



EPC020-08

12.12.2013

(Vol Ref. 7.2.1.00)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 2

FUNCTIONAL REQUIREMENTS

PART OF THE APPROVED VERSION OF SCS VOLUME v7.0

Payments and Withdrawals with Cards in SEPA Applicable Standards and Conformance Processes

© European Payments Council/Conseil Européen des Paiements AISBL.
Any and all rights are the exclusive property of
EUROPEAN PAYMENTS COUNCIL - CONSEIL EUROPEEN DES PAIEMENTS AISBL.

Volume v7.0 and its constituent Books supersede the SEPA Cards Standardisation Volume v6.0.

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.2.1.00
Date of Version	12 December 2013
Reason for Issue	Publication
Reviewed	Approved for publication by the EPC Plenary of 12 December 2013 and endorsed by the CSG GM of 7 November 2013
Produced by	CSG Secretariat
Owned and Authorised by	EPC
Circulation	Public

Table of Contents

1	GENERAL.....	3
1.1	Book 2 - Executive Summary.....	3
1.2	Description of Changes since the Last Version of Book 2.....	5
2	SCOPE.....	6
3	CARD FUNCTIONAL REQUIREMENTS.....	10
3.1	Introduction	10
3.2	Chip with Contact.....	10
3.3	Contactless.....	11
4	POI FUNCTIONAL REQUIREMENTS.....	12
4.1	Introduction	12
4.2	General Requirements	12
4.2.1	POI Application.....	13
4.2.2	Configuration	15
4.2.3	Functions for Card Service Processing	16
4.3	Payment Services	25
4.3.1	Payment	25
4.3.2	Refund.....	28
4.3.3	Cancellation.....	30
4.3.4	Pre-Authorisation Services.....	32
4.3.5	Deferred Payment.....	37
4.3.6	No-Show.....	40
4.3.7	Instalment Payment.....	41
4.3.8	Recurring Payment.....	45
4.3.9	Quasi-Cash Payment	48
4.4	Cash Services.....	50
4.4.1	ATM Cash Withdrawal	50

4.4.2	Cash Advance (attended).....	52
4.5	Card Inquiry Services.....	55
4.5.1	Card Validity Check	55
4.5.2	Balance Inquiry.....	56
4.6	Card Electronic Transfer.....	59
4.6.1	Card Funds Transfer	59
4.6.2	Original Credit	61
4.6.3	Prepaid Card - Loading/Unloading.....	63
4.7	Additional Features.....	66
4.7.1	Payment with Increased Amount	66
4.7.2	Payment with Cashback.....	66
4.7.3	Payment with Purchasing or Corporate Card Data.....	67
4.7.4	Payment with Aggregated Amount	68
4.7.5	Payment with Deferred Authorisation.....	68
4.7.6	Dynamic Currency Conversion (DCC).....	69
4.7.7	Surcharging/Rebate	70
5	PROTOCOL FUNCTIONAL REQUIREMENTS	72
6	FIGURES AND TABLES.....	76

1 GENERAL

1.1 Book 2 - Executive Summary

This book provides functional requirements applicable to transactions initiated at the card acceptor's POI either as "Cardholder Present" transactions initiated by a "Card"¹ or as "Cardholder Not Present" transactions based on Stored Card Data. These transactions result in the provision to the cardholder of the Services specified in this document.

These, so called "Card Services",

- ⇒ involve, in general, a cardholder and the issuer of a card, a card acceptor and its acquirer;
- ⇒ refer to services where the cardholder and the acceptor interact using a particular *Acceptance Technology* within a particular *Acceptance Environment* supporting *Cardholder Verification Methods and Card Authentication Methods (including none)*;
- ⇒ are processed through a succession of *Functions* executed in the card, in the Point Of Interaction (POI)¹, in the Terminal to Acquirer Domain, and in the Acquirer to Issuer domain.

"Card Services", "Acceptance Technologies", "Card Authentication Methods", "Cardholder Verification Methods" and "Functions" are listed in section 2.

Out of Scope:

1. Different stakeholders, e.g. a processor, could provide what are deemed to be acquiring services. Intermediaries² are considered as out of scope of this.
2. The Functions executed solely in the Acquirer to Issuer Domain are out of scope for this book.
3. The functional requirements for remote transactions are out of scope for this book. The "Cardholder Not present" transactions covered in this book are not considered as remote transactions since they are initiated at the card acceptor's terminal and not at the cardholder's computer or mobile device.

¹ See definition in Book 1

² The cards value chain includes a lot of stakeholders between the cardholder and the issuer, mainly the merchant and the acquirer. A cards intermediary is a third party offering services between those stakeholders or acting on their behalf.

The scope of this book is summarised in section 2.

Section 3 defines core functional requirements for the card applications.

Section 4 defines core functional requirements for the POI applications.

Section 5 lists core functional requirements for protocols.

Note:

Card and POI implementations may have additional functions implemented, as long as they are not contrary to the Volume requirements.

1.2 Description of Changes since the Last Version of Book 2

This is the first version of Book 2

2 SCOPE

In this section, the scope of this book is summarised by listing:

- ⇒ "Card Services"
- ⇒ Acceptance Technologies and Acceptance Environments
- ⇒ Cardholder Verification Methods and Card Authentication Methods
- ⇒ Functions

Definitions of the different Cards Services, Acceptance Technologies, Acceptance Environments, Cardholder Verification Methods, Card Authentication Methods and Functions are given in Book 1.

CARD SERVICES	SCS Volume Book 2 Scope (Yes/No)
PAYMENT SERVICES	
Payment	Y
Refund (partial or total)	Y
Cancellation	Y
Pre-Authorisation Services <ul style="list-style-type: none"> • Pre-Authorisation • Update Pre-Authorisation • Payment Completion 	Y
Deferred Payment	Y
No-Show	Y
Instalment Payment	Y
Recurring Payment	Y
Quasi-Cash Payment	Y
CASH SERVICES	
ATM Cash Withdrawal	Y
Cash Advance (attended)	Y
Cash Deposit	N
CARD INQUIRY SERVICES	
Card Validity Check	Y
Balance Inquiry	Y
CARD ELECTRONIC TRANSFER	
Card Funds Transfer	Y
Original Credit	Y
Prepaid Card - Loading/Unloading	Y
e-Purse - Loading/Unloading	N
ADDITIONAL FEATURES	
Payment with Increased Amount	Y
Payment with Cashback	Y
Payment with Purchasing or Corporate Card Data	Y
Payment with Aggregated Amount	Y
Payment with Deferred Authorisation	Y
Dynamic Currency Conversion (DCC)	Y
Surcharging/Rebate	Y

Payment with Deferred Clearing	N
Payment with Loyalty Information	N
Unsolicited Available Funds	N
CARD MANAGEMENT SERVICES	
PIN Change / Un(b)lock	N
Card Activation	N
Return Card to Cardholder Request	N
Card Pick-up Advice	N
Return Card Advice	N
ACCEPTANCE TECHNOLOGIES	SCS Volume Scope (Yes/No)
Chip with Contact	Y
Magnetic Stripe	Y
Manual Entry	Y
Chip Contactless	Y
Contactless with Mobile	Y
Stored Card Data	Y
Imprint	N
ACCEPTANCE ENVIRONMENTS	SCS Volume Scope (Yes/No)
Attended	Y
Unattended	Y
Semi-Attended ³	Y
CARDHOLDER VERIFICATION METHODS	SCS Volume Scope (Yes/No)
Offline Plaintext PIN	Y
Offline Enciphered PIN	Y
Online PIN	Y
Signature	Y
Mobile Code	Y
No CVM Required	Y
Biometric	N

³ According to the definition in Book 1, semi-attended is treated as attended.

CARD AUTHENTICATION METHODS	SCS Volume Scope (Yes/No)
EMV Offline SDA	Y
EMV Offline DDA	Y
EMV Offline CDA	Y
EMV Online Authentication	Y
Card Security Code	Y
FUNCTIONS	SCS Volume Scope (Yes/No)
Configuration	Y
Transaction Initialisation	Y
Language Selection	Y
Technology Selection	Y
Application Selection	Y
Card Data Retrieval	Y
Card Authentication	Y
Cardholder Verification	Y
Authorisation	Y
Referral	Y
Completion	Y
Reversal	Y
Data Capture	Y
Financial Presentment	N
Settlement	N
Chargeback	N
ADMINISTRATIVE SERVICE	SCS Volume Scope (Yes/No)
Reconciliation	N

TABLE 1: BOOK 2 SCOPE

3 CARD FUNCTIONAL REQUIREMENTS

3.1 Introduction

This section defines core functional requirements for Volume conformance regarding contact and contactless Card applications (sections 3.2 and 3.3).

The actual transaction processing of contactless Card applications is out of scope. In order to be accepted at a POI that supports the contactless Acceptance Technologies, the contactless Card application has to support processing corresponding to at least one of the kernels supported by the contactless POI application.

The Acceptance Technologies Magnetic Stripe and Manual Entry are not required for Volume conformance but are covered by the POI Functional Requirements for migration purposes. If these Acceptance Technologies are supported by a Card, they shall comply with current industry standards concerning coding and contents of the magnetic stripe Track 2 and presentation of card data on the card body.

The Acceptance Technology Imprint is out of scope for Volume conformance.

3.2 Chip with Contact

Req C1: The Card-to-Terminal communication shall be compliant with [EMV B1]. The functionality (commands and data structure) implemented by Card Applications shall comply with the relevant requirements in [EMV].

Req C2: Cards shall support Application Selection through PSE⁴.

Req C3: PSE and Card Applications shall include the Language Preference data element. It is recommended that this data element also includes English.

Req C4: Card Applications shall support PIN as CVM. Other CVMs as defined by [EMV] may also be supported.

Card Applications shall support Offline PIN and Online PIN.

Card Applications that support Offline PIN may support either Offline Plaintext PIN or Offline Enciphered PIN or both, where Offline Enciphered PIN is preferred.

The requirement to support PIN may be waived in exceptional circumstances, to allow card usage by people who, for reasons of disability, are unable to enter, memorise and/or safeguard a PIN.

Req C5: Card Applications shall support Online Mutual Authentication (OMA).

⁴ According to [EMV] support of "Payment System Environment" by the Card is optional. It is mandated for SEPA compliance in alignment with Req C7. Migration considerations are provided in Book 6.

Req CN1: Card Applications that support offline transactions shall support Offline Data Authentication.

Card Applications that support Offline Data Authentication shall support DDA or CDA or both.

3.3 Contactless

Req C6: The Card-to-Terminal communication shall be compliant with [EMV D].

Req C7: Cards shall support Combination Selection through PPSE according to the card requirements in [EMV B].

Req C8: The PPSE shall include the Language Preference data element. It is recommended that this data element also includes English.

Req CN2: Contactless Card applications shall comply with the card requirements in [EMV A] and [EMV B].

Req C9: The contactless Card Application shall allow identification of the Form Factor.

4 POI FUNCTIONAL REQUIREMENTS

4.1 Introduction

This section defines core functional requirements for Volume conformance for POI Applications. This includes ATM Applications since ATMs are specific POIs. The section is mainly structured according to the Card Services, Functions and Additional Features, as listed in section 2.

Section 4.2 contains general requirements that apply to all Card Services, regarding the POI Application, the Configuration Function and the Functions used for Card Service Processing.

These general requirements are followed by sections per Card Service which contain the following:

- Allowed combinations of Acceptance Technologies and Acceptance Environments for the Card Service.
- Applicable Functions defined as not applicable, mandatory, optional or conditional for the Card Service according to the Function's description, either in the general section 4.2 or in a Service specific section on the respective Function.
- Card Service dependent requirements for the POI Application and for Configuration, if any.
- Card Service dependent requirements for the Functions that are applicable for processing the Card Service, if any.

The sections on the individual Card Services are grouped according to section 2, i.e. in Payment Services (section 4.3),

Cash Services (section 4.4), Card Inquiry Services (section 4.5) and Card Electronic Transfer (section 4.6).

