ECSG001-17 01.03.2017

(Vol Ref. 8.2.00)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

STANDARDS' REQUIREMENTS

BOOK 2

FUNCTIONAL REQUIREMENTS

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	ECSG001-17
Issue	Book 2 - v8.2.00
Date of Version	1 March 2017
Reason for Issue	Publication
Reviewed by	Approved for publication by the ECSG Board of 9 February 2017
Produced by	ECSG Secretariat
Owned and Authorised by	ECSG
Circulation	Public

European Cards Stakeholders Group AISBL - Cours Saint-Michel 30 - B 1040 Brussels
Tel: +32 2 733 35 33 Fax: +32 2 736 49 88 Enterprise N° 656.829.362 www.e-csg.eu secretariat@e-csg.eu

Change History of Book 2		
6.2.0.x	2012-2013	Working version of Book 2
7.2.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.2.1.0x	2014-2015	Working version 2014-2015
7.2.1.05	11.02.2015 (published 10.03.2015)	Consultation version 2015
7.2.2.1	08.12.2015	EPC Published version - Volume v7.1
7.2.2.11-7.2.2.5	16.12.2015-	Working Version 2015-2016
8.2.00	01.03.2017	ECSG Published version - Volume v8.0

Table of Contents

1 GENERAL

1.1 Book 2 - Executive Summary

This book defines functional requirements for Local and Remote Card Transactions for the provision of the Card Services listed in Section 2.

These Card Services,

- ⇒ Involve, in general, a Cardholder and their Issuer, an Acceptor and their Acquirer;
- ⇒ Refer to Services where the Cardholder and the Acceptor interact using a particular *Cardholder Environment* within a particular *Acceptance Environment* supporting *Cardholder Verification Methods and Card Authentication Methods;*
- ⇒ Are processed through a succession of *Functions* which may be executed in the Physical Card or Consumer Device, in the Physical or Remote POI, in the Terminal to Acquirer Domain, and in the Acquirer to Issuer domain.

Section 2 describes the scope of this book by presenting an overview in the following Tables:

Table 1: Usage of Acceptance Environments and Cardholder Environments for Local and Remote Transactions

Table 2: Book 2 Scope

Table 3: Mapping of Acceptance Technologies to Cardholder Environments

Section 3 defines core functional requirements for Cardholder Environments.

Section 4 defines core functional requirements for the POI.

Section 5 lists core functional requirements for protocols.

Details on security requirements may be found in Book 4.

References, definitions of terms and abbreviations are provided in Book 1.

Note: Card and POI Application implementations may support additional functionality, provided they do not conflict with the Volume requirements.

1.2 Description of Changes since the Last Version of Book 2

This new version of Book 2 dedicated to functional requirements was amended to incorporate the following:

- Book 2 has been updated as described in the Bulletin 001 published by the EPC on 29 February 2016 taking into account an editorial improvement proposed by EMVCo. In particular, Section 3.2 has been inserted in Book 2 describing how to use the data object defined by EMVCo for Electronic Product Identification, easing the compliance with the Interchange Fee Regulation [IFR].

- The POI functional requirements on Selection of the Application have been updated to cover Cardholder override in contactless and to clarify that there is no restriction regarding the chronological order of events in terms of giving the Cardholder the right to override.

- In the description of Pre-Authorisation Services additional detail on the unique ID (linking the steps of Pre-Authorisation) has been added.

- General implementation guidelines have been moved from Book 6 to Book 2; this is the case for Card Data Authentication Methods as well as for PIN based Cardholder Verification Methods for issuance side.

2 SCOPE

This Volume differentiates between Local and Remote Card Transactions.

- A **Local Card Transaction** is a Card Transaction conducted at the Acceptor's Physical POI which may be Attended (including Semi-Attended) or Unattended. A Local Transaction is normally[1] initiated by the Cardholder using a Physical Card (Contact or Contactless) or an MCP Application on a Mobile Device.

- A **Remote Card Transaction** is a Card Not Present transaction which is e-commerce, m-commerce or MOTO:

  - **e- and m-commerce** Transactions are normally[2] initiated by the Cardholder using a Consumer Device and conducted via a Virtual POI to buy products and services over the internet.

    If the Consumer Device is an Electronic Device, this is referred to as an e-commerce transaction.

    If the Consumer Device is a Mobile Device, this is referred to as an m-commerce transaction.

  - **MOTO** Transactions are conducted in the Acceptor's environment and initiated by the Acceptor, normally[2] using Manual Entry with the Cardholder interacting remotely for MOTO.

    A Physical POI, configured to handle Card Not Present transactions or a Virtual Terminal may be used to process the Card Data.

An overview of the Acceptance Environments, the entity operating the POI in those environments and the Acceptance Technologies used in the Acceptance and Cardholder Environments, is shown in the following Table.

---

1 For Pre-Authorisation Services, No Show, subsequent transactions of Instalment Payments and Recurring Payments, Local Transactions may be initiated by the Acceptor based on Stored Card Data.

2 For some Card Services, Remote Transactions may be initiated by the Acceptor based on Stored Card Data, e.g., No Show, subsequent transactions of Instalment Payments and Recurring Payments.

	Local Transactions		Remote Transactions		
Environment	Physical POI		Physical POI	Remote POI	
Acceptance Environments:	Attended/Semi-Attended POI	Unattended POI	Attended POI	Virtual Terminal	Virtual POI
Operated by:	Acceptor/Cardholder[3]	Cardholder	Acceptor	Acceptor/Cardholder[4]	Cardholder
Type of Transaction:	Local Transactions in Acceptors environment and attended by the Acceptor	Local Transactions in Acceptors environment, but not attended by the Acceptor.	MOTO in an Acceptor attended environment.	MOTO	e- & m-commerce
Cardholder Environment:	Physical Card or Consumer Device[5] or no Cardholder Environment involved[6]	Physical Card or Consumer Device[5]	Physical Card or Virtual Card or no Cardholder Environment involved[6]	Physical Card or Virtual Card or no Cardholder Environment involved[6]	Physical[7] Card or Virtual Card or Consumer Device or no Cardholder Environment involved[6]
Acceptance Technologies:	Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe, Manual Entry by Acceptor, Stored Card Data (stored by Acceptor)[6]	Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe	Manual Entry by Acceptor, Stored Card Data (Stored by Acceptor)[6]	Manual Entry by Acceptor or by Cardholder[4], Stored Card Data (Stored by Acceptor)[6]	Manual Entry by Cardholder, Payment Credentials on Consumer Device, Payment Credentials on Consumer Device with Authentication Application, (M)RP Application on Consumer Device, Stored Card Data (Stored by Acceptor)[6]

TABLE 1: USAGE OF ACCEPTANCE ENVIRONMENTS AND CARDHOLDER ENVIRONMENTS FOR LOCAL AND REMOTE TRANSACTIONS

3 Cardholder only if Semi-Attended

4 Cardholder only if DTMF used

5 Using the Mobile Device for Mobile Contactless

6 This concerns Card Services which are based on Stored Card Data and therefore do not involve any Cardholder Environment, e.g., No Show, subsequent transactions of Instalment Payments and Recurring Payments.

