DE095	NOT PERMITTED	YES VIA F095	Adjustment for partial ATM dispenses	NOT DEFINED
PARTIAL APPROVAL	NOT PERMITTED	N/A	Not allowed	N/A	Not permitted		N/A		YES	N/A	NOT PERMITTED (ONLY IN USA)		N/A
PREAUTHORIZATION	NOT PERMITTED	N/A	Yes	YES	Yes		N/A		ALLOWED	N/A	NOT PERMITTED		N/A
REFUNDS	N/A	ALLOWED	Yes	YES	Yes		Yes		ALLOWED		NOT PERMITTED	This is a Reversal	ALLOWED
DEBIT/CREDIT	DEBIT AT THE MOMENT	DEBIT AT THE MOMENT	DEBIT and CREDIT	DEBIT and CREDIT	Debit and credit (not including addendum messages)				DEBIT AND CREDIT		DEBIT AND CREDIT		

	BERLIN GROUP		CARTES BANCAIRES		EUFISERV				MASTERCARD		VISA		
STAND-IN	N/A	N/A	N/A	N/A	Permitted via MT0120		N/A		YES DE100 PRESENT	N/A	YES F44,1 PRESENT	YES F63.4 PRESENT	N/A
EMV	VIA BMP55		BMP55	SET of ELEMENT coming from authorization BMP 55	VIA BMP55				VIA DE055		VIA F55 (Prefered) OR 3^{RD} BIT MAP		VISA PROPIETARY
E-COMMERCE	NOT DEFINED YET		3DSECURE (VbV/SECURECODE)		3DSECURE (VbV/SECURECODE)				SECURE CODE - 3DSECURE		VbV -> 3D SECURE		
TRANSACTION FEE	N/A	PROVIDED BY THE ACQUIRER	N/A	decided by “CB” and Provided by Acquirer	PROVIDED BY THE ADQUIRER	IDED BY EUFI	Provided by Acquirer	PROVIDED BY EUFISERV	N/A	PROVIDED BY MASTERCARD	N/A	PROVIDED BY VISA	PROVIDED BY VISA (AGGREGATED)
KEY DATA FIELDS REQUEST/RESPONSE MATCHING	BMP11 BMP12 BMP32	N/A	BMP002 BMP004 BMP011 BMP012 BMP013 BMP032 “CB” banks are free to choose their own criteria	N/A	BMP007 BMP011 BMP032 BMP033 BMP071		N/A		DE02 DE11 DE32 DE33	N/A	F32 F37 F41 F42 & CPS	F32 F37 F07 F11	N/A (CPS)
REQUEST/REVERSAL MATCHING	BMP11 BMP12 BMP32		BMP002 BMP004 BMP011 BMP012 BMP013 BMP032 Compared to in reversal BMP090 Nota : “CB” banks are free to choose their own criteria	Authorization equivalent data	In request BMP007 BMP011 BMP032 BMP033 BMP071 compared to in reversal BMP090				DE02 DE11 DE32 DE33	DE02 DE31	F32 F37 F62.1 Possible	F11 F32 F37	PAN + ARN
TRANSACTION LIFE CYCLE ID AUTHORIZATION / CLEARING / CHARGEBACKS / RFC MATCHING	BMP11 BMP12 BMP32		N/A	All data of original transaction	BMP007 BMP011 BMP032 BMP033 BMP071				DE 63, or (when not available): DE02, DE11 DE32, DE33	DE 63, or (when not available): DE02, DE31	F32 F37 F41 F42	F07 F11 F32 F37	PAN + ARN

7 ANNEXES

7.1 European Payments Council - EPC

7.1.1 Introduction

The European Payments Council (EPC) is the decision-making and coordination body of the European banking industry in relation to payments whose declared purpose is to support and promote the creation of the Single euro Payments Area (SEPA).

The vision for the SEPA was formulated in 2002 at the time of the launch of EPC, when some 42 banks, the three European Credit Sector Associations (ECSAs) and the euro Banking Association (EBA) came together and, after an intensive workshop, released the White Paper in which the following declaration was made and subsequently incorporated into the EPC Charter:

> "*We, the European banks and European Credit Sector Associations:*
>
> - *share the common vision that Euroland payments are domestic payments,*
> - *join forces to implement this vision for the benefit of European customers, industry and banks and accordingly,*
> - *launch our Single Payments Area.*"

The definition of SEPA is part of EPC Roadmap as approved by the December 2004 Plenary. “SEPA will be the area where citizens, companies and other economic actors will be able to make and receive payments in euro, within Europe (currently defined as consisting of the EU 25 member states plus Iceland, Norway, Lichtenstein and Switzerland), whether between or within national boundaries under the same basic conditions, rights and obligations, regardless of their location.”