Section 4.7 contains requirements that apply to the Additional Features.

The functional requirements for POI Applications are only applicable, if the respective application implementation supports the Card Service and/or Function addressed by the requirement.

The term "Contactless" is used to refer to both Acceptance Technologies, the Chip Contactless Acceptance Technology and the Contactless with Mobile Acceptance Technology, unless described otherwise.

The requirement T3 below, to comply with [EMV A] and [EMV B] for POI Applications supporting the Contactless Acceptance Technologies enables the usage of kernels according to [EMV C1], [EMV C2], [EMV C3], [EMV C4] and [EMV C5] as well as any other kernel that complies with [EMV A] and [EMV B].

4.2 General Requirements

This section contains requirements that apply to all or several Card Services. These requirements are grouped in requirements for the POI Application (section 4.2.1), for the Configuration Function (section 4.2.2) and for the Functions used for Card Service Processing (section 4.2.3).

4.2.1 POI Application

The POI Application is the POI software for processing the Card Services. Refer to the Volume, Book 1, "General" for the POI Application terminology.

The following figure shows the logical relationship between the POI Application, the Card Services, the Functions and the configuration parameters:

- POI parameters configure the POI Application independently of the Card Services, e.g. define which of the supported Acceptance Technologies, Acceptance Environments, Card Services and Functions are available for transaction processing.
- Card Service parameters configure the Card Service, e.g. define which of the available Acceptance Technologies are allowed for a Card Service.
- Application Profile parameters configure the Application Profile for a Card Service, e.g. define the limits to be used.

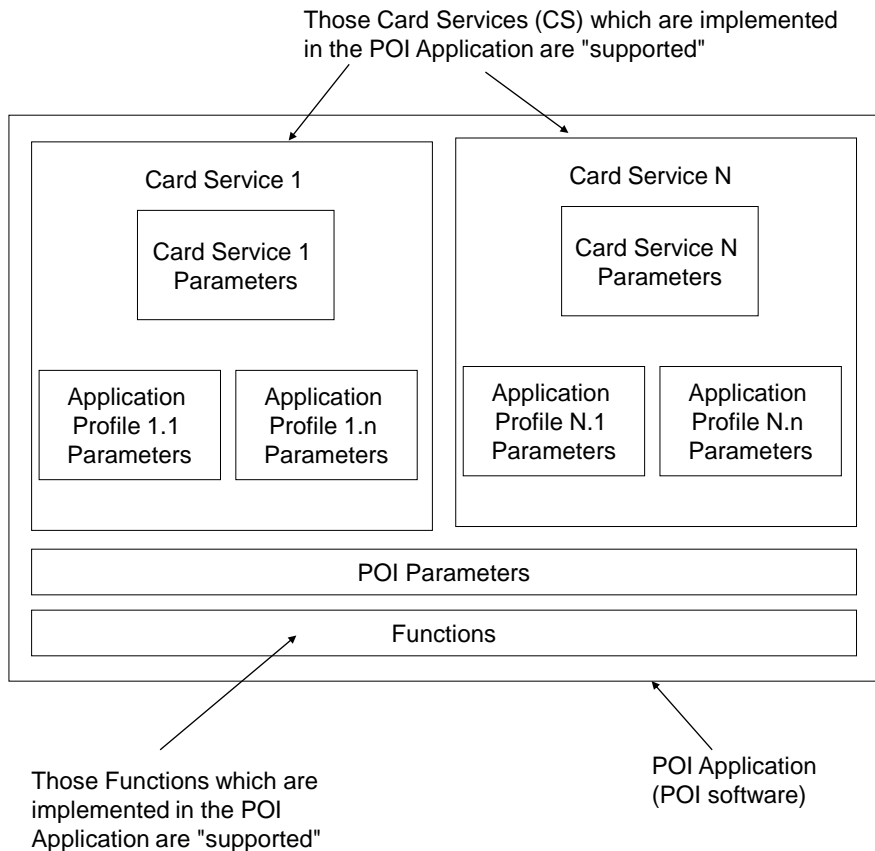


FIGURE 2: POI APPLICATION - LOGICAL STRUCTURE AND CONFIGURATION PARAMETERS

A POI Application shall meet the requirements listed in this section, depending on the Acceptance Technologies that are supported.

- Req T1: The POI Application supporting the Chip with Contact Acceptance Technology shall be compliant with [EMV].
- Req T2: For the Chip with Contact Acceptance Technology, the POI Application shall support Application Selection through PSE ("Payment System Environment").
- Req T5: The POI Application supporting the Chip Contactless Acceptance Technology shall also support the Contactless with Mobile Acceptance Technology and vice versa, as defined for "Card" in Book 1. The POI Application supporting the Contactless Acceptance Technologies shall be able to identify and react adequately to whichever form factor if the form factor information is available. If the form factor information is not present, the POI Application shall assume that the Chip Contactless Acceptance Technology is used.
- Req T3: The POI Application supporting the Contactless Acceptance Technologies shall support and comply with [EMV A], [EMV B] and [EMV D].
- Req T7: The POI Application shall support at least a local language and English for the cardholder display. English only is allowed if English is the local language.
- Req T8: The POI Application shall support updating of text tables for cardholder display languages.
- Req T11: All POIs, attended and unattended, shall be protected from unauthorised use of the Card Service Refund, Original Credit and Cancellation.
- Req T12: For the unattended POI, independent of the level of integration with the sale system, the following communications shall be exchanged:
- Communication to request a transaction, including the transaction amount and Transaction Type if applicable, from the sale system to the POI Application.
 - Communication of the authorisation result, including authorised transaction amount if applicable, from POI Application to sale system.
 - In the event the final amount differs from the amount authorised, the fact needs to be communicated from the sale system to the POI Application, including the final amount if needed to take the appropriate actions.
- In addition the following communication should be supported by the unattended POI:
- Communication of card presence from POI Application to sale system.
- Req T13: The POI Application shall not prevent processing with different acquirers.
- Req TN1: If the Chip with Contact Acceptance Technology has been tried and failed, and if subsequently Magnetic Stripe Acceptance Technology is tried, and the magnetic stripe data indicates that chip processing is supported, then the POI Application shall check the Application Profile configuration to determine, whether the

magnetic stripe transaction is allowed and if it has to be considered as a fallback transaction (see TN4).

4.2.2 Configuration

Configuration is the act and result of setting the parameters for configurable Card Services and configurable Functions within a POI Application. Refer to SEPA CARDS STANDARDISATION (SCS) "VOLUME", Book 1, "General" for the POI Application terminology.

This section contains requirements for configuration of several or all Services and Functions.

- Req T6: It shall be possible to configure the Card Services, the Application Profiles and the Functions, when applicable. In particular it shall be possible to configure the POI Application to activate or deactivate specific Card Services and/or Functions.
- Req T9: For POIs with a cardholder display it shall be possible to configure the default language for the cardholder display and there shall always be one language set to be the default language.
- Req TN2: It shall be possible to configure which of the supported Acceptance Technologies are activated per Card Service. Activation of the Contactless Acceptance Technology shall mean both, activation of Chip Contactless and Contactless with Mobile.
- Req TN3: It shall be possible to configure per Card Service if the Chip with Contact Acceptance Technology is not required to have priority over the Magnetic Stripe Acceptance Technology to support the particular Card Services that require it, e.g. Refund or Cancellation.
- Req TN4: It shall be configurable per Application Profile whether a magnetic stripe transaction shall be allowed and considered as a fallback transaction in case the Chip with Contact Acceptance Technology has been tried and failed, and if the transaction is afterwards performed based on the magnetic stripe Acceptance Technology, and if magnetic stripe data indicates that chip processing is supported by the card.
- Req T43: It shall be possible to configure the supported CVMs per Application Profile.
- Req TN5: For attended POIs that support referrals it shall be configurable per Application Profile whether referrals are activated.
- Req TN6: It shall be configurable per transaction result (approved, declined or aborted) and per Card Service whether a cardholder receipt shall be printed either never or always or on request.⁵

⁵ If there is a legal requirement to print a receipt, the POI shall be configured to do so

4.2.3 Functions for Card Service Processing

The following sections contain the Function specific requirements which are not only applicable to an individual Card Service but to all or to several Card Services.

4.2.3.1 Transaction Initialisation

Transaction Initialisation is the Function which allows selection of the Card Service for the next transaction and where the transaction amount is set, transaction data is initialised and processing of the Card Service is started.

- Req T14: The attendant, cardholder or sale system shall be able to select the required Card Service from the list of Card Services that are activated. If Card Service selection is not performed, then the default Card Service is the selected Card Service.
- Req T15: For transaction initialisation the cardholder display shall always display a message, called Welcome Message, to the cardholder, the contents of which will depend on the selected Card Service.
- Req T16: The Welcome Message shall be shown only in the selected language if the default language was overridden. Otherwise the Welcome Message 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 Welcome Message in two different languages at the same time, it shall alternate between the two.
- Req T17: For all Acceptance Technologies with the exception of Chip Contactless, the transaction shall be initiated either by attendant action or by card insertion/swiping or by external activation by the sale system.
- Req T20: For contactless transactions, the transaction shall be initialised (i.e. Card Service selection, amount availability) prior to the activation of the contactless reader of the POI.
- Req T21: For unattended POIs capable of, and configured for, printing a transaction receipt, if the POI knows in advance that it cannot print a transaction receipt, it shall inform the cardholder that a receipt cannot be printed and offer the choice to continue or abort the transaction.

4.2.3.2 Language Selection

Language Selection is the Function which allows selecting one of the languages supported by the POI for the cardholder display. If cardholder is not present, Language Selection is not applicable.

Language Selection may be performed either as POI based or Card based Language Selection.

For the POI based Language Selection, either the sale system selects one of the languages supported by the POI or the POI Application offers to the attendant or the cardholder to select one of the languages supported by the POI.

For the Card based Language Selection, the POI selects one of the supported languages automatically, without cardholder or attendant interaction, through retrieving and evaluating the Language Preference of the card. Card based Language Selection is only applicable for Acceptance Technologies Chip with Contact and Contactless.

Req T36: If the POI receives the language from a sale system before the start of the financial transaction, it shall use it as the selected language for the duration of this transaction (POI based Language Selection by the sale system).

Req T33: If the POI does not receive a language from the sale system before the start of the financial transaction, or if the language that the POI receives is not supported by the POI, it may offer the attendant or the cardholder the option to override the default language for the cardholder display (see Req T9) and to select one of the languages supported by the POI for the cardholder display (POI based Language Selection on the POI). If this option is supported, then it shall only be possible prior to the start of the transaction. If chosen in this manner, the language shall become the selected language for the duration of this transaction.

Req T34: If the POI based Language Selection for the cardholder display was not (successfully) performed prior to the start of the transaction and if the Acceptance Technology is Chip with Contact or Contactless and if the card data element Language Preference is retrieved, the selection of the language for the cardholder display shall be performed according to [EMV] (Card based Language Selection) and the POI Application shall use from that moment on the first language in the Language Preference that it supports.

If the Acceptance Technology is neither Chip with Contact nor Contactless, or if the card data element Language Preference is not retrieved, or if the POI Application does not support any of the languages in the Language Preference, the POI Application shall continue to use the default language without performing any (additional) language selection.

Req T35: For attended POI, the messages for the attendant shall be displayed in a local language.

4.2.3.3 Technology Selection

Technology Selection is a Function which allows the Acceptance Technology (e.g. Chip with Contact, Magnetic Stripe, Chip Contactless, Manual Entry, etc.) to be selected to process a service for a transaction.

Req TN7: If a transaction is processed based on Stored Card Data, Technology Selection shall not be performed.

Req TN8: Technology Selection shall be based on the configuration of the Card Service to be performed: Activated Acceptance Technologies and no priority of Chip with Contact - if defined (see Reqs. TN2 and TN3).