7 In some scenarios an EMV Authentication Application stored on a Physical Card, in combination with an Additional Authentication Device, may be used.

Table 2 below represents the scope of Book 2 and lists for Local and Remote Transactions which of the following items are or are not covered by the Volume (this is indicated by a "Y" or "N" respectively):

⇒ Card Services

⇒ Cardholder Environments and Acceptance Environments

⇒ Acceptance Technologies

⇒ Cardholder Verification Methods and Card Authentication Methods

"Y" also indicates that the item is allowed for a specific transaction type.

"N" also indicates that the item is not allowed for a specific transaction type.

"N/A" indicates that the item is not covered in this version of the Volume but may be covered in future releases.

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

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
CARD SERVICES			
PAYMENT SERVICES			
Payment	**Y**	**Y**	**Y**
Refund (partial or total)	**Y**	**Y**	**Y**
Cancellation	**Y**	**Y**	**Y**
Pre-Authorisation Services • **Pre-Authorisation** • **Update Pre-Authorisation** • **Payment Completion**	**Y**	**Y**	**Y**
Deferred Payment	**Y**	**N**	**N**
No-Show	**Y**	**N**	**N**

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
Instalment Payment	Y	Y	Y
Recurring Payment	Y	Y	Y
Quasi-Cash Payment	Y	Y	Y
CASH SERVICES			
ATM Cash Withdrawal	Y	N	N
Cash Advance (attended)	Y	N	N
Cash Deposit	N/A	N/A	N/A
CARD INQUIRY SERVICES			
Card Validity Check	Y	Y	Y
Balance Inquiry	Y	N/A	N
CARD ELECTRONIC TRANSFER			
Card Funds Transfer	Y	Y	N
Original Credit	Y	Y	Y
Prepaid Card - Loading & Unloading	Y	Y	Y
e-Purse - Loading/Unloading	N/A	N/A	N/A
ADDITIONAL FEATURES			
Payment with Increased Amount	Y	N	N
Payment with Cashback	Y	N	N
Payment with Purchasing or Corporate Card Data	Y	Y	Y
Payment with Aggregated Amount	Y	Y	Y
Payment with Deferred Authorisation	Y	Y	N
Dynamic Currency Conversion (DCC)	Y	Y	Y
Surcharging/Rebate	Y	Y	Y
Payment with Deferred Clearing	N/A	N/A	N/A
Payment with Loyalty Information	N/A	N/A	N/A
Unsolicited Available Funds	N/A	N/A	N/A
CARD MANAGEMENT SERVICES			
PIN Change / Unlock	N/A	N/A	N/A
Card Activation	N/A	N/A	N/A
Return Card to Cardholder Request	N/A	N/A	N/A

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
Card Pick-up Advice	N/A	N/A	N/A
Return Card Advice	N/A	N/A	N/A
ACCEPTANCE TECHNOLOGIES			
Chip with Contact	Y	N	N
Magnetic Stripe	Y	N	N
Chip Contactless[8]	Y	N	N
Mobile Contactless[8]	Y	N	N
Manual Entry by Acceptor[9]	Y	N	Y
Manual Entry by Cardholder[10]	N	Y	N[11]
Stored Card Data (stored by the Acceptor)[10]	Y	Y	Y
Consumer Device with Payment Credentials[10]	N	Y	N
Consumer Device with Payment Credentials and Authentication Application[10]	N	Y	N
Consumer Device with (M)RP Application[10]	N	Y	N
Imprint	N/A	N/A	N/A

8 If it is not necessary to distinguish the Cardholder Environment in use, Chip Contactless and Mobile Contactless are referred to as Contactless Acceptance Technology, because they are both implementations of [EMV D] and communication and behaviour are the same from the perspective of the POI

9 Acceptor may also stand for an Attendant in the Acceptor's environment

10 This Acceptance Technology is used for remote transactions

11 Except if a touch-tone facility on a telephone handset is supported for Telephone Orders

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
CARDHOLDER ENVIRONMENTS			
Physical Card	**Y**	**Y**	**Y**[12]
Consumer Device	**Y**[13]	**Y**	**N**
Virtual Card	**N**	**Y**	**Y**
ACCEPTANCE ENVIRONMENTS			
Physical POI			
Attended[14]	**Y**	**N**	**Y**
Unattended	**Y**	**N**	**N**
Remote POI			
Virtual POI	**N**	**Y**	**N**
Virtual Terminal	**N**	**N**	**Y**
CARDHOLDER VERIFICATION METHODS			
EMV Offline Plaintext PIN[15]	**Y**	**Y**	**N**
EMV Offline Enciphered PIN15	**Y**	**Y**	**N**
Online PIN	**Y**	**N**	**N**
Signature	**Y**	**N**	**N**[16]
No CVM Required	**Y**	**Y**[17]	**N**
Biometrics	**N/A**[18]	**N/A**[18]	**N/A**[18]

12 Using the relevant data extracted from the Card

13 Using the Mobile Device for Mobile Contactless

14 According to the definition in Book 1, this Acceptance Technology also comprises Semi-Attended.

15 Where this Book refers to "Offline PIN", it is referring to both EMV Offline Plaintext PIN and EMV Offline Enciphered PIN

16 However, a mail order form contains a cardholder signature

17 The No CVM Required goes beyond the verification process defined by EMV (see 4.2.3.7.2).

18 Biometrics is recognised as a technology which may be used for CVM purposes. However, the CSG considers that, as Biometrics as a CVM is still evolving, this version of the Volume is not identifying specific requirements for this technology. The CSG will continue to analyse Biometrics in the context of Card Services. Future versions of the Volume will provide functional requirements for the use of Biometrics as a CVM.