The SEPA will be delivered as a priority within the Eurozone. Within SEPA, but outside the Eurozone, there will be opportunities to participate in euro payment systems, and communities will be able to adopt SEPA standards and practices to contribute to the single market for payment services. The EPC aims for the widest acceptance of the Scheme, but recognises that some laws may only apply in the scope of the European Union (EU).

7.1.2 Excerpts of EPC Charter

7.1.2.1 Article 2: EPC Purpose and Objectives

The purpose of the EPC is to support and promote the Single Euro Payments Area (SEPA) in accordance with the vision formulated in the Preamble to this Charter. To that effect, the EPC shall, amongst others, develop the activities mentioned below.

For credit institutions within the Single Euro Payments Area (SEPA) the EPC shall:

- define common positions for core payment services,

- provide strategic guidance for standardization,
- formulate best practices,
- support and monitor the implementation of decisions taken,

So that they can:

- maintain self-regulation,
- meet regulators and stakeholders' expectations as efficiently as possible.

The scope of the EPC's focus is core payment services (retail and commercial payments) in Euro in Europe, and their settlement (see Interpretation in Annex).

The objectives and critical success factors are defined as being:

- widespread acceptance of reusable standards and best practices, which are simple, easy to understand and implement,
- reconciling the implementation of new solutions with the implications of existing legacy systems of banks, market infrastructures and customers,
- the sustained lowering of the cost base for the payments business,

All objectives should be achieved through self-regulation by decisions taken by the EPC Plenary.

7.1.2.2 Article 3: The role of the EPC

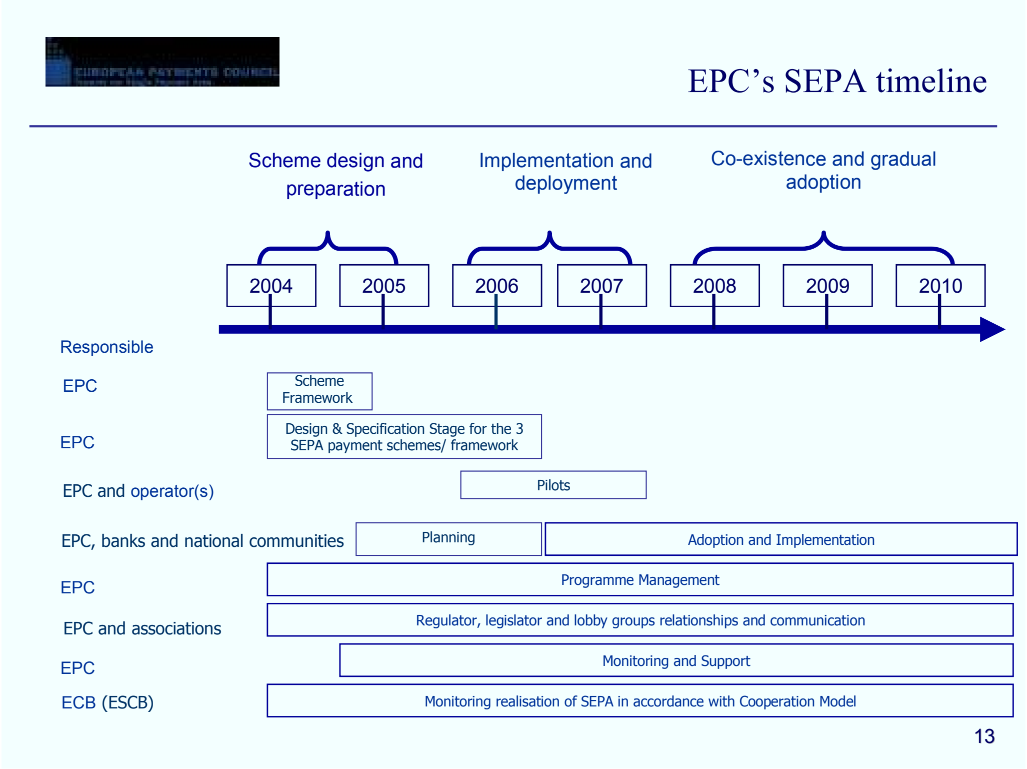
Within the above scope the EPC is established to serve as the decision-making organization for the European payments industry. It will also supervise the implementation of such decisions.