- Req TN9: If an Acceptance Technology is selected, all other Acceptance Technologies shall no longer be taken into account until Technology Selection is re-started.
- Req T24: The POI shall display a message to use the chip, if all of the following are true: A card is swiped and the service code within Track 2 indicates that chip processing is supported by the card and there has not been an attempt to read the chip during the current transaction and Chip Acceptance Technology is activated for the Service (see Req. TN2) and Chip is configured to have priority (see Req. TN4).
- Req T25: If the Acceptance Technology Chip with Contact is activated and if a card is inserted in the chip reader of a POI with separate readers or in a hybrid reader before any other Acceptance Technology is selected, the POI Application shall recognise this and shall initiate reset processing according to [EMV B1].
- Req T26: If a card is inserted in the chip reader of a POI with separate readers or in the hybrid reader, and if the reset processing is unsuccessful, and if the POI Application allows for additional re-reading of the chip, a message shall be displayed to retry the chip.
- Req T27: If a card is inserted in the chip reader of a POI with separate readers or in the hybrid reader, and if the chip technology does not work and if the magnetic stripe Acceptance Technology is activated, then the POI Application shall initiate magnetic stripe processing.

4.2.3.4 Application Selection

Application Selection is the Function which allows

- for chip based transactions, selecting an application supported by both the card and the POI, either manually (by the cardholder) or automatically (without cardholder interaction) to be used to process a Card Service,
- and for all Acceptance Technologies, selecting an Application Profile.

Req T32: For Application Selection for chip based transactions, in addition to Application Selection requirements of [EMV B1] and [EMV B], the following clarification rules shall apply:

1. The terminal shall always construct the list of mutually supported applications between the card and the terminal.

If an agreement exists between all relevant parties (e.g. acceptors, acquirers, issuers, schemes), applications may be filtered out from this list. This can only be applied in cases where the cardholders and issuers agree this makes no difference to the cardholder's perspective.

The terminal shall then proceed either according to rule 2 or rule 3.

Rule 3 should be used for:

- Environments that do not require PIN based cardholder verification including but not limited to toll roads, parking, etc.

- Contactless transactions.
 - Environments where the speed of transactions is a priority.
2. The terminal shall present without discrimination all mutually supported applications for choice by the cardholder if more than one application is mutually supported.⁶ The POI display ergonomics shall be designed such that the cardholder is able to choose from the mutually supported applications in a convenient way.
 3. The terminal shall select the mutually supported application with the highest priority without cardholder interaction (automatic selection).

Automatic selections in case they would happen shall follow the priority indicators associated with the different applications in the card.

In the case of automatic selection, where practical, cardholders shall have the possibility to go back in the process and ask for their preferred application.

Req TN10: The Application Profile shall be selected for a transaction based on the Card Service and on the Payment Product. The selection of the Payment Product is primarily based on the selected AID for Chip with Contact transactions, on the Combination for Chip Contactless and on the PAN for Magnetic Stripe, Manual Entry and Stored Card Data transactions.

4.2.3.5 Card Data Retrieval

Card Data Retrieval is the Function which allows the POI to retrieve card data according to the Acceptance Technology.

4.2.3.6 Card Authentication

Card Authentication is the Function by which a chip Card is authenticated to the POI (Offline Data Authentication) and/or the Issuer (Online Mutual Authentication). Card Authentication applies only to the chip based Acceptance Technologies.

Req T39: Online-only POI Applications are not required to support Offline Data Authentication.

Req T40: The POI Application supporting the Chip with Contact Acceptance Technology and Offline Data Authentication shall support all Offline Data Authentication methods as defined in [EMV].

⁶ Not applicable for contactless

4.2.3.7 Cardholder Verification

Cardholder Verification is the Function by which a Cardholder Verification Method (CVM) is determined and performed. If cardholder is not present, Cardholder Verification is not applicable. The CVMs to be used are defined in the EMV specifications and may also be used for other Acceptance Technologies according to the conditions below:

- Offline Plaintext PIN and Offline Enciphered PIN (commonly referred to as "Offline PIN"), if the Acceptance Technology is chip based,
- Online PIN, if the Acceptance Technology is chip based or Magnetic Stripe,
- Mobile Code, if the Acceptance Technology is Contactless with Mobile,
- Signature, No CVM Required, for all Acceptance Technologies.

4.2.3.7.1 *General Requirements for Cardholder Verification*

Req T44: The POI Application shall not support PIN Bypass.

Req T45: All POI shall have a PIN Entry Device; with the exception of environments where the interaction with the cardholder must be minimized for cardholder or acceptor convenience (e.g. low value payments, transaction speed, highway tolls).

Req T46: For POIs having a PIN Entry Device, the POI Application shall be able to support PIN as CVM.

4.2.3.7.2 *Cardholder Verification for contact transactions*

Req TN11: The following requirements shall be met by POIs with a PIN Entry Device:

For offline-only POIs the POI Application shall support Offline PIN.

For offline with online capability POIs the POI Application shall support Offline PIN and may support, in addition, Online PIN.

For online-only POIs the POI Application shall support Offline PIN, or Online PIN or both.

POIs that support Offline PIN shall support both, Offline Plaintext PIN and Offline Enciphered PIN.

For ATMs the POI Application shall support Online PIN.

Other CVMs as defined by [EMV], including No CVM Required, may be supported in addition to PIN, except that for unattended POIs (including ATMs), Signature CVM and Combined CVM containing Signature are prohibited. In addition, for ATMs No CVM Required is prohibited.

4.2.3.7.3 *Cardholder Verification for contactless transactions*

Req TN12: POIs supporting a contactless POI Application shall support Online PIN and/or Signature and/or No CVM Required and/or Mobile Code according to the requirements of the contactless kernels implemented in that POI.

4.2.3.7.4 *Cardholder Verification for Magnetic Stripe Transactions*

Req TN13: The following requirements shall be met by POIs with a PIN Entry Device:

The only PIN CVM supported for magnetic stripe transactions shall be Online PIN.

The CVMs No CVM Required and Signature may also be supported. Unattended POIs (including ATMs) shall not support Signature CVM. In addition, ATMs shall not support No CVM Required.

4.2.3.7.5 *Cardholder Verification for Manual Entry Transactions*

Req TN14: The following requirements shall be met by POIs having a PIN Entry Device:

Neither Online PIN nor Offline PIN shall be supported for Manual Entry transactions.

The CVMs No CVM Required and Signature may be supported.

4.2.3.8 Authorisation

Authorisation is the Function performed by the POI to help the Acceptor to make a decision to proceed with a card service or not. It can be processed online to Issuer or Acquirer or processed offline to the Chip card.

Req TN15: For attended POIs, for all Card Services with the exception of the Payment Service (see Req T84), the attendant shall not be allowed to force a declined transaction to be accepted.

Req T28: Magnetic Stripe and Manual Entry transactions shall be sent online for authorisation. If the magnetic stripe transaction is a fallback transaction, it shall be identified as a fallback transaction.

Req T58: If the Authorisation Response Code indicates that the Online PIN entered did not verify correctly ("Wrong PIN"), for chip based Acceptance Technologies, the transaction shall be declined and Online PIN re-entry shall not be allowed within this transaction.

In this case, if the Acceptance Technology is Chip with Contact, the POI may start a new transaction transparently for the cardholder to facilitate the re-entry of the PIN (i.e. without ejecting the card, without repeating language and application selection, but with repeating the complete EMV card process including Online PIN entry).

4.2.3.9 Referral

Referral is the Function where a Card Service is completed with a verbal dialogue to obtain an approval code when the Authorisation response contains a response code requesting to perform such a function. This Function does not necessarily involve the card or the cardholder.

Req T60: If the attended POI supports referrals, then it shall support it for all Acceptance Technologies supported. If the POI does not support referrals or if referrals are not activated for the Application Profile and the POI receives a request for referral it shall decline the transaction.

Req T61: Unattended POIs shall not support referrals. If the POI receives a request for referral it shall decline the transaction.

Req T62: For attended POIs that support referrals, if a request for referral is received, in case of a chip based transaction, chip processing shall be terminated by requesting a decline from the card and (in all cases) a message shall be displayed requesting the removal of the card. The phone number to be called shall be displayed to the attendant for a voice authorisation. It shall then request an approval code to be manually entered in the POI. If no approval code is entered, the transaction remains declined. If an approval code is entered, the transaction shall be approved.

Req T63: The Referral Function shall be protected against unauthorised use.

4.2.3.10 Completion

Completion is the Function which provides information on how the transaction was completed. It depends on the Card Service and on the Acceptance Environment whether all or some of the following steps are performed:

- Complete the transaction for the card
- Inform cardholder, attendant and/or acquirer about the result of the transaction
- Deliver a receipt to cardholder and/or attendant

Req T65: If the POI is capable of printing receipts, a transaction receipt shall be provided for the cardholder if configured for the Application Profile. The receipt for the cardholder shall be printed in a local language. The transaction receipt may be combined with the sales receipt, if any.

The following are the minimum data that shall be printed on receipts⁷. The sequence of the data elements shown is not mandatory for the receipt. Additional data may be printed but is out of scope of this document.

- Transaction Date and Transaction Time (local date/time)
- Terminal Identification

⁷ Provided these requirements are in line with the local laws and regulations

- Transaction Reference, e.g. a sequence number or a sale reference number
- Transaction Amount⁸ and Transaction Currency⁹
- Application Primary Account Number (PAN), truncated
- DF Name (as returned by the card) for chip based transactions
- Payment product name, e.g. Application Preferred Name or Application Label for chip based transactions, or as retrieved from the Application Profile for Magnetic Stripe, Manual Entry or Stored Card Data transactions.
- Card acceptor name and location
- The Card Service, e.g. "Payment"
- Transaction Result, e.g. "Approved"

Req T66: If the transaction (approved, declined or aborted) is not immediately online-captured, it shall be logged in the POI.

4.2.3.11 Reversal

Reversal is the Function where the sender informs the receiver that a transaction cannot be processed as instructed with the intention to partially or completely nullify the effects of this transaction. This Function involves neither the card nor the Cardholder. Reversal can be performed online or offline in the POI by removing the transaction data or by storing cancellation data for capture.

Req TN16: Reversal shall be performed online if Authorisation is performed online and any of the following is true:

- No correct response or no response (timeout) is received
- or the transaction is declined/aborted after an online (full or partial) approval.

⁸ For Pre-Authorisation and Update Pre-Authorisation, this is the estimated amount that has been authorised.

⁹ For transactions with Dynamic Currency Conversion see Req. T106.

4.2.3.12 Data Capture

Data Capture is the Function to transfer data captured at a Point of Interaction to the Acquirer for "Financial Presentment". Data Capture can be performed either as part of the Authorisation message, or after transaction completion through either an Advice message or a Batch File transfer.

Req T72: One of the following methods or combinations thereof, of transferring the transactions to an Acquirer shall be supported:

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

4.3 Payment Services

4.3.1 Payment

TABLE 3: shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Payment Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 3: PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 4: shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Payment Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	O
Completion	M
(Partial) Reversal	C
Data Capture	M

TABLE 4: FUNCTIONS USED FOR PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Payment Service.

4.3.1.1 POI Application

- Req TN17: The transaction amount shall be checked against a minimum allowed amount and/or a maximum allowed amount if configured for the Application Profile.
- Req T52: For Payment, the cardholder shall be able to confirm the transaction amount and the payment product when performing the CVM.
- The only exception is the CVM No CVM Required, where the confirmation of the transaction amount shall be implicit by presenting the Card.
- Req T54: For unattended POIs, if the transaction amount is defined before the delivery of the goods or service, the amount used to process the transaction shall be the actual amount.
- Req TN18: If the POI supports partial approvals of online authorisations, then it shall support it for all Acceptance Technologies supported.