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
Offline Mobile Code[19]	Y	Y	N
Online Mobile Code	N	Y	N
Offline Personal Code	N	Y	N
Online Personal Code	N	Y	N
CARD AUTHENTICATION METHODS			
EMV Offline SDA	Y	Y	N
EMV Offline DDA	Y	Y	N
EMV Offline CDA	Y	Y	N
EMV Offline fDDA[20]	Y	N	N
EMV Online Authentication	Y	Y	N
Static Authentication[21]	Y	Y	Y
Dynamic Authentication - One Time Password (OTP)[22]	N	Y	N
Dynamic Authentication - Challenge Response based on Additional Authentication Device[22]	N	Y	N
Dynamic Authentication - Challenge Response based on Authentication/Remote Payment Application on a Consumer Device[22]	N	Y	N
FUNCTIONS			
Configuration	Y	Y	Y
Transaction Initialisation	Y	Y	Y
Language Selection	Y	Y	N
Technology Selection	Y	N	N
Selection of the Application	Y	Y	Y[23]

19 Offline Mobile Code and Biometrics verified on the Consumer Device are examples of CDCVM. The use of Biometrics verified on the Consumer Device will be expanded upon in the next version of the Volume.

20 Only applicable to the contactless Acceptance Technologies

21 Typically the Card Security Code (CSC) is used.

22 This Card Authentication Method is used for e- and m-commerce and may use EMV authentication methods.

23 Only the Application Profile is selected

	SCS Volume Book 2 Scope		
	Transactions		
	Local	Remote	
		e- and m-commerce	MOTO
Card Data Retrieval	Y	Y	Y
Card Authentication	Y	Y[24]	Y[24]
Cardholder Verification	Y	Y	N
Authorisation	Y	Y	Y
Referral	Y	N	N
Completion	Y	Y	Y
Reversal	Y	Y	Y
Data Capture	Y	Y	Y
Financial Presentment	N/A	N/A	N/A
Settlement	N/A	N/A	N/A
Chargeback	N/A	N/A	N/A
ADMINISTRATIVE SERVICE			
Reconciliation	N/A	N/A	N/A

TABLE 2: BOOK 2 SCOPE

Table 3 shows which Acceptance Technologies can be used to retrieve Card Data from the Cardholder Environments.

ACCEPTANCE TECHNOLOGIES	CARDHOLDER ENVIRONMENTS		
	Physical Card	Virtual Card	Consumer Device
Chip with Contact	Y	N	N
Magnetic Stripe	Y	N	N
Chip Contactless	Y	N	N
Mobile Contactless	N	N	Y

[24] Cardholder authentication is an important issue in the remote environment. In this environment the boundaries between authentication and / or verification of the Card and the Cardholder may become blurred. However, for this version of the Volume, the functions Card Authentication and Cardholder Verification have been kept separate to respect compatibility with the functions defined for Local Transactions.

ACCEPTANCE TECHNOLOGIES	CARDHOLDER ENVIRONMENTS		
	Physical Card	Virtual Card	Consumer Device
Manual Entry by Acceptor	Y	N	N
Manual Entry by Cardholder	Y	Y	N
Stored Card Data (stored by the Acceptor)[25]	N/A	N/A	N/A
Payment Credentials on Consumer Device	N	N	Y
Payment Credentials on Consumer Device with Authentication Application	N	N	Y
(M)RP Application on Consumer Device	N	N	Y

TABLE 3: MAPPING OF ACCEPTANCE TECHNOLOGIES TO CARDHOLDER ENVIRONMENTS

[25] For Acceptance Technology Stored Card Data, PAN and Expiry Date will have been provided earlier. Therefore no Cardholder Environment is involved, which is denoted as "N/A".

3 FUNCTIONAL REQUIREMENTS FOR CARDHOLDER ENVIRONMENTS

3.1 Introduction

This section defines core functional requirements for Volume conformance for the Cardholder Environment.

3.2 Electronic Product Identification

In the Application Selection Registered Proprietary Data (tag '9F0A'), the ID '0001' for EEA Product Identification has been allocated by EMVCo to the ECSG in line with [IFR].

- The value field for ID '0001' has a variable length of 1 to 5 bytes.
- The format of the value field is binary.
- The first byte is defined as follows:

Value	IFR Product Type
'01'	Debit Product
'02'	Credit Product
'03'	Commercial Product
'04'	Prepaid Product
All other values	Reserved for future use

- Bytes 2 to 5 are reserved for future use by the ECSG and if present, they shall be filled with '00' for this version of the Volume.
- Presence of tag '9F0A' with ID = '0001' indicates an EEA issued card.

Electronic Product Identification only applies to Chip with Contact, Chip Contactless and Mobile Contactless.

3.3 Local Transactions

For Local Transactions, the Cardholder Environments Physical Card or Consumer Device[26] are used. Functional requirements for Card Applications in these Cardholder Environments are defined in section 3.3.1 for the Acceptance Technology Chip with Contact and in section 3.3.2 for the Acceptance Technologies Chip Contactless and Mobile Contactless.

[26] Using the Mobile Device for Mobile Contactless

3.3.1 Chip with Contact

Req C1: The Physical Card-to-Reader 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 B1].

Req C2: Physical Cards shall support Application Selection through PSE according to [EMV B1][27].

Req C3: PSE and Card Applications shall include the Language Preference data element and the Application Selection Registered Proprietary Data.

It is recommended that the Language Preference also includes English to ease use in international markets.

The Application Selection Registered Proprietary Data with ID = '0001' shall be present:

- In the Directory Discretionary data (tag '73') within every ADF Directory Entry,
- AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of every ADF.

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

Card Applications may support either Offline Enciphered PIN or Offline Plaintext PIN or both. Offline Enciphered PIN is preferred and required for newly issued and replacement cards. Offline Plaintext PIN may still be present in the CVM List for use outside EEA, but only with a lower priority than Offline Enciphered PIN.