However the EPC is neither a market infrastructure, nor a payments association.

The EPC is an international not-for-profit association ("A.I.S.B.L.") governed by the provisions of Title III of the law of 27 June 1921 of the Kingdom of Belgium on not-for-profit associations, international not-for-profit associations and foundations.

7.1.3 EPC 2004 – 2010 Roadmap (approved in December 2004)

Slide 13 of the 2004 – 2010 EPC Roadmap



EPC's SEPA timeline

Scheme design and preparation
Implementation and deployment
Co-existence and gradual adoption
2004
2005
2006
2007
2008
2009
2010

Responsible	
EPC	Scheme Framework
EPC	Design & Specification Stage for the 3 SEPA payment schemes/ framework
EPC and operator(s)	Pilots
EPC, banks and national communities	Planning Adoption and Implementation
EPC	Programme Management
EPC and associations	Regulator, legislator and lobby groups relationships and communication
EPC	Monitoring and Support
ECB (ESCB)	Monitoring realisation of SEPA in accordance with Cooperation Model

13

Slide 21 of the 2004 – 2010 EPC Roadmap:

"Banks as EPC Members and/or as members of European and national banking communities are asked to:

- Support the SEPA vision & scope (Charter articles 1, 2 and 3).
- Contribute to the EPC deliverables at EPC and at national level.
- Plan & prepare for change in 2005, including timely decision-making as to mobilisation & execution.
- Implement & monitor progress at bank and at national community level.
- Give timely guidance to their associations, payment scheme organisations and infrastructures.
- Engage constructively with customers, consumer & lobby groups, governments and other stakeholders, with appropriate communication programmes.
- Support the start-up of the national SEPA implementation organisation in 2005."

7.1.4 Crowne Plaza Declaration by the European Payments Council (Brussels, 17 March 2005)

We, the EPC, are committed to building the Single Euro Payments Area (SEPA) and have already delivered SEPA Payment solutions which are in growing use by European citizens and corporates. We have approved and are delivering a Roadmap for the fill realisation of SEPA.

We will deliver the two new Pan-Euro Payment Schemes for electronic credit transfers and for direct debits. We will also design a cards Framework to define a single market for cards. The scheme rulebooks and the cards Framework definition will be delivered by end 2005, and the services will be operational by January 2008.

We know from feedback from our community in the Eurozone that by the beginning of 2008 the vast majority of banks will offer these new Pan-Euro services to their customers.

We are also convinced that a critical mass of transactions will naturally migrate to these payment instruments by 2010 such that SEPA will be irreversible through the operation of market forces and network effects.

SEPA will be delivered by the banking industry in close conjunction with all stakeholder communities (consumers, SMEs, merchants, corporates and government bodies) and supportive public authorities. The community of European banks is strongly committed to this ambitious programme of action, based on self-regulation and a full recognition of the role of market forces and competition.

We have created the necessary conditions for success through commitment and consensus on the part of the EPC and all its banking communities.

7.2 SEPA cards framework

7.2.1 Introduction

This SEPA[6] Cards Framework[7] (referred to as "the Framework") spells out high level principles and rules[8] which when implemented by banks, schemes, and other stakeholders, will enable European customers to use general purpose cards to make payments and cash withdrawals in euro throughout the SEPA area with the same ease and convenience than they do in their home country. There should be no differences whether they use their card(s) in their home country or somewhere else within SEPA. No general purpose card scheme designed exclusively for use in a single country, as well as no card scheme designed exclusively for cross-border use within SEPA, should exist any longer.

7.2.2 Reference

This document (Cards-027/05 - SEPA Cards Framework - Version 2.0 - 23 January 2006) is downloadable at the EPC site:

www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=18

[6] SEPA: whilst Europe is currently being defined as the EU 25 Member States plus Iceland, Liechtenstein, Norway, and Switzerland, SEPA is the area within this space where customers can make and receive payments in euro (source: EPC 2004 – 2010 Roadmap, December 2004).
[7] Framework: the SEPA Cards Framework is a common set of principles and rules for the provision by banks and card schemes of a pan-European card payment instrument. This common set of principles, rules and practices is agreed at SEPA interbank level, as explained in Section 1.3.1.
[8] Rules: for the purpose of this Framework rules shall mean such rights and obligations that will be accepted either by banks and card schemes as a consequence of them being spelled out in the present Framework and from time to time updated, or as a consequence of banks' participation in one or several card schemes.