4.3.1.2 Configuration

- Req T22: It shall be configured that chip processing (contact and/or contactless) shall be supported (see Req. TN2) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req. TN4).
- Req T51: For attended POIs that support Payment with increased amount, it shall be possible to configure the POI to support the addition of a gratuity to be entered and confirmed by the cardholder.
- Req T53: It shall be possible to configure per Application Profile, if the transaction amount shall be checked against a minimum allowed amount and/or a maximum allowed amount.
- Req TN19: For the specific Unable-to-go-online processing described in Req. T56, the POI Application shall be configurable per Application Profile to either approve the transaction or, for attended POIs, perform a voice authorisation according to scheme rules, or decline.
- Req TN20: For attended POIs that support partial approvals of online authorisations it shall be configurable per Application Profile whether partial approvals are activated.
- Req T82: For attended POIs, if the POI is offline with online capability, it shall be possible to configure the POI Application to allow/not allow the attendant to force a transaction online.
- Req T84: For attended POIs, if the POI is off line with online capability or online-only, it shall be possible to configure the POI Application to allow/not allow the attendant to force a declined transaction to be accepted.

Req T85: For unattended POIs, forcing a declined transaction to be accepted shall not be supported.

Except for unattended environments where the interaction with the cardholder must be minimized because of a need of speed, if the POI is offline with online capability or offline-only, it shall be possible to configure the POI Application to allow/not allow the transaction approval to be automatically forced.

4.3.1.3 Transaction Initialisation

Req T19: For Payment, the transaction amount (i.e. the authorised amount, which includes any additional amount) shall be available to the POI Application at Transaction Initialisation.

4.3.1.4 Authorisation

Req T56: For chip-based contact transactions, if it is not possible to perform an online authorisation, the EMV Unable-to-go-online processing shall be performed with the following extension. If the POI requests an approval, and the card approves the transaction, and the amount exceeds the POI floor limit, the POI Application shall be configured to either approve the transaction (or for attended POIs perform a voice authorisation according to scheme rules) or decline. Approval, Voice Authorisation or decline shall be configurable per Application Profile.

Req T83: Forcing a transaction to go online shall not be supported on unattended POIs.

Req TN21: For Authorisation, the transaction amount as defined in Req. T19 shall be used.

Req TN22: For online authorisation, the authorisation response may return a lower authorised amount (partial approval).

If the POI does not support partial approvals for online authorisation or if partial approvals are not activated for the Application Profile and the POI receives a partial approval it shall decline the transaction.

If partial approvals are supported and activated, the POI shall always return the actual authorised amount to the sale system and/or to the attendant.

4.3.1.5 Completion

Req T70: The unattended POI shall send a message to the sale system to indicate the transaction result. The unattended POI shall receive the delivery result, including the final transaction amount if available, from the sale system.

Req T87: Forcing a declined transaction to be accepted shall be protected against unauthorised use.

Req T69: To prevent the cardholder from leaving the card in the unattended POI, card removal shall always be prompted prior to goods or service delivery.

4.3.1.6 Reversal

Req T80: If the actual amount was authorised but no goods or service could be delivered, the POI shall receive an indication of this from the sale system. If the transaction was authorised online, the POI shall then perform a reversal to nullify the original authorisation.

Req T81: If the actual amount was authorised but not all the goods or service could be delivered; the POI shall receive an indication of this from the sale system, including the reduced amount. If the transaction was authorised online, the POI shall then perform a partial reversal. The captured data shall always include the final, reduced amount.

4.3.2 Refund

TABLE 5: shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Refund Service.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip Contactless	✓	✗
Contactless with Mobile	✓	✗

TABLE 5: REFUND: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 6** shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Refund Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A

Function	Requirement
Cardholder Verification	N/A
Authorisation	O
Referral	N/A
Completion	M
Reversal	C
Data Capture	M

TABLE 6: FUNCTIONS USED FOR REFUND

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Refund Service.

4.3.2.1 POI Application

- Req T153: In the case of a chip based Refund transaction, the Refund shall follow EMV processing until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date. The chip process shall be terminated by requesting a decline from the card. The transaction amount given to the chip during the Refund should be zero to avoid unnecessary card risk management.
- Req TN23: The transaction amount shall be checked against a maximum allowed amount if configured for the Application Profile.

4.3.2.2 Configuration

- Req T151: The maximum amount and the allowed maximum amount that can be performed without additional security (e.g. a supervisor password) shall be configurable for the Refund Service.
- Req T154: It shall be configurable per Application Profile, whether the Refund is performed online or not.

4.3.2.3 Transaction Initialisation

- Req TN24: The Refund amount shall be available to the POI Application at Transaction Initialisation. The way to link the Refund transaction to a previous Payment is out of scope.

4.3.2.4 Authorisation

Req TN25: If required by the Application Profile, the Refund shall be processed online.

4.3.3 Cancellation

TABLE 7: shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Cancellation Service.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip Contactless	✓	✗
Contactless with Mobile	✓	✗

TABLE 7: CANCELLATION: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 8:** shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Cancellation Service

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	C
Referral	N/A
Completion	M
Reversal	O
Data Capture	C

TABLE 8: FUNCTIONS USED FOR CANCELLATION

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Cancellation Service.

4.3.3.1 POI Application

- Req T157: A Cancellation is always performed for the full amount of the original transaction.
- Req T161: In the case a of chip based Cancellation transaction, the Cancellation shall follow EMV processing until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date. The chip process shall be terminated by requesting a decline from the card. The transaction amount given to the chip during the Cancellation should be zero to avoid unnecessary card risk management.
- Req T173: It shall be possible for attended POIs to cancel approved Pre-Authorisations with the Cancellation Service.
- Req T187: It shall be possible for attended POIs, to cancel approved Update Pre-Authorisations with the Cancellation Service.
- Req T197: It shall be possible for attended POIs, to cancel a Payment Completion with the Cancellation Service.

4.3.3.2 Configuration

- Req T156: It shall be configurable per Application Profile which of the Card Services can be cancelled.
- Req T158: It shall be possible to configure per Application Profile whether Cancellations shall be restricted to the last transaction processed at the POI or may be extended to previous transactions.
- Req TN26: It shall be possible to configure per Application Profile, whether Cancellations shall be declined or processed online in case the original transaction has already been captured to the Acquirer.
- Req TN27: It shall be possible to configure per Application Profile, whether Cancellations shall be declined or processed online in case the original transaction cannot be recognised by the POI.
- Req TN28: It shall be possible to configure per Application Profile, whether Cancellations shall be performed offline or processed online if the original transaction was authorised offline and has not been captured to the Acquirer.

4.3.3.3 Authorisation

Req T162: If the original transaction cannot be recognised by the POI or has been already captured to the Acquirer, the Cancellation shall either be declined or be processed online according to the configuration of the Cancellation Service.

Req TN29: If the original transaction can be recognised by the POI and has not been captured to the Acquirer, Cancellation shall be performed as follows:

If the original transaction was authorised online, Cancellation shall also be processed online.

If the original transaction was authorised offline, Cancellation shall be either performed offline or processed online according to the configuration of the Cancellation Service.

For offline Cancellation either the original transaction data is removed from the POI or the cancellation data is stored for capture.

Upon successful online processing of the Cancellation, either the original transaction data is removed from the POI or the cancellation data is stored for capture.

4.3.3.4 Data Capture

Req TN30: Data Capture shall be performed according to the conditions described in TN29.

Req T159: Every captured Cancellation transaction shall include a (set of) data element(s) uniquely referencing the original transaction.

4.3.4 Pre-Authorisation Services

Pre-Authorisation Services consist of the Pre-Authorisation Service, the Payment Completion Service and optionally the Update Pre-Authorisation Service.

Support of the Pre-Authorisation Services requires support of Pre-Authorisation and Payment Completion but not Update Pre-Authorisation (optional). Although processing of the Pre-Authorisation Service and the Update Pre-Authorisation Service is similar, the Pre-Authorisation Service may be supported without supporting the Update Pre-Authorisation Service.

Each of the Pre-Authorisation Services may also be performed as a "Cardholder Not present" transaction. In this case, and only in this case, the Acceptance Technology Stored Card Data is used.

TABLE 9: shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Pre-Authorisation Services.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓
Stored Card Data	✓	✗

TABLE 9: PRE-AUTHORISATION SERVICES: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

4.3.4.1 Pre-Authorisation Service and Update Pre-Authorisation Service

The column "Requirement" in **TABLE 10:** shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Pre-Authorisation and Update Preauthorisation Service.

Function	Requirement
Language Selection	C
Transaction Initialisation	M
Technology Selection	C
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	C
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	N/A

TABLE 10: FUNCTIONS USED FOR PRE-AUTHORISATION AND UPDATE PREAUTHORISATION

4.3.4.1.1 *Pre-Authorisation*

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Pre-Authorisation Service.

4.3.4.1.1.1 *POI Application*

- Req T164: Pre-Authorisation shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.
- Req T166: The POI shall either receive the amount from the attendant or the sale system or use a default amount, which - in both cases - should be an estimated amount, or be based on known or expected expenditure.
- Req T167: If the cardholder is participating, the cardholder display shall clearly indicate that the amount is an estimated amount.
- Req T172: Approved Pre-Authorisations shall be stored for performing subsequent steps (i.e. Update Pre-Authorisation, Payment Completion), either in the POI or in a system external to the POI.
- Req TN31: A Pre-Authorisation shall include a (set of) data element(s) uniquely referencing this Pre-Authorisation.

4.3.4.1.1.2 *Configuration*

- Req T168: The POI Application shall be configurable to allow the Pre-Authorisation amount to be received or to be a configurable default amount.
- Req TN32: The POI Application shall be configurable to allow the Pre-Authorisation validity period to be received or to be a configurable default value.

4.3.4.1.1.3 *Authorisation*

- Req T170: A Pre-Authorisation shall be authorised online in order to reserve the funds.
- Req TN33: The Pre-Authorisation shall include the validity period that this Pre-Authorisation is to remain valid.

4.3.4.1.1.4 *Data Capture*

- Req T171: Approved Pre-Authorisations shall not be captured.

4.3.4.1.2 *Update Pre-Authorisation*

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Update Pre-Authorisation Service.

4.3.4.1.2.1 *POI Application*

- Req T175: Update Pre-Authorisation shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.
- Req T176: Acceptance Technology for Update Pre-Authorisation may be different from the Pre-Authorisation (or previous Update Pre-Authorisation) Acceptance Technology.
- Req T177: An Update Pre-Authorisation shall be linked to a previous Pre-Authorisation (or Update Pre-Authorisation) and shall include the (set of) data element(s) uniquely referencing this previous Pre-Authorisation (or Update Pre-Authorisation).
- Req T178: An Update Pre-Authorisations shall only be allowed while the Pre-Authorisation (or Update Pre-Authorisation) to which it is linked is still valid.
- Req T179: An approved Update Pre-Authorisation shall replace the previously linked Pre-Authorisation (or Update Pre-Authorisation) which it is updating.
- Req T182: Approved Update Pre-Authorisations shall be stored for performing subsequent steps (i.e. Update Pre-Authorisation, Payment Completion), either in the POI or in a system external to the POI.
- Req T183: An Update Pre-Authorisation shall include the new estimated amount and/or validity period.
- Req T184: If the cardholder is participating, the cardholder display shall clearly indicate that the amount is a new estimated amount replacing the previous one.
- Req T186: If the Update Pre-Authorisation is declined, then the previously linked Pre-Authorisation (or Update Pre-Authorisation) shall remain unchanged. In particular, the previously authorised amount and validity period shall remain unchanged.

4.3.4.1.2.2 *Configuration*

- Req TN34: The configuration of the POI Application for Pre-Authorisation shall also be used for Update Pre-Authorisation.

4.3.4.1.2.3 *Authorisation*

- Req T180: An Update Pre-Authorisation shall be authorised online.
- Req TN35: The Update Pre-Authorisation shall include the validity period that this Update Pre-Authorisation is to remain valid.