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

Req C5: Card Applications shall support Online Authentication as defined by [EMV].

Req C6: Card Applications that support offline transactions shall support Offline Data Authentication as follows:

- SDA is not permitted on newly issued cards.

[27] The support of "Payment System Environment" (PSE) by the Physical Card is optional in [EMV B1]. The support of PSE is mandatory for SEPA compliance as defined in Req C2.

- DDA is mandatory.
- CDA is mandatory on newly issued cards.

Card Applications that support only online transactions shall support Offline Data Authentication as follows:

- SDA is not permitted on newly issued cards.
- DDA is mandatory on newly issued cards.
- CDA is mandatory on newly issued cards.

3.3.2 Chip and Mobile Contactless

Req C7: The Physical Card or Mobile Device-to-Reader communication shall be compliant with [EMV D].

Req C8: (Mobile) Contactless Card Applications shall comply with any card requirements in [EMV A] and [EMV B].

Req C9: The (Mobile) Contactless Card Application shall allow identification of the Form Factor for use in authorisation and data capture.

Req C10: Physical Cards and Mobile Devices shall support Combination Selection through PPSE according to the card requirements in [EMV B].

Req C11: Mobile Contactless Card Applications and Mobile Devices shall be compliant with [EMV M1], [EMV M2].

Req C12: The PPSE and the Card Applications shall include the Application Selection Registered Proprietary Data.

The Application Selection Registered Proprietary Data with ID = '0001' shall be present:

- In every Directory Entry (tag '61') within the FCI of the PPSE,
- AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of every ADF.

3.4 MOTO

In MOTO transactions, the Cardholder Environment Physical Card or Virtual Card is used.

Req C13: Card Data shall be derived from either a Physical or a Virtual Card and shall include a PAN, Expiration date and Card Security Code (CSC).

3.5 e- and m-commerce

For e- and m-commerce, Card Data may be entered on a Consumer Device or may be derived from data stored on a Consumer Device. This may include a (Mobile) Remote Payment Application or Cardholder Payment Credentials. In addition, the Cardholder Payment Credentials may be combined with an Authentication Application. Entering Card Data on a Consumer Device may also require the use of a Physical Card or a Virtual Card. For some Services, also Stored Card Data can be used.

Req C14: If a (Mobile) Remote Payment Application, Cardholder Payment Credentials or an Authentication Application is used, they shall be stored in a Secure Environment accessible via the Consumer Device.

Req C15: A (Mobile) Remote Payment Application or an Authentication Application shall support a Dynamic Authentication method listed in Table 2.

Req C16: A (Mobile) Remote Payment Application or an Authentication Application shall support one of the following CVMs: "No CVM Required" or "Personal/Mobile Code" (online or offline). If an Additional Authentication Device is used with an EMV Card Authentication Application on a Physical Card, "Offline PIN" shall be supported as CVM by the EMV Card Authentication Application.

Req C17: Whether a Physical Card, a Virtual Card, Payment Credentials, or an Authentication / (M)RP Application is involved in the Remote Transaction shall be identifiable by the issuer.

Req C18: Card Data used for Manual Entry shall include PAN, Expiration date and Card Security Code (CSC).

4 POI FUNCTIONAL REQUIREMENTS

4.1 Introduction

This section defines core functional requirements for Volume conformance for POI Applications on Physical and Remote POIs including Virtual POIs and Virtual Terminals. This includes ATM Applications since ATMs are specific Physical 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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal):

- For the POI Application,
- For the Configuration Function and
- For the Functions used for transaction processing.

Section 4.2 is followed by sections detailing the specific functional requirements for each individual Card Service.

The sections on the individual Card Services are grouped according to section 2 as follows:

- Payment Services (section 4.3),
- Cash Services (section 4.4),
- Card Inquiry Services (section 4.5) and
- Card Electronic Transfer (section 4.6).

These sections contain the following for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal):

- Allowed combinations of Acceptance Technologies and Acceptance Environments for each Card Service.
- Applicability of the Functions for each Card Service in the different Acceptance Environments.
- 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 as appropriate.

Section 4.7 contains requirements that apply to the Additional Features.

A functional requirement for POI Applications is only applicable to POI Application implementations which support the Card Service and/or Function addressed by the requirement.

If it is not necessary to distinguish the Cardholder Environment in use, the term "Contactless" is used to refer to both Acceptance Technologies, Chip Contactless and Mobile Contactless, because they are both implementations of [EMV D] and communication and behaviour are the same from the perspective of the POI.

The requirement T6 below provides for the usage of kernels according to [EMV C] 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 an application consisting of software and data used to perform a Card Service. Depending on the architecture of the POI, the POI Application may be implemented on one component or distributed on several components.

4.2.1.1 Local Transactions, e- and m-commerce and MOTO (Physical POI, Virtual POI and Virtual Terminal)

Req T1: The POI Application shall support processing with multiple acquirers.

4.2.1.2 Local Transactions (Physical POI)

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, for example:
    - define the limits to be used;

- restrict functionality for accepting EEA issued cards, e.g. CVM supported.

The way Application Profiles are referenced is described in Req T52, T54 and T55.