7.3 Card Security Requirements

7.3.1 Introduction

This document contains payment scheme's security requirements for a payment application embedded in a smart card.

It is intended for use in a payment scheme's approval process whose purpose is to provide confidence in a smart card product. In that process, the Security Target against which the Embedded Payment Application (EPA) is to be evaluated is checked by the payment scheme for conformance to the security requirements. The present document provides guidance for writing such a security target. Its format is similar to that of a security target.

The approval process also requires that the sponsor of the evaluation deliver to the payment scheme an Evaluation Technical Report for Risk Management drafted by the evaluator and verified by the certification body. The ETR for Risk Management, whose template is provided by the payment scheme, contains the information needed by the payment scheme risk management to assess the exploitability of smart card residual vulnerabilities in the payment scheme.

To perform this task, risk management requires that residual vulnerabilities be expressed in terms of assets and security objectives that are meaningful for the payment scheme. To that end, the present document provides the list of assets and the list of security objectives to be declared in the security target and excludes the possibility for developers to add to those lists.

The payment scheme's approval process also calls for continuous assurance through updated state-of-the-art attacks as long as the product is in use in the payment scheme. Note that the assurance continuity program described in [CC] does not meet this objective, since a product that is not modified, or whose modifications do not impact security, will not be submitted to updated attacks. Fortunately, several CC Evaluation and Certification Schemes offer adequate, although dissimilar, surveillance or re-evaluation programs.

This document reflects a payment scheme's view of a smart card. It does not assume any specific organisation of the supply chain, except where the supply chain interfaces with the payment scheme. The requirements expressed in this document apply globally to the TOE, never specifically to a part of the TOE, for example its hardware, basic software or middleware. There is no reference either to protection profiles that part of the TOE would comply with.

It is the responsibility of the smart card suppliers, together with their own suppliers higher up the supply chain, to decide how the requirements in this generic ST are best met. They may choose to organise the evaluation of an EPA as a composition, using a previously evaluated IC or software platform (assuming that the TOE design includes one). They may choose to use protection profiles for ICs or software platforms.

Payment schemes recognise the efficiency of composition. They also appreciate that IC evaluation gives them advanced notice on the capacity of IC state-of-the-art technology to defeat attackers. Therefore they encourage smart card suppliers to resort to it.

7.3.2 Reference

Title	CAS Guidance on Writing a Security Target for a Smartcard Embedded Payment Application
Version	working draft 0.9
Date of Version	July 11th, 2007
Author	Common Approval Scheme (CAS)
TOE Identification	[product dependent]
TOE version	[product dependent]
CC Version	2.3 Final
Status	working draft

The document can be obtained from CAS upon request at the following address: paul-trescases@cartes-bancaires.com

7.4 EPAS information

7.4.1 Context

The need to harmonise protocols in card payment environments has become more acute the last years with the wish of the European Commission and of the European Central Bank to create a Single Euro Payments Area (SEPA).

One of the objectives of the European Commission in creating a Single European Market is to facilitate the dissemination of payments products and services Europe-wide as it is the case today for most national – domestic – markets in Europe.

The SEPA Card Framework document - committing the European banking industry in the implementation of SEPA - stated that "… In order for the objectives of this framework to be achieved, SEPA-level interoperability must be ensured in the following 4 domains :

a) cardholder to terminal interface;

b) cards to terminal (EMV),

c) terminal to acquirer interface (protocol or core requirements) and

d) acquirer to issuer interface, including network protocols (authorisation and clearing)".

The need for developing such standards to create a large internal market of financial services has been largely endorsed - not only by the banking industry - but also by solution providers, manufacturers, retailers and users.

With the development of "terminal-to-acquirer" protocol specifications, EPAS intends to address the missing links mentioned above in the creation of a unified market of electronic payments services.