4.3.4.1.2.4 *Completion*

Req T185: The transaction receipt, if any, shall clearly show that this is a new Pre-Authorisation performed and show the new estimated amount and indicate that it is replacing the previous one.

4.3.4.1.2.5 *Data Capture*

Req T181: Approved Update Pre-Authorisations shall not be captured.

4.3.4.2 Payment Completion

The column "Requirement" in TABLE 11 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Payment Completion Service.

Function	Requirement
Language Selection	C
Transaction Initialisation	M
Technology Selection	C
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	N/A
Referral	N/A
Completion	M
Reversal	N/A
Data Capture	M

TABLE 11: FUNCTIONS USED FOR PAYMENT COMPLETION

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Payment Completion Service.

4.3.4.2.1 *POI Application*

Req T189: A Payment Completion may be done only if the final amount does not exceed the estimated amount of the previous Pre-Authorisation (or Update Pre-Authorisation) plus the configurable overspent percentage (according to scheme rules).

- Req T190: Payment Completion may be performed in all Acceptance Environments and in all Acceptance Technologies, using its own configuration. Acceptance Environment and Acceptance Technology for Payment Completion may be different from the previous Pre-Authorisation (or Update Pre-Authorisation) Acceptance Environment and Technology.
- Req TN36: In the case of a chip based Payment Completion transaction, the Payment Completion shall follow EMV processing until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date. The chip process shall be terminated by requesting a decline from the card. The transaction amount given to the chip during the Payment Completion should be zero to avoid unnecessary card risk management.
- Req T191: A Payment Completion shall be linked to the previous Pre-Authorisation (or Update Pre-Authorisation) to which it relates and shall include the (set of) data element(s) uniquely referencing this previous Pre-Authorisation (or Update Pre-Authorisation).
- Req T192: A Payment Completion shall only be allowed while the previous Pre-Authorisation (or Update Pre-Authorisation) to which it is linked is still valid.
- Req T194: A Payment Completion shall include the final amount.
- Req T195: If the cardholder is participating, the POI display shall clearly indicate that the amount is the final amount.

4.3.4.2.2 *Configuration*

- Req T193: The POI Application shall be configurable to either perform online capture by sending a completion message immediately after the Payment Completion, or perform batch capture.

4.3.5 Deferred Payment

TABLE 12 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Deferred Payment Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 12: DEFERRED PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 13 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Payment Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 13: FUNCTIONS USED FOR DEFERRED PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Deferred Payment Service.

4.3.5.1 POI Application

- Req T55: For Deferred Payment, the unattended POI shall use as transaction amount for authorisation either a predefined amount available in the POI Application, or an amount available and provided by the sale system (e.g. a selected amount). The predefined amount may be configurable per Application Profile.
- Req TN37: The transaction amount for authorisation shall be checked against a maximum allowed amount if configured for the Application Profile.
- Req T52: The cardholder shall be able to confirm the transaction amount for authorisation and the payment product when performing the CVM if confirmation of the transaction amount is configured for the Application Profile.

If the CVM is No CVM Required, then the confirmation of the transaction amount shall either be implicit by presenting the Card or explicit with a confirmation display, if confirmation of the transaction amount is configured for the Application Profile.

4.3.5.2 Configuration

- Req T22: It shall be configured that chip processing (contact and/or contactless) shall be supported (see Req. TN2) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req. TN4).
- Req T53: It shall be possible to configure per Application Profile, if the transaction amount shall be checked against a maximum allowed amount.
- Req TN38: For Deferred Payment, it shall be possible to configure per Application Profile, if the transaction amount shall be confirmed by the cardholder.
- Req T84: For attended POIs, it shall be possible to configure the POI Application to allow/not allow the attendant to force a declined transaction to be accepted.
- Req TN39: It shall be possible to configure for the POI Application the timeframe in which reception of the delivery result is expected from the sale system.

4.3.5.3 Authorisation

- Req TN40: Deferred Payment shall be authorised online.
- Req T59: For Deferred Payment, the authorisation response may return a lower authorised amount. In any case the POI shall always return the actual authorised amount to the sale system.

4.3.5.4 Reversal

- Req TN41: Online Reversal shall not be performed if the transaction is declined/aborted after an online approval. Instead a notification message with final amount zero shall be used as described in TN42.

4.3.5.5 Completion

- Req T71: The POI shall receive the delivery result from the sale system, including the final amount which must be lower than, or equal to, the authorised amount. The delivery result may also be a zero amount.
- Req TN42: A notification of the final amount (e.g. an Advice message) shall be sent online immediately after the delivery result is received. This notification shall also be sent to nullify the effects of the authorisation if the final amount is zero (no delivery or a delivery result is not received in the configured timeframe).
- Req TN43: The POI shall send a message to the sale system to indicate the transaction result.

4.3.5.6 Data Capture

Req TN44: Data Capture shall be performed either as online capture through a completion message sent after each transaction (referred to as notification message in TN42) or through batch capture.

Data Capture shall always include the final amount. If the final amount is zero Data Capture is not required.

4.3.6 No-Show

No-Show is a "Cardholder Not present" Service. Therefore, Stored Card Data is the only Acceptance Technology used for this Service.

TABLE 14 shows which combination of Acceptance Technology and Acceptance Environments are allowed (✓) or not allowed (✗) for the No Show Service.

	Attended	Unattended
Stored Card Data	✓	✗

TABLE 14: NO SHOW: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 15: Functions used for No Show shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the No Show Service.

Function	Requirement
Language Selection	N/A
Transaction Initialisation	M
Technology Selection	N/A
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 15: FUNCTIONS USED FOR NO SHOW

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the No Show Service.

4.3.6.1 Authorisation

Req TN45: No Show transactions shall be authorised online and shall be identified as No Show.

4.3.6.2 Data Capture

Req TN46: No Show transactions shall be identified as No Show when they are captured.

4.3.7 Instalment Payment

The Instalment Payment Service is initiated by a first transaction from the POI which is a Payment transaction and contains specific information which identifies it as an Instalment Payment transaction and which shall describe the payment schedule and conditions.

The subsequent transactions of an Instalment Payment are "Cardholder Not present" transactions where the card data used is extracted from Stored Card Data and are not necessarily initiated by the POI that performed the first Instalment Payment transaction.

The requirements for the first transaction of an Instalment Payment are described in section 4.3.7.1.

The requirements for the subsequent transactions of an Instalment Payment are described in section 4.3.7.2.

4.3.7.1 First Transaction

TABLE 16 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the first transaction of an Instalment Payment.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip contactless	✓	✗
Contactless with mobile	✓	✗

TABLE 16: INSTALMENT PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION

The column "Requirement" in TABLE 17 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the first transaction of an Instalment Payment.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 17: FUNCTIONS USED FOR FIRST TRANSACTION OF AN INSTALMENT PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the first transaction of an Instalment Payment.

4.3.7.1.1 *POI Application*

Req TN47: The first transaction of an Instalment Payment shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.3.7.1.2 *Configuration*

Req TN48: The allowed maximum total Instalment amount shall be configurable.

4.3.7.1.3 *Authorisation*

Req TN49: The first transaction of an Instalment Payment shall be online and shall include the information which identifies it as the first transaction of an Instalment Payment and how many Payments shall be made in the payment plan, e.g. 1:6 to indicate that this is the first of 6 Payment transactions.

4.3.7.1.4 *Data Capture*

Req TN50: The data captured for clearing of the first transaction of an Instalment Payment shall include the information which identifies it as the first transaction of an Instalment Payment and how many Payments shall be made in the payment plan, e.g. 1:6 to indicate that this is the first of 6 Payment transactions.

4.3.7.2 *Subsequent Transactions*

TABLE 18 shows which combination of Acceptance Technology and Acceptance Environments is allowed (✓) or not allowed (✗) for the subsequent transactions of an Instalment Payment.

	Attended	Unattended
Stored Card Data	✓	✗

TABLE 18: INSTALMENT PAYMENT: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS FOR SUBSEQUENT TRANSACTIONS

The column "Requirement" in TABLE 21 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of an Instalment Payment.

Function	Requirement
Language Selection	N/A
Transaction Initialisation	M
Technology Selection	N/A
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 19: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF AN INSTALMENT PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the subsequent transactions of an Instalment Payment.

4.3.7.2.1 *Authorisation*

Req TN51: Subsequent Instalment Payment transactions shall be authorised online and shall include the information which identifies the instalment number being processed from the payment plan, e.g. 3:6 to indicate that this is the third of 6 Payment transactions.

4.3.7.2.2 *Data Capture*

Req TN52: The data captured for clearing of subsequent Instalment Payment transactions shall include the information which identifies the instalment number being processed from the payment plan, e.g. 3:6 to indicate that this is the third of 6 Payment transactions.

4.3.8 Recurring Payment

The Recurring Payment Service is initiated by a first transaction from the POI which is a Payment transaction and contains specific information which identifies it as a Recurring Payment transaction.

The subsequent transactions of a Recurring Payment are "Cardholder Not present" transactions where the card data used is extracted from Stored Card Data and are not necessarily initiated by the POI that performed the first Recurring Payment transaction.

The requirements for the first transaction of a Recurring Payment are described in section 4.3.8.1.

The requirements for the subsequent transactions of a Recurring Payment are described in section 4.3.8.2.

4.3.8.1 First Transaction

TABLE 20 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the first transaction of a Recurring Payment.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip contactless	✓	✗
Contactless with mobile	✓	✗

TABLE 20: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION

The column "Requirement" in TABLE 21 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the first transaction of a Recurring Payment.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M

Function	Requirement
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 21: FUNCTIONS USED FOR FIRST TRANSACTION OF A RECURRING PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the first transaction of a Recurring Payment.

4.3.8.1.1 *POI Application*

Req TN53: The first transaction of a Recurring Payment shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.3.8.1.2 *Authorisation*

Req TN54: The first transaction of a Recurring Payment shall be online and it shall contain specific information which identifies it as a Recurring Payment transaction.

4.3.8.1.3 *Data Capture*

Req TN55: The data captured for clearing of the first transaction of a Recurring Payment shall contain specific information which identifies it as a Recurring Payment transaction.

4.3.8.2 *Subsequent Transactions*

TABLE 22 shows which combination of Acceptance Technology and Acceptance Environments is allowed (✓) or not allowed (✗) for the subsequent transactions of a Recurring Payment.

	Attended	Unattended
Stored Card Data	✓	✗

TABLE 22: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS FOR SUBSEQUENT TRANSACTIONS

The column "Requirement" in TABLE 23 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of a Recurring Payment.

Function	Requirement
Language Selection	N/A
Transaction Initialisation	M
Technology Selection	N/A
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	M
Referral	O
Completion	M
Reversal	C
Data Capture	M

TABLE 23: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF A RECURRING PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the subsequent transactions of a Recurring Payment.

4.3.8.2.1 *Authorisation*

Req TN56: Subsequent Recurring Payment transactions shall be authorised online and shall contain specific information which identifies it as a Recurring Payment transaction.

4.3.8.2.2 *Data Capture*

Req TN57: The data captured for clearing of subsequent Recurring Payment transactions and shall contain specific information which identifies it as a Recurring Payment transaction.

4.3.9 Quasi-Cash Payment

TABLE 24 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Quasi-Cash Payment Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip contactless	✓	✓
Contactless with mobile	✓	✓

TABLE 24: QUASI-CASH PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 25 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Quasi-Cash Payment Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	O
Completion	M
(Partial) Reversal	C
Data Capture	M

TABLE 25: FUNCTIONS USED FOR QUASI-CASH PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Quasi-Cash Payment Service.

4.3.9.1 POI Application

Req TN58: The Quasi-Cash Payment shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.3.9.2 Cardholder Verification

Req TN59: No CVM Required is not allowed as CVM for Quasi-Cash Payment transactions.

4.3.9.3 Authorisation

Req TN60: The Quasi-Cash Payment shall be authorised online and it shall be identified as a Quasi-Cash Payment.