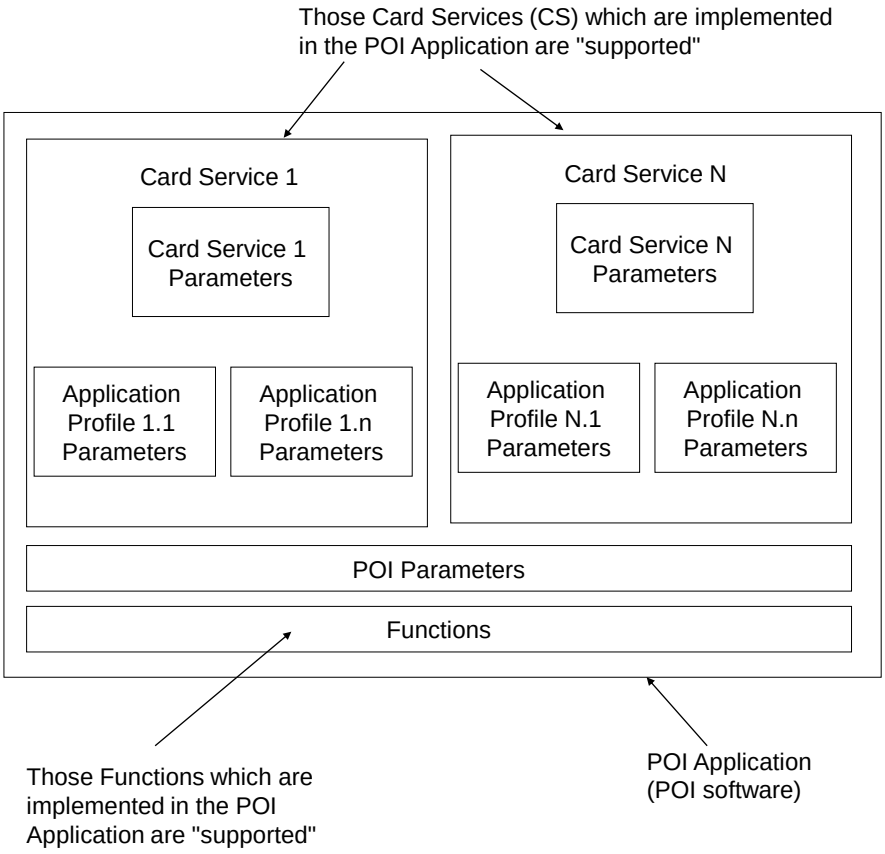

FIGURE 4: POI APPLICATION - LOGICAL STRUCTURE AND CONFIGURATION PARAMETERS

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

Req T2: The POI Application supporting the Chip with Contact Acceptance Technology shall be compliant with [EMV].

Req T3: For the Chip with Contact Acceptance Technology, the POI Application shall support Application Selection through PSE ("Payment System Environment").

Req T4: The POI Application supporting the Contactless Acceptance Technology shall support any contactless form factor.

Req T5: The POI Application supporting the Contactless Acceptance Technology shall be able to identify and react appropriately to whichever form factor is presented if the information is available from the form factor. If the form factor information is not

available, the POI Application shall assume that a Contactless Chip Card of the ID 1 form factor (as defined in ISO/IEC 7810) is used. When required by scheme rules the form factor information shall be included in authorisation and data capture.

Req T6: The POI Application supporting the Contactless Acceptance Technology shall support and comply with [EMV A], [EMV B] and [EMV D].

ReqT7: 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 displayable messages for cardholder display languages.

Req T9: All POIs, attended and unattended, shall have mechanisms to ensure that only the authorised user can initiate the Card Services Refund, Original Credit and Cancellation.

Req T10: 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, this event 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 presence of a Physical Card and, if the Contactless Acceptance Technology is supported, of a Mobile Device from POI Application to sale system.

Req T11: If the Chip with Contact Acceptance Technology has been tried and failed, and if subsequently, within the same transaction, Magnetic Stripe Acceptance Technology is tried, then the POI Application shall check the Application Profile configuration and, if applicable, whether the magnetic stripe data indicates that the Chip with Contact Acceptance Technology is supported, to determine, whether the magnetic stripe transaction is allowed and if it has to be considered as a fallback transaction (see Req T23).

4.2.1.3 e- and m-commerce (Virtual POI)

For e- and m-commerce, a Card Acceptor website is involved which typically includes the following components:

- The "shopping" pages;
- The checkout page, where the consumer selects the payment method (e.g., through a logo or brand name) and provides the necessary information for delivery of the goods or services.

It may also include

- A secure payment page where the Cardholder provides the relevant payment related data

Or

- A redirection to such a payment page hosted externally to the Acceptor's website on a payment gateway, typically provided by a third party.

Regardless of location, the payment page is part of the "Virtual POI". The payment related data is transferred from the payment page via the payment gateway to the Acquirer.

The Virtual POI may also facilitate redirection services to support "direct" remote authentication of the Cardholder by the Card Issuer via a so-called Authentication server.

Since the Virtual POI is implementation dependent, the Virtual POI Application may be implemented on one component or distributed on several components.

The payment page may be accessed by the Cardholder via a (mobile) browser or via a dedicated application on their consumer device.

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

Req T12: All Virtual POI Applications shall support at least one method of authenticating the cardholder. Supported method(s) may be static or dynamic, and may include a redirection to the Card Issuer domain as needed.

Req T13: The Virtual POI Application shall support at least the language(s) of the shopping page(s) for the dialog with the cardholder.

Req T14: Refund, Original Credit and Cancellation Services shall be initiated by the Card Acceptor. These Payment Services shall never be initiated by the Cardholder.

Req T15: Refund, Original Credit and Cancellation Services shall have mechanisms to ensure that only the authorised user can initiate these Services.

4.2.1.4 MOTO (Physical POI and Virtual Terminal)

For MOTO transactions, the Card Data provided by the Cardholder may be communicated to the Acceptor in writing or verbally. This Card Data enters the acquiring system via a POI Application on a Physical POI or a Virtual Terminal which will be referred to as MOTO Application in the rest of this book.

A Virtual Terminal facilitates the exchange of Card Data and information between the Acceptor and the Acquirer. It provides the Acceptor with a secure connection via a web-browser to a third party that hosts a Payment Page. The third party may be a processor, acquirer, or other third-party service provider who stores, processes, and/or transmits Card Data to authorise and settle an Acceptor's payment transactions.

- For Mail Order transactions the Card Data and address data (as needed) are provided by the Cardholder in writing (e.g., by mail or fax or a chat facility) and the Acceptor enters the data manually
    - Into a MOTO application on a Physical POI or
    - Via a web-browser into a MOTO application on a Virtual Terminal.
- For Telephone Order transactions, the Card Data and address data (as needed) are provided by the Cardholder
    - Verbally over a phone to the Acceptor who enters the data manually
        - Into a MOTO application on a Physical POI or
        - Via a web-browser into a MOTO application on a Virtual Terminal.
    - By Manual Entry using the phone keypad e.g., via Touch Tone facility using Dual-Tone-Multi-Frequency-encoded technology (DTMF), to automatically populate a MOTO application on a Virtual Terminal.

For MOTO the address and Card Data provided by the Cardholder may be used for validation. "Signature on File", when available, may also be used for dispute resolution.

Req T16: The Acceptor shall be able to confirm the transaction including the transaction amount to execute the transaction.