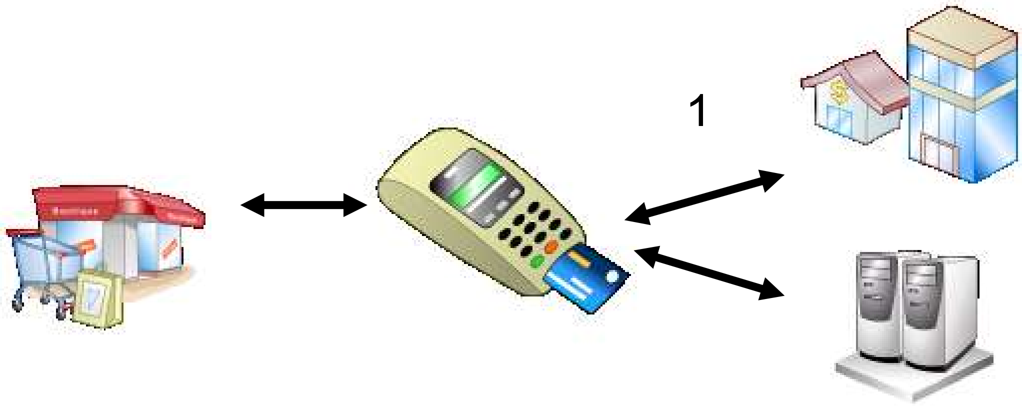
Partners belonging to the above industries have come together to develop and disseminate a set of data protocols which would complement the existing business standards needed to achieve and implement the necessary SEPA standards.

7.4.2 EPAS Consortium Information

The EPAS Consortium is an initiative which was launched in the framework of a European ITEA Project.

The objectives of EPAS is to define:

1. An Acquirer Protocol
2. A Terminal Management System Protocol
3. A Retailer Protocol



The EPAS Consortium is constituted of 21 members from 10 countries:

- Atos Worldline SA (Banksys) (BE)
- Atos Worldline GmbH (DE)
- BP (DE)
- Groupement des Cartes Bancaires (FR)
- Cetrel (LU)
- Equens (Interpay) (NL)
- Galitt (FR)
- Ingenico (FR)
- Integri (BE)
- Lyra Network (FR)
- Pan Nordic Card Association (SE)
- Paylife (Europay Austria) (AT)
- RSC (DE)
- Sermepa (ES)
- SIBS (PT)
- ZKA (SRC) (DE)
- Royal Bank of Scotland (UK)
- Thales e-Transactions (ES)
- Thales e-Transactions (FR)
- Total (FR)
- Wincor Nixdorf (ES)

There are also 12 Associated members:

- American Express (UK)
- Verifone (FR)
- Sagem Monetel (FR)
- Scheidt & Bachmann (DE)
- Gemalto (FR)
- Mellon Technologies (GR)
- Point International (SE)
- Quercia (Unicredit Groupà (IT)
- Servebase Computers (UK)
- The Logic Group (UK)
- Visa Europe (UK)
- Experian (FR)

These members represent the following sectors:

- Payment Schemes
- Banks
- Merchant
- Petrol
- Terminal manufacturers
- Service
- Software

The EPAS Consortium is open to new associated members. Details can be obtained from the EPAS Coordinator: william-vanobberghen@cartes-bancaires.com

EPAS Project Organisation and Work-Packages:

Requirements

- WP1 : Business and market requirements
- WP2 : Risk analysis and security requirements

Specifications

- WP3 : Terminal management protocol specifications
- WP4 : Retailer application protocol specifications
- WP5 : Acquirer protocol specification

Software

- WP6 : Terminal management protocol software development
- WP7 : Retailer application protocol software development
- WP8 : Acquirer protocol software development

Integration

- WP9 : Integration and interoperability demonstrator

Organisation and Communication

- WP10 : Exploitation and dissemination
- WP11 : Project management.

7.4.3 Reference

Draft Version 1.00 - 2 May 2007 - © 2007 EPAS

Dissemination restricted (EPAS and EPC)

7.5 ERIDANE

7.5.1 Consortium information

The ERIDANE Consortium is constituted of 10 members:

Axalto (part of Gemalto Group)
GIE - Groupement des Cartes Bancaires "CB"
Ingenico
MasterCard International
Sagem Monetel (part of Ingenico Group)
SRC - Security Research & Consulting
Thales e-Transactions
Atos Worldline SA/NV (Observer)
Equens (Observer)
CETREL (Observer)
Sermepa (Observer)
APACS (Observer)

7.5.2 Reference

ERIDANE - Business and Market requirements Draft Version 1.00 19 April 2007

Dissemination restricted (ERIDANE & EPC)

8 INDEX