4.3.9.4 Reversal

Req TN61: If the actual amount was authorised but items could not be delivered, the POI shall receive an indication of this from the sale system. The POI shall then perform a reversal to nullify the original authorisation.

Req TN62: If the actual amount was authorised but not all items could be delivered; the POI shall receive an indication of this from the sale system, including the reduced amount. The POI shall then perform a partial reversal. The captured data shall always include the final amount.

4.3.9.5 Data Capture

Req TN63: The data captured for clearing of a Quasi-Cash Payment shall identify it as a Quasi-Cash Payment.

4.4 Cash Services

4.4.1 ATM Cash Withdrawal

An ATM is a specific Unattended POI supporting the ATM Cash Withdrawal Card Service. In this section, "Application" refers to a POI Application that supports the ATM Cash Withdrawal Service.

TABLE 26 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the ATM Cash Withdrawal Service.

	Attended	Unattended
Chip with Contact	✗	✓
Magnetic Stripe	✗	✓
Manual Entry	✗	✗
Chip Contactless	✗	✓
Contactless with Mobile	✗	✓

TABLE 26: ATM CASH WITHDRAWAL: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 27 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the ATM Cash Withdrawal Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	N/A
Completion	M
(Partial) Reversal	M
Data Capture	M

TABLE 27: FUNCTIONS USED FOR ATM CASH WITHDRAWAL

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the ATM Cash Withdrawal Service.

4.4.1.1 Configuration

Req A10: It shall be configured that chip processing shall be supported (see Req. TN2) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req. TN4).

4.4.1.2 Transaction Initialisation

Req A7: The Welcome Screen shall be shown initially in the default language and English (or in the default language only if it is English).

Req A8: Transactions on the ATM shall be initiated by card insertion or by cardholder interaction.

4.4.1.3 Cardholder Verification

Req A17: The Application shall support Online PIN as CVM.

4.4.1.4 Authorisation

Req A20: ATM Cash Withdrawal transactions shall be authorised online. Otherwise ATM transactions shall be declined.

4.4.1.5 Transaction Completion

Req A27: To minimise the risk of the cardholder leaving the card in the ATM; if the cardholder did not confirm proceeding with more transactions after the cash withdrawal, then the card removal shall always be prompted prior to the cash delivery.

Req A28: If the card is inserted in the reader of an ATM with capture card capability and if the cardholder does not retrieve his card, the Card shall be retained.

Req A32: If the Card is retained in response to the authorisation response message, an appropriate message shall be displayed to inform the cardholder.

Req A33: An ATM shall not allow a declined transaction to be accepted.

Req TN64: For contactless ATM Cash Withdrawal transactions further transactions after the cash withdrawal are not allowed without new presentment of the card.

4.4.1.6 Reversal

- Req A31: If the actual amount was authorised but no cash could be delivered, a reversal shall be performed to nullify the original authorisation.
- Req TN65: If the actual amount was authorised but only part of the requested cash could be prepared for delivery and if the ATM supports detection of partial delivery of cash, the ATM shall then perform a partial reversal. The captured data shall always include the final, reduced amount.

4.4.2 Cash Advance (attended)

TABLE 28 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Cash Advance Service.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip Contactless	✓	✗
Contactless with Mobile	✓	✗

TABLE 28: CASH ADVANCE: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 29 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Cash Advance Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	O
Completion	M
Reversal	C

Function	Requirement
Data Capture	M

TABLE 29: FUNCTIONS USED FOR CASH ADVANCE

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Cash Advance Service.

4.4.2.1 POI Application

Req TN66: The transaction amount shall be checked against a minimum allowed amount and/or a maximum allowed amount if configured for the Application Profile.

Req TN67: For Cash Advance, the cardholder shall be able to confirm the transaction amount and the payment product when performing the CVM.

4.4.2.2 Configuration

Req TN68: For Cash Advance, it shall be configured that chip processing (contact and/or contactless) shall be supported (see Req. TN2) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req. TN4).

Req TN69: It shall be possible to configure per Application Profile, if the transaction amount shall be checked against a minimum allowed amount and/or a maximum allowed amount.

4.4.2.3 Transaction Initialisation

Req TN70: For Cash Advance, the transaction amount (i.e. the authorised amount) shall be available to the POI Application at Transaction Initialisation.

4.4.2.4 Cardholder Verification

Req TN71: No CVM Required shall not be supported for the Cash Advance Service.

4.4.2.5 Authorisation

Req TN72: Cash Advance transactions shall be authorised online or - if the Referral Function is activated and Referral is requested by the Authorisation result - authorised by Referral. Otherwise Cash Advance transactions shall be declined.

4.4.2.6 Reversal

Req TN73: If the actual amount was authorised but no cash could be delivered, a reversal shall be performed to nullify the original authorisation.

4.5 Card Inquiry Services

4.5.1 Card Validity Check

TABLE 30 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Card Validity Check Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 30: CARD VALIDITY CHECK: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 31 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Card Validity Check Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	O
Authorisation	M
Referral	N/A
Completion	M
(Partial) Reversal	N/A
Data Capture	N/A

TABLE 31: FUNCTIONS USED FOR CARD VALIDITY CHECK

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Card Validity Check Service.

4.5.1.1 POI Application

Req TN74: A Card Validity Check transaction shall be performed like a Payment transaction, but using its own configuration and without displaying and printing the transaction amount.

4.5.1.2 Transaction Initialisation

Req TN75: For Card Validity Check, the authorised amount sent to the chip Card shall be set to 0.

4.5.1.3 Authorisation

Req TN76: Card Validity Check transactions shall be authorised online. Otherwise Card Validity Check transactions shall be declined.

Req TN77: Card Validity Check transactions shall be identified as such in the online authorisation.

4.5.1.4 Data Capture

Req TN78: Card Validity Check transactions shall not be captured for "Financial Presentment".

4.5.2 **Balance Inquiry**

TABLE 32 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Balance Inquiry Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 32: BALANCE INQUIRY: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 33 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Balance Inquiry Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C
Cardholder Verification	M
Authorisation	M
Referral	N/A
Completion	M
(Partial) Reversal	N/A
Data Capture	N/A

TABLE 33: FUNCTIONS USED FOR BALANCE INQUIRY

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Balance Inquiry Service.

4.5.2.1 POI Application

Req TN79: A Balance Inquiry transaction shall be performed like a Payment transaction, but using its own configuration and without displaying and printing the transaction amount.

4.5.2.2 Transaction Initialisation

Req TN80: For Balance Inquiry, the authorised amount sent to the chip Card shall be set to 0.

4.5.2.3 Authorisation

Req TN81: Balance Inquiry transactions shall be authorised online. Otherwise Balance Inquiry transactions shall be declined.

Req TN82: Balance Inquiry transactions shall be identified as such in the online authorisation.

Req TN83: The balance of the card account shall only be retrieved from a positive authorisation response.

4.5.2.4 Completion

- Req TN84: If the balance of the card account is retrieved from a positive authorisation response, it shall be displayed to the cardholder and printed on the cardholder receipt, if any.
- Req TN85: If Balance Inquiry is performed in an attended Acceptance Environment, the balance shall not be displayed to the attendant or printed on a merchant receipt.

4.6 Card Electronic Transfer

4.6.1 Card Funds Transfer

For the Card Funds Transfer Service it has to be distinguished whether the card account is credited or debited.

A credit of the card account is only allowed from an account that may be accessed with the card to be credited. Normally this requires pre-registration of the card for debiting the respective account. Such an account is called funding account. There may be more than one funding account (pre-registered) for a card. If several funding accounts are defined for a card, one of these accounts shall be defined as default. The entity that processes authorisations for the card shall know the funding account(s) defined for the card and which is the default funding account. In addition, this entity shall be able to get authorisation for debiting the funding account(s). It is out of scope how this is achieved.

Card Funds Transfer is a Cardholder Present transaction. The card acceptor for the Card Funds Transfer is not involved in the funds transfer to or from the card account but may receive a fee for offering the Service.

TABLE 34 shows which combinations of Acceptance Technologies for the funding card and Acceptance Environments are allowed (✓) or not allowed (✗) for the Card Funds Transfer Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 34: CARD FUNDS TRANSFER: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 35** shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Card Funds Transfer Service

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C

Function	Requirement
Cardholder Verification	M
Authorisation	M
Referral	N/A
Completion	M
Reversal	C
Data Capture	C

TABLE 35: FUNCTIONS USED FOR CARD FUNDS TRANSFER

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Card Funds Transfer Service.

4.6.1.1 POI Application

Req TN86: The Card Funds Transfer shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.6.1.2 Transaction Initialisation

Req TN87: The cardholder shall be able to select whether funds shall be transferred to the card account from another account (funding account) or whether funds shall be transferred from the card account to another account.

Req TN88: The cardholder shall be able to select the transaction amount to be credited to or debited from the card account.

Req TN89: In the case of a chip based Card Funds Transfer transaction, the transaction amount given to the chip during the Card Funds Transfer shall be set to zero to avoid unnecessary card risk management.

4.6.1.3 Card Data Retrieval

Req TN90: If funds shall be transferred to the card account from a funding account the cardholder shall have the opportunity either to select the default funding account or to provide information to identify one of the other funding accounts, if any. This information may be retrieved from the card for chip or mobile Acceptance Technology.

Req TN91: If funds shall be transferred from the card account to another account the cardholder shall have the opportunity to provide information to identify the account to be credited.

Req TN92: After the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date, the card acceptor may decide to raise a fee for the Card Funds Transfer Service.

The cardholder shall be informed of any fee to be paid to the card acceptor for the Card Funds Transfer and the cardholder shall have the opportunity to accept or decline the conditions of the Card Funds Transfer.

4.6.1.4 Authorisation

Req TN93: Card Funds Transfer transactions shall be authorised online and shall be identified as Card Funds Transfer.

Req TN94: The authorisation message shall identify the amount to be credited to or debited from the card account, the account to be debited or credited, and any fee raised by the card acceptor as an additional amount.

4.6.1.5 Data Capture

Req TN95: Data Capture for "Financial Presentment" is required only if the card acceptor raises a fee for the Card Funds Transfer.

4.6.2 Original Credit

TABLE 36 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Original Credit Service.

	Attended	Unattended
Chip with Contact	✓	✗
Magnetic Stripe	✓	✗
Manual Entry	✓	✗
Chip Contactless	✓	✗
Contactless with Mobile	✓	✗

TABLE 36: ORIGINAL CREDIT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 37 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Original Credit Service.

Function	Requirement
Language Selection	M
Transaction Initialisation	M

Function	Requirement
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	O
Referral	N/A
Completion	M
Reversal	C
Data Capture	M

TABLE 37: FUNCTIONS USED FOR ORIGINAL CREDIT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Original Credit Service.

4.6.2.1 POI Application

- Req T153: In the case of a chip based Original Credit transaction, the Original Credit shall follow EMV processing until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date. The chip process shall be terminated by requesting a decline from the card. The transaction amount given to the chip during the Original Credit should be zero to avoid unnecessary card risk management.
- Req TN96: The transaction amount shall be checked against a maximum allowed amount if configured for the Application Profile.

4.6.2.2 Configuration

- Req T151: The maximum amount and the allowed maximum amount that can be performed without additional security (e.g. a supervisor password) shall be configurable for the Original Credit Service.
- Req T154: It shall be configurable per Application Profile, whether the Original Credit is performed online or not.

4.6.2.3 Transaction Initialisation

Req T19: The Original Credit amount shall be available to the POI Application at Transaction Initialisation.

4.6.2.4 Authorisation

Req TN97: If required by the Application Profile, the Original Credit shall be authorised online.

4.6.3 Prepaid Card - Loading/Unloading

The Prepaid Card Loading Service requires that the cardholder and the issuer of the prepaid card have agreed on an account of the cardholder used to load/unload the prepaid card account. This account is called funding account.

The card acceptor for the Prepaid Card - Loading/Unloading is not involved in the funds transfer to or from the prepaid card account but may receive a fee for offering the Service.