4.2.2 Configuration

Configuration is the act and result of setting the parameters for Card Services and Functions within a POI Application or MOTO Application.

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

4.2.2.1 *Local Transactions, e- and m-commerce and MOTO (Physical POI, Virtual POI and Virtual Terminal)*

Req T17: It shall be possible to configure the Card Services, the Application Profiles and the Functions. In particular it shall be possible to configure the POI Application to activate or deactivate specific Card Services and/or Functions.

Req T18: 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 Mobile Contactless.

Req T19: For Manual Entry, it shall be possible to configure the Physical POI or Virtual Terminal to prompt for the entry of the CSC. For No-Show transactions and transactions processed from Stored Card Data for Instalment or Recurring Payments it shall be possible to bypass entry of the CSC.

4.2.2.2 *Local Transactions and e- and m-commerce (Physical POI and Virtual POI)*

Req T20: It shall be possible to configure the supported CVMs per Application Profile.

4.2.2.3 *Local Transactions (Physical POI)*

Req T21: 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 T22: As a default configuration, the Chip with Contact Acceptance Technology shall have priority over the Magnetic Stripe Acceptance Technology. However, 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.

Req T23: It shall be configurable per Application Profile whether a magnetic stripe transaction shall be allowed and considered as a fallback transaction in the event the Chip with

Contact Acceptance Technology has been tried and failed and afterwards, within the same transaction, the Magnetic Stripe Acceptance Technology is tried.

In addition, it shall be configurable per Application Profile, if this configuration applies:

- Only if magnetic stripe data indicates that the Chip with Contact Acceptance Technology is supported by the Physical Card,
- Or irrespective of whether magnetic stripe data indicates or does not indicate that the Chip with Contact Acceptance Technology is supported by the Physical Card.

Req T24: It shall be configurable per Application Profile whether PIN Bypass is allowed.

Req T25: For attended POIs that support referrals it shall be configurable per Application Profile whether referrals are activated.

Req T26: It shall be configurable per transaction result (approved, declined or aborted) and per Card Service whether a cardholder receipt shall be printed or delivered electronically, either never, always or on request.[28]

4.2.2.4 MOTO (Physical POI and Virtual Terminal)

Req T27: It shall be configurable per transaction result (approved, declined or aborted) and per Card Service, whether a cardholder receipt shall be printed or delivered electronically either never, always or on request.

[28] 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.

4.2.3.1.1 Local Transactions (Physical POI)

Req T28: 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 T29: 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 T30: 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 T31: For all Acceptance Technologies with the exception of the Contactless Acceptance Technology, the transaction shall be initiated either by attendant action or by insertion/swiping of a Physical Card or by external activation by the sale system.

Req T32: For contactless transactions, the transaction shall be initiated either by attendant action or by external activation by the sale system prior to the activation of the contactless reader of the POI.

Req T33: 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.

4.2.3.1.2 e- and m-commerce (Virtual POI)

Req T34: If more than one Card Service is available for the transaction, the cardholder shall be able to select the Card Service from the list of Card Services that are available. If only one Card Service is available, this Card Service shall be selected by default.

4.2.3.1.3 MOTO (Physical POI and Virtual Terminal)

Req T35: All transactions shall be initiated by the Card Acceptor only.

Requirements T28, T29, T30 and T31 defined above for Physical POIs also apply for MOTO, albeit it is the Acceptor that is interfacing with the POI.

Req T36: The default Service on a Virtual Terminal shall be the Payment.

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.

4.2.3.2.1 Local Transactions (Physical POI)

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 the attendant or the cardholder the option to select one of the languages supported by the POI.

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

Req T37: 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 T38 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 T21) 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 T39: If all of the following are true:

- the POI based Language Selection for the cardholder display was not (successfully) performed prior to the start of the transaction,
- and the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology is used,
- and the card data element Language Preference is retrieved,

then 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 any of the following is true:

- neither the Chip with Contact Acceptance Technology nor the Contactless Acceptance Technology is used,
- or the card data element Language Preference is not retrieved,
- or the POI Application does not support any of the languages in the Language Preference,

then the POI Application shall continue to use the default language without performing any (additional) language selection.

Req T40: For attended POI, the messages for the attendant shall be displayed in a local language.

4.2.3.2.2 e- and m-commerce (Virtual POI)

Req T41: If the language selected on the merchant's website before the start of the transaction is supported by the POI, then it shall be the language used by the POI for the whole transaction.

Req T42: If the language selected on the merchant's website before the start of the transaction is not supported by the POI, then the POI shall offer its own language selection or it shall perform the whole transaction in English language.

4.2.3.2.3 MOTO (Physical POI and Virtual Terminal)

Language Selection is not performed for MOTO

4.2.3.3 Technology Selection

Technology Selection is a Function of Physical POIs performed only for Local Transactions which allows for the selection of one of the following Acceptance Technologies for transaction processing: Chip with Contact, Contactless, Magnetic Stripe, or Manual Entry.

Req T43: If a transaction is processed based on Stored Card Data, Technology Selection shall not be performed.

Req T44: Technology Selection shall be based on the configuration of the Card Service to be performed i.e., which Acceptance Technologies are activated for the Service and whether Chip with Contact has priority over Magnetic Stripe for this Service (see Reqs T18 and T22).

Req T45: If an Acceptance Technology is selected, all other Acceptance Technologies shall be deactivated until Technology Selection is re-started. However if the Contactless Acceptance Technology is selected, insertion of a card in the contact reader must be detected according to [EMV A].

Req T46: The POI shall display a message to use the Chip with Contact Acceptance Technology, if all of the following are true:

- The Magnetic Stripe Acceptance Technology is used,
- and the service code within Track 2 indicates that the Chip with Contact Acceptance Technology is supported by the Physical Card,
- and there has not been an attempt to use the Chip with Contact Acceptance Technology during the current transaction,
- and the Chip with Contact Acceptance Technology is activated for the Service (see Req T18),
- and the Chip with Contact Acceptance Technology is configured to have priority (see Req T22).

Req T47: If before any other Acceptance Technology is selected a Chip Card is inserted in the chip reader and the Acceptance Technology Chip with Contact is activated, then the POI Application shall recognise this and shall initiate reset processing according to [EMV B1].