TABLE 38 shows which combinations of Acceptance Technologies and Acceptance Environments are allowed (✓) or not allowed (✗) for the Prepaid Card - Loading/Unloading Service.

	Attended	Unattended
Chip with Contact	✓	✓
Magnetic Stripe	✓	✓
Manual Entry	✓	✗
Chip Contactless	✓	✓
Contactless with Mobile	✓	✓

TABLE 38: PRE-PAID CARD - LOADING: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 39 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Prepaid Card - Loading/Unloading Service

Function	Requirement
Language Selection	M
Transaction Initialisation	M
Technology Selection	M
Application Selection	M
Card Data Retrieval	M
Card Authentication	C

Function	Requirement
Cardholder Verification	M
Authorisation	M
Referral	N/A
Completion	M
Reversal	C
Data Capture	C

TABLE 39: FUNCTIONS USED FOR PREPAID CARD - LOADING/UNLOADING

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Prepaid Card - Loading/Unloading Service.

4.6.3.1 POI Application

Req TN98: The Prepaid Card Loading/Unloading shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.6.3.2 Transaction Initialisation

Req TN99: The cardholder shall be able to select whether the prepaid card shall be loaded or unloaded.

Req TN100: The cardholder shall be able to select the transaction amount to be loaded to or unloaded from the prepaid card account.

Req TN101: In the case of a chip based Prepaid Card Loading/Unloading transaction, the transaction amount given to the chip during the Prepaid Card Loading/Unloading shall be set to zero to avoid unnecessary card risk management.

4.6.3.3 Card Data Retrieval

Req TN102: After the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the expiry date, the card acceptor may decide to raise a fee for the Prepaid Card - Loading/Unloading Service.

The cardholder shall be informed of any fee to be paid to the card acceptor for the Prepaid Card Loading/Unloading and the cardholder shall have the opportunity to accept or decline the conditions of the Prepaid Card Loading/Unloading.

4.6.3.4 Authorisation

- Req TN103: Prepaid Card - Loading/Unloading transactions shall be authorised online and shall be identified as Prepaid Card - Loading/Unloading.
- Req TN104: The authorisation message shall identify the amount to be loaded or unloaded and any fee raised by the card acceptor as an additional amount.

4.6.3.5 Data Capture

- Req TN105: Data Capture for "Financial Presentment" is required only if the card acceptor raises a fee for the Prepaid Card Loading/Unloading.

4.7 Additional Features

4.7.1 Payment with Increased Amount

- Req TN106: Payment with Increased Amount shall be restricted to the Payment Service in the attended Acceptance Environment.
- Req TN107: Any extra amount shall be included in the transaction amount before or during Transaction Initialisation.
- Req TN108: The extra amount shall be displayed separately for transaction confirmation and printed on the receipt, if any.

4.7.2 Payment with Cashback

- Req T90: All requirements applicable to the Payment Service shall also apply to Payment with Cashback. Requirements that are specific for Payment with Cashback are listed below (separately).
- Req T91: Payment with Cashback shall be restricted to the Payment Service in the attended Acceptance Environment.
- Req T92: For a Payment with Cashback, the transaction amount shall be the total of the payment amount and the Cashback amount.
- Req T93: For a Payment with Cashback transaction, the Cashback amount(s) to be confirmed shall be displayed (with their unique label) to the cardholder in one of the following ways:
- Payment amount, Cashback amount and (total) transaction amount shall be displayed in this order. This method is preferred and shall be used if display size permits.
 - Cashback amount and (total) transaction amount shall be displayed.
 - Only (total) transaction amount shall be displayed.
- Req T94: Cardholder confirmation of the Cashback amount shall be implicit with the confirmation of the transaction amount.
- Req T95: For attended POIs that support Payment with Cashback, it shall be possible to configure per Application Profile to support the addition of a Cashback amount or not.
- Req T96: If a Cashback amount is entered for an Application Profile that does not support the addition of a Cashback amount, the transaction shall be declined.
- Req T97: For attended POIs that support Payment with Cashback, it shall be possible to configure per Application Profile a maximum Cashback amount.

- Req T98: For attended POIs that support Payment with Cashback, it shall be possible to configure whether the POI Application supports magnetic stripe processing for Payment with Cashback.
- Req T99: Payment with Cashback transactions shall be authorised online.
- Req T100: The POI Application shall support handling of an authorisation response indicating the payment part is authorised but the cashback is not.
- Req T101: If a receipt is printed for a Payment with Cashback transaction, then in addition to the data listed in Req T65 the following data shall also be printed:
- Payment amount
 - Cashback amount

4.7.3 Payment with Purchasing or Corporate Card Data

- Req TN109: For a POI Application that supports Payment with Purchasing or Corporate Card Data it shall be configurable per Application Profile whether this additional feature is activated for Payment.
- Req TN110: If a POI Application supports Payment with Purchasing or Corporate Card Data and if this additional feature is activated the POI shall be able to identify a purchasing or corporate card.
- Req TN111: If a Payment transaction is performed with a card for which the Payment with Purchasing or Corporate Card Data is activated in the POI Application, the additional data required for clearing of Payments with Purchasing or Corporate Card Data shall be stored and captured at the POI.

4.7.4 Payment with Aggregated Amount

- Req T73: When batch capture is used, if allowed by scheme rules, the Payment transactions may be aggregated by the acceptor before sending the transactions to the acquirer for capture.
- Req T74: When online capture methods are used, if allowed by scheme rules, only the Acquirer may aggregate the Payment transactions.
- Req T75: The maximum amount of the aggregated Payment transactions shall be defined by Scheme rules.
- Req T76: The chip based Payment transactions shall be aggregated separately from the magstripe Payment transactions.
- Req T77: The aggregation can only be made for the Payment transactions with the same PAN, the same merchant and for a maximum period of time. The maximum period of time is defined by scheme rules.
- Req T78: For aggregated chip based Payment transactions, the cryptogram of the last aggregated chip based transaction shall be sent together with the data elements used to calculate it.

4.7.5 Payment with Deferred Authorisation

- Req TN112: With the exception of Completion and Data Capture, all requirements applicable to the Payment Service shall also apply to Payment with Deferred Authorisation. Requirements that are specific for Payment with Deferred Authorisation are listed below (separately).
- Req TN113: Payment with Deferred Authorisation shall be restricted to the Payment Service in the attended Acceptance Environment.
- Req TN114: For attended POIs that support Payment with Deferred Authorisation, it shall be configurable which of the Acceptance Technologies supported for Payment are allowed for Deferred Authorisation.
- Req TN115: For attended POIs that support Payment with Deferred Authorisation, it shall be configurable whether Deferred Authorisation is initiated automatically or only on request of the attendant.
- Req TN116: For attended POIs that support Payment with Deferred Authorisation, it shall be possible to activate/deactivate Deferred Authorisation for Payment per Application Profile.
- Req TN117: For attended POIs that support Payment with Deferred Authorisation, a minimum amount and a maximum amount for Payment with Deferred Authorisation shall be configurable per Application Profile.
- Req TN118: For attended POIs that support Payment with Deferred Authorisation, it shall be configurable per Application Profile which of the CVMs supported for Payment are

allowed for Deferred Authorisation. Online PIN shall never be allowed for Payment with Deferred Authorisation.

- Req TN119: For attended POIs that support Payment with Deferred Authorisation, it shall be configurable per Application Profile whether Deferred Authorisation shall only be allowed for chip-based transactions if Offline Data Authentication was performed and successful.
- Req TN120: For attended POIs that support Payment with Deferred Authorisation, the configuration of the POI shall be checked during Completion, whether Deferred Authorisation is to be performed for the transaction in the following case: The Payment transaction shall be authorised online but the POI is (temporarily) unable to go online and the transaction is not subsequently authorised offline by the card. If necessary according to POI configuration, confirmation of the attendant shall be requested for Deferred Authorisation.
- Req TN121: If Deferred Authorisation shall not be performed the transaction shall be declined, and Completion and Data Capture for a declined Payment transaction are performed. This may include forcing acceptance by the attendant.
- Req TN122: If Deferred Authorisation shall be performed, Completion of an approved transaction shall be performed for the cardholder (display and receipt, if any).
- Req TN123: If Deferred Authorisation shall be performed, the transaction shall be stored in the POI and authorised online when the POI is again able to go online. In case of a chip-based transaction the chip data generated for online authorisation (including the ARQC) shall be stored and used for online authorisation.
- Req TN124: If Deferred Authorisation has been performed for a chip-based transaction, the chip data generated for online authorisation (including the ARQC) shall be used for Data Capture.

4.7.6 Dynamic Currency Conversion (DCC)

If not stated otherwise, in this section "terminal" denotes a POI in the merchant environment as well as an ATM.

- Req TN125: It shall be configurable per Application Profile, whether DCC is supported.
- Req T102: To perform DCC, the terminal or attendant shall give the cardholder the choice of currency they want to be billed in, the cardholder's currency or the card acceptor's currency.

To make this choice, before confirming the Payment, the cardholder shall be informed of

- the original transaction amount in the card acceptor's currency,
- the transaction amount in the cardholder's currency and
- the conversion rate (ratio) between these two amounts.

- Req T103: If the terminal is used to offer the choice to the cardholder, in particular if DCC is performed on an ATM, the following items shall be displayed to the cardholder:
- the original transaction amount in the card acceptor's currency together with an indication of the currency,
 - the transaction amount in the cardholder's currency together with an indication of the currency and
 - the conversion rate (ratio) between these two amounts,
- and the cardholder shall have the opportunity to select the currency the transaction will be performed in.
- Req T104: If the cardholder selects the transaction amount in the cardholder's currency, then the cardholder's currency shall become the transaction currency and all applicable amounts, such as transaction amount, floor limits, a Cashback amount¹⁰, and/or a surcharge/rebate amount shall be in the cardholder's currency when used to perform the Card Service.
- Req T105: If the cardholder selects the transaction amount in the card acceptor's currency, then the card acceptor's currency shall remain the transaction currency and all applicable amounts shall be in the card acceptor's currency when used to perform the Card Service as if no DCC option was offered.
- Req T106: If the cardholder has selected the transaction amount in the cardholder's currency and if a transaction receipt is printed for the cardholder, for all amounts printed on the receipt in the cardholder's currency (i.e. the transaction currency) the original amount in the card acceptor's currency and the conversion rate used shall also be printed.
- Req T107: If for a chip-based transaction data from the chip are needed to determine the cardholder's currency, then the transaction shall be started with the card acceptor's currency. If after the retrieval of the necessary data the cardholder has selected the transaction amount in the cardholder's currency, then the chip-based transaction shall be re-started without further cardholder interaction with the previously selected application.

4.7.7 Surcharging/Rebate

- Req T199: In the merchant environment, any kind of surcharge/rebate will be part of the agreed total sales amount. Therefore the POI Application shall not support any specific handling of surcharging/rebate for Card Services¹¹.

¹⁰ Cash obtained from the card acceptor in the process of Cash back may however be in the card acceptor's currency.

¹¹ Note that surcharging/rebate is subject to scheme or legal regulations.

- Req A34: If a surcharge/rebate is applied at the ATM for a Cash Withdrawal, the surcharge/rebate shall be displayed to the cardholder prior to authorisation, and the cardholder shall have the opportunity to abort the transaction or to continue with the understanding of a surcharge/rebate being applied.
- Req A35: For a Cash Withdrawal with surcharge/rebate, the transaction amount shall be the total of the withdrawal amount and the surcharge/rebate amount.

5 PROTOCOL FUNCTIONAL REQUIREMENTS

This section defines core functional requirements for Volume conformance for protocols. The term protocol is used to mean the data exchange messages that are used to perform the different functions covered in this document ("Authorisations", "Financial Presentments", "Reversals" ...).