Req T48: If a Physical Card is inserted in the chip reader and if the reset processing is unsuccessful and if the POI Application allows for additional re-reading of the chip, then a message shall be displayed to retry the Chip with Contact Acceptance Technology.

Req T49: If a Physical Card is inserted in the chip reader and if the Chip with Contact Acceptance Technology does not work and if the Magnetic Stripe Acceptance Technology is activated, then the POI Application shall initiate magnetic stripe processing identified as fallback according to Req T23.

4.2.3.4 Selection of the Application

4.2.3.4.1 IF Regulation Article 8.6 and Article 10.5 Requirements

The IF Regulation referred here is IFR 715/2015 ([IFR]).

4.2.3.4.1.1 Remits of IF Regulation Applicability

[IFR] only applies to EEA issued cards acquired in the EEA region. All cards issued outside the EEA area are out of scope, and not under the remit of [IFR].

IFR Req T1: The technical solution to implement [IFR] shall not impact international interoperability at the POI and global acceptance of cards:

- There shall be no impact on interregional (EEA/non EEA) transactions (both incoming and outgoing) to and from the EEA.
    - An EEA issued card shall have no detriment to acceptance when used outside of the EEA region.
    - A non-EEA issued card shall continue to be accepted when used inside the EEA region.
- The technical solution to implement [IFR] shall not impact non-EEA terminals or cards.
    - The requirements shall not force international cards to be re-issued.
    - The requirements shall not force terminals outside of the EEA to be upgraded.

4.2.3.4.1.2 IF Regulation Requirements

The following requirements are stated in [IFR], Article 8.6:

> *"Payment card schemes, issuers, acquirers, processing entities and other technical service providers shall not insert automatic mechanisms, software or devices on the payment instrument or at equipment applied at the point of sale which limit the choice of payment brand or payment application, or both, by the payer or the payee when using a co-badged payment instrument.*
>
> *Payees shall retain the option of installing automatic mechanisms in the equipment used at the point of sale which make a priority selection of a particular payment brand or payment application but payees shall not prevent the payer from overriding such an automatic priority selection made by the payee in its equipment for the categories of cards or related payment instruments accepted by the payee."*

The choice of the payment brand or payment application (including overriding) occurs when there are multiple mutually supported brands or payment applications in the Cardholder's payment instrument and in the POI of the Acceptor.

The following requirements are stated in [IFR], Article 10.5:

> *"Issuers shall ensure that their payment instruments are electronically identifiable and, in the case of newly issued card-based payment instruments, also visibly identifiable, enabling payees and payers to unequivocally identify which brands and categories of prepaid cards, debit cards, credit cards or commercial cards are chosen by the payer."*

To address Article 8.6 the following requirements shall be met:

IFR Req T2: The option to have a priority selection of a particular payment brand or payment application by the Acceptor shall only be allowed if the priority payment brand or payment application is displayed to the Cardholder and the Cardholder is clearly given the possibility to override the Acceptor's priority selection.

Note:

- There are various contexts where it is not technically feasible to allow the Cardholder to override a priority selection (e.g., Environment with no screen and /or no Pin/touch/key Pad ...).
- The priority payment brand or payment application shall be displayed on the POI or at the POS, e.g. together with the accepted payment brands.
- Acceptor’s priority selection can be achieved through various mechanisms. Examples and implementation guidance are provided in Book 6.

- Override of the Acceptor's priority selection by the Cardholder can be achieved through various mechanisms. It may include early Cardholder preference mechanisms. Examples and implementation guidance are provided in Book 6.

IFR Req T3: If the Acceptor has chosen to implement priority selection, then the Cardholder shall be informed of their ability to override the Acceptor's priority selection and how to override it so that the Cardholder can select their preferred application.

Note:

Information of the ability to override the Acceptor's priority selection and how to override it shall be displayed on the POI or at the POS.

IFR Req T4: The method of cancelling a transaction and the method of overriding an Acceptor's priority selection shall be clearly distinguishable from each other for the Cardholder.

In addition to the red/Cancel button, a clear override choice shall be available to the cardholder through the use of the yellow/Correction button or a specific "Change Choice" button or some other means on the POI.

IFR Req T5: If a Cardholder has chosen a specific combination of Product Type and Payment Brand, the Acceptor shall not change the combination chosen by the Cardholder for that transaction.

To address Article 10.5 the following requirement shall be met:

IFR Req T6: In order to support Electronic Product Identification:

- For Local transactions, a Card resident data element, [EMV] tag '9F0A' with ID = '0001', shall be used as the target solution. If this data element is not available, solutions based on BIN tables may be used.

- For Remote transactions as currently defined in the Volume, solutions based on BIN tables shall be used.

Note:

Solutions based on BIN tables can be achieved through various mechanisms.

4.2.3.4.2 Local Transactions (Physical POI)

Selection of the Application is the Function which allows the selection of an:

- Application supported by the Chip Card or Mobile Device and the POI, either manually (by the Cardholder) or automatically (without Cardholder interaction) to be used to process a

Card Service, for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology,

- Application Profile for all Acceptance Technologies.

Req T50: For Selection of the Application for the Chip with Contact Acceptance Technology, in addition to Application Selection requirements of [EMV B1], the following rules shall apply only for EEA issued cards, in line with the IFR Requirements in Section 4.2.3.4.1.2:

1. The POI shall always construct the list of mutually supported applications between the Chip Card and the POI.

   If the POI successfully reads [EMV] tag '9F0A' with ID = '0001' for any application, then the POI may use the value assigned to ID '0001' (as described in Section 3.2) to determine whether to exclude the application from the list of mutually supported applications.

2. If the list contains only one entry, then proceed according to [EMV B1] with the following modification: If the cardholder has expressed the wish to make a choice, then this single application shall be shown for confirmation.

   If the list contains more than one entry, the POI shall proceed according to Paragraph 3 or 4 or 5.

   Paragraph 5 shall only apply where it is not technically feasible to allow the Cardholder to override a choice of application (e.g., Environment with no screen and /or no Pin/touch/key Pad ...).

3. The POI shall present without discrimination all mutually supported applications to enable Cardholder choice. The POI display ergonomics shall be designed such that the Cardholder is able to choose from the mutually supported applications in a convenient way.

   - The Acceptor may put their prioritised application on top.