The term T2A protocol denotes the data exchange messages that are used between POI and acquirer. There are many different configurations how a POI may be connected to one or more acquirers. The configuration depends on the infrastructure. Data elements in messages can be populated at the POI or in some cases by an intermediate host (terminal provider host, merchant host etc.) before the messages reach the acquirer.

Some examples of different configurations are given below. Other configurations are possible. However, the requirements for the T2A protocol stated in this section apply to all such configurations (see Req. P8 below).

POI connected directly to an acquirer host:



FIGURE 40: POI CONNECTED DIRECTLY TO AN ACQUIRER HOST

POI directly connected to several acquirers:

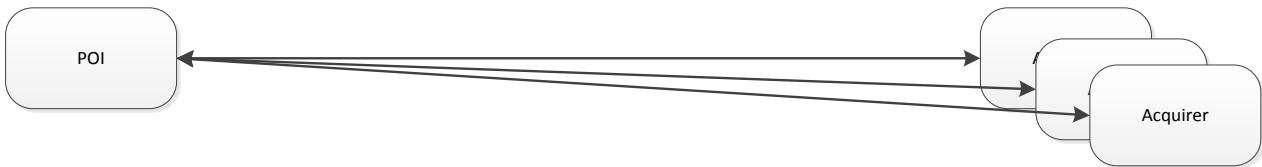


FIGURE 41: POI DIRECTLY CONNECTED TO SEVERAL ACQUIRERS

Environment of large retailer:

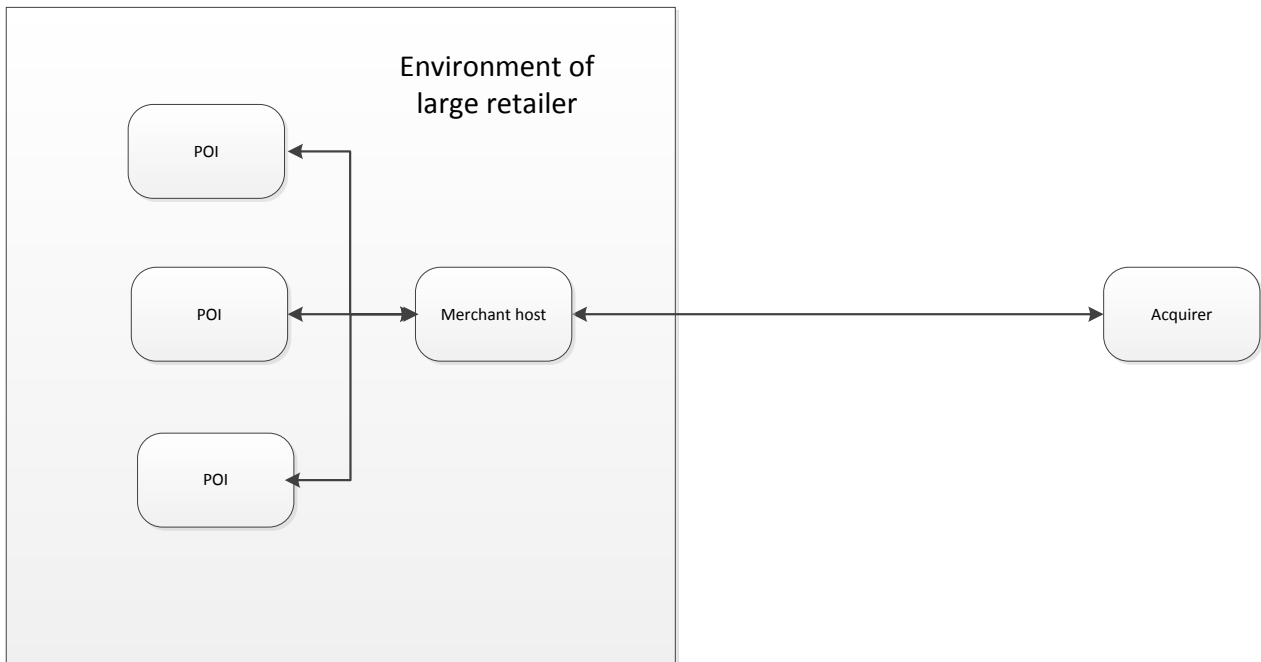


FIGURE 42: ENVIRONMENT OF LARGE RETAILER

Environment of a terminal provider:

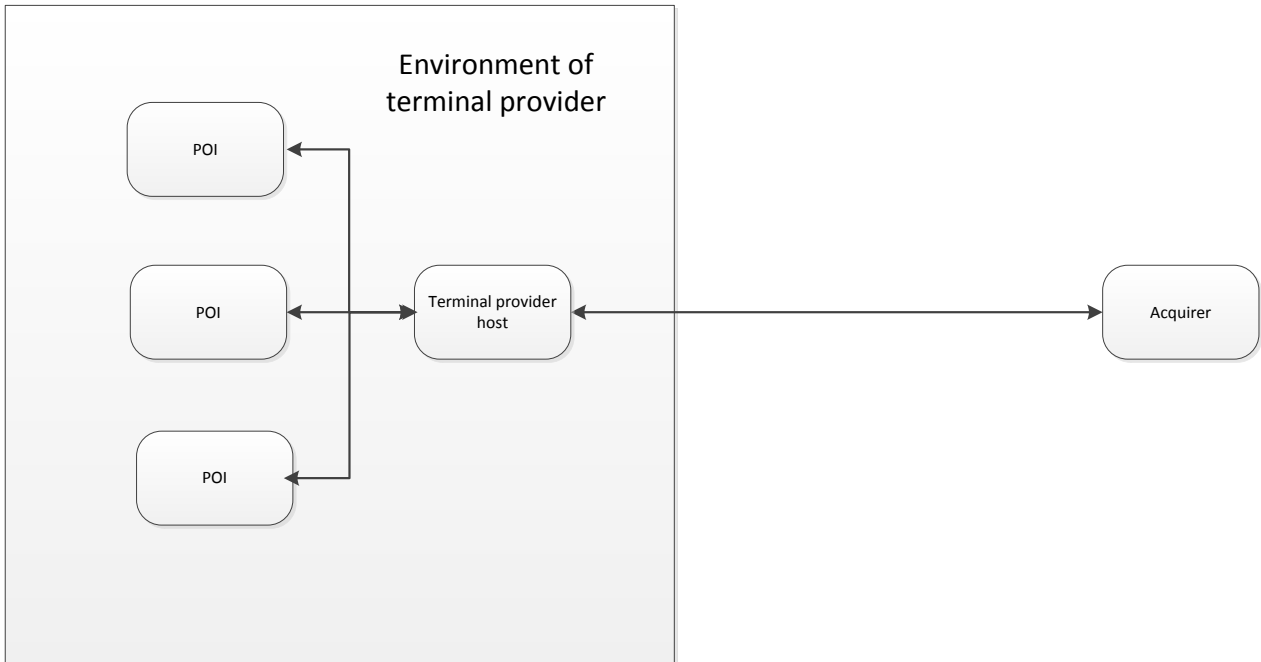


FIGURE 43: ENVIRONMENT OF A TERMINAL PROVIDER

Environment with an intermediate agent:



FIGURE 44: ENVIRONMENT WITH AN INTERMEDIATE AGENT

Intermediate host connected to several acquirers:



FIGURE 45: INTERMEDIATE HOST CONNECTED TO SEVERAL ACQUIRERS

- Req P1: The T2A protocols shall support the Card Services according to the description in this document.
- Req P2: For implemented services, the protocols shall support all corresponding Data Elements as defined in Book 3.
- Req P3: The protocols shall be independent of the communication channel.

- Req P4: The protocols shall support SEPA conformant schemes but should not exclude non SEPA conformant schemes.
- Req P5: The protocols and the communication layers shall support the security requirements on integrity and confidentiality of the information conveyed as defined in Book 4.
- Req P6: The protocols shall support a unique message identification, so to be able to detect duplicate messages.
- Req P7: The protocols should permit to transport additional data other than the ones defined in this document.
- Req P8: The T2A protocols shall be designed to accommodate all types of POI architectures (e.g. standalone POIs to high-end distributed POI systems).
- Req P9: The T2A protocols shall support one of the following capture modes for transactions:
- Online capture through the authorisation message
 - Online capture through a separate completion message
 - Batch capture through file transfer, or transaction by transaction
- Req P10: The T2A protocols shall support to send an online message which notifies the result of the successful online authorisation, either never, or always, or only if requested by an entity in the online approval.
- Req P11: The T2A protocols shall be designed to allow POIs to process transactions with different acquirers.

6 FIGURES AND TABLES

TABLE 1: BOOK 2 SCOPE9

FIGURE 2: POI APPLICATION - LOGICAL STRUCTURE AND CONFIGURATION PARAMETERS13

TABLE 3: PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS.....25

TABLE 4: FUNCTIONS USED FOR PAYMENT25

TABLE 5: REFUND: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS28

TABLE 6: FUNCTIONS USED FOR REFUND.....29

TABLE 7: CANCELLATION: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS30

TABLE 8: FUNCTIONS USED FOR CANCELLATION.....30

TABLE 9: PRE-AUTHORISATION SERVICES: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS33

TABLE 10: FUNCTIONS USED FOR PRE-AUTHORISATION AND UPDATE PREAUTHORISATION...33

TABLE 11: FUNCTIONS USED FOR PAYMENT COMPLETION36

TABLE 12: DEFERRED PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS37

TABLE 13: FUNCTIONS USED FOR DEFERRED PAYMENT38

TABLE 14: NO SHOW: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS40

TABLE 15: FUNCTIONS USED FOR NO SHOW40

TABLE 16: INSTALMENT PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION.....41

TABLE 17: FUNCTIONS USED FOR FIRST TRANSACTION OF AN INSTALMENT PAYMENT.....42

TABLE 18: INSTALMENT PAYMENT: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS FOR SUBSEQUENT TRANSACTIONS43

TABLE 19: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF AN INSTALMENT PAYMENT43

TABLE 20: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION.....45

TABLE 21: FUNCTIONS USED FOR FIRST TRANSACTION OF A RECURRING PAYMENT46

TABLE 22: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS FOR SUBSEQUENT TRANSACTIONS46

TABLE 23: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF A RECURRING PAYMENT 47

TABLE 24: QUASI-CASH PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS48

TABLE 25: FUNCTIONS USED FOR QUASI-CASH PAYMENT48

TABLE 26: ATM CASH WITHDRAWAL: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS50

TABLE 27: FUNCTIONS USED FOR ATM CASH WITHDRAWAL50

TABLE 28: CASH ADVANCE: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	52
TABLE 29: FUNCTIONS USED FOR CASH ADVANCE	53
TABLE 30: CARD VALIDITY CHECK: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	55
TABLE 31: FUNCTIONS USED FOR CARD VALIDITY CHECK.....	55
TABLE 32: BALANCE INQUIRY: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	56
TABLE 33: FUNCTIONS USED FOR BALANCE INQUIRY.....	57
TABLE 34: CARD FUNDS TRANSFER: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	59
TABLE 35: FUNCTIONS USED FOR CARD FUNDS TRANSFER	60
TABLE 36: ORIGINAL CREDIT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	61
TABLE 37: FUNCTIONS USED FOR ORIGINAL CREDIT	62
TABLE 38: PRE-PAID CARD - LOADING: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS	63
TABLE 39: FUNCTIONS USED FOR PREPAID CARD - LOADING/UNLOADING.....	64
FIGURE 40: POI CONNECTED DIRECTLY TO AN ACQUIRER HOST.....	72
FIGURE 41: POI DIRECTLY CONNECTED TO SEVERAL ACQUIRERS	72
FIGURE 42: ENVIRONMENT OF LARGE RETAILER	73
FIGURE 43: ENVIRONMENT OF A TERMINAL PROVIDER.....	74
FIGURE 44: ENVIRONMENT WITH AN INTERMEDIATE AGENT	74
FIGURE 45: INTERMEDIATE HOST CONNECTED TO SEVERAL ACQUIRERS.....	74