   - Once the Cardholder decides which application to be used for that specific transaction, the Acceptor shall not override that decision.

4. The Cardholder will only be presented with the Acceptor's prioritised application (automatic mechanism according to [IFR], Article 8.6).

If the Acceptor has chosen to implement priority selection, the Cardholder shall be offered an override mechanism. This mechanism shall be made available prior to EMVCo's Card Action Analysis being performed. In particular, this may be an early cardholder preference mechanism.

If the Cardholder overrides the Acceptor's priority selection, then Paragraph 3 shall apply.

5. The POI shall select the first mutually supported application. The Acceptor may put their prioritised application on top.

Req T51: For Selection of the Application for the Contactless Acceptance Technology, Combination Selection shall follow [EMV B].

For EEA issued cards the following modifications are allowed for building the list of mutually supported combinations described in [EMV B]:

- If the POI successfully reads [EMV] tag '9F0A' with ID = '0001' for any combination, then the POI may use the value assigned to ID '0001' (as described in Section 3.2) to determine whether to exclude the combination from the list of mutually supported combinations.

- The Acceptor may put their prioritised application on top.

For EEA issued cards the following modification applies for [EMV B] Final Combination Selection: If the list of mutually supported combinations contains only one application and the cardholder has expressed the wish to make a choice, then this single application shall be shown for confirmation.

For EEA issued cards, if the list of mutually supported combinations contains more than one application (different DF Names), then the following modifications apply for Final Combination Selection described in [EMV B]:

- The Cardholder shall have the means to select the application of their choice. If the Cardholder makes a choice, then the chosen application shall be used in Final Combination Selection.

- If the Cardholder does not wish to make a choice, then Final Combination Selection shall follow [EMV B] using the list of mutually supported combinations built as described above with the allowed modifications for EEA issued cards.

- If it is not technically feasible to allow the Cardholder to select the application of their choice (e.g., Environment with no screen and /or no Pin/touch/key Pad ...), then Final Combination Selection shall follow [EMV B] using the list of mutually supported combinations built as described above with the allowed modifications for EEA issued cards.

Req T52: The Application Profile shall be selected for a transaction based on the Card Service and primarily on the following:

- The selected AID for the Chip with Contact Acceptance Technology,
- The selected Combination for the Contactless Acceptance Technology,
- The PAN for the Magnetic Stripe, Manual Entry and Stored Card Data Acceptance Technologies.

In addition, for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology, the Application Profile may be selected based on the presence/absence of [EMV] tag '9F0A' with ID = '0001' and on the value assigned to ID '0001'.

4.2.3.4.3 e- and m-commerce (Virtual POI)

Selection of the Application is the Function which allows the selection

- Of an application supported by the Cardholder Environment or Stored Card Data and the POI, either manually (by the cardholder) or automatically (without cardholder interaction) to be used to process a Card Service,
- Of an Application Profile by the POI, which is transparent for the Cardholder and the Acceptor.

Req T53: The Payment Brands and Product Types accepted by the Acceptor for the transaction shall be displayed so the Cardholder can choose the application to be used to perform the transaction. The Acceptor may determine the method and the order in which the Payment Brands and Product Types are displayed to the Cardholder. If not all Payment Brands and Product Types are displayed at once for selection, the Acceptor shall inform the Cardholder how to select the other supported Payment Brands and Product Types.

Req T54: The Application Profile shall be selected for a transaction based on the Card Service and on the Payment Brand. In addition, the Application Profile may be selected based on the Product Type.

4.2.3.4.4 MOTO (Physical POI and Virtual Terminal)

Selection of the Application is the Function which allows the POI to select an Application Profile, which is transparent for the Cardholder and the Acceptor.

Req T55: The Application Profile shall be selected for a transaction based on the Card Service and on the Payment Brand. In addition, the Application Profile may be selected based on the Product Type.

4.2.3.5 Card Data Retrieval

Card Data Retrieval is the Function which allows Card Data to be retrieved according to the Acceptance Technology.

4.2.3.5.1 Local Transactions, e- and m-commerce and MOTO (Physical POI, Virtual POI and Virtual Terminal)

Req T56: All authorisation and completion messages shall identify the Acceptance Technology used to retrieve Card Data.

4.2.3.5.2 Local Transactions (Physical POI)

Req T57: For Local transactions at a Physical POI, the Acceptance Technology shall be Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe, and Manual Entry by Acceptor or Stored Card Data.

Req T58: When Manual Entry by Acceptor is supported, the Physical POI Application shall facilitate entering the PAN, the expiration date and, when appropriate, the Card Security Code.

4.2.3.5.3 e- and m-commerce (Virtual POI)

Req T59: For e- and m-commerce transactions, the Acceptance Technology shall be Manual Entry by Cardholder, Payment Credentials on Consumer Device, Payment Credentials on Consumer Device with Authentication Application, (M)RP Application on Consumer Device or Stored Card Data.

Therefore the POI shall display a payment page to the Cardholder. This page shall facilitate either the entry of the PAN, the Expiration date, and the Card Security Code or the retrieval of Stored Card Data, or it shall support automatic reading of the Card Data from the (M)RP application, Authentication Application or the Payment Credentials accessed via a Consumer Device.

4.2.3.5.4 MOTO (Physical POI and Virtual Terminal)

Req T60: For MOTO transactions, the Acceptance Technology shall be Manual Entry by Attendant or Stored Card Data. The interface with the cardholder is just to facilitate the entry of the Card Data via a Telephone keypad when Touch-Tone using DTMF

technology is supported. Therefore the Physical POI and Virtual Terminal shall facilitate the entry of the PAN, the Expiration date, and the Card Security Code by the Acceptor and where DTMF is enabled; the Virtual Terminal shall support the entry of the Card Data by the cardholder via a telephone keypad.

Req T61: The MOTO Application shall also support the entry and transmission of Address Data if address validation is supported.

4.2.3.6 Card Authentication

4.2.3.6.1 Local Transactions (Physical POI)

Card Authentication for Local Transactions is the Function defined by EMV by which a Card Application is authenticated to the POI (Offline Data Authentication) and/or the Issuer (Online Authentication). Card Authentication applies only to the Chip with Contact Acceptance Technology and to the Contactless Acceptance Technology.

Req T62: Online-only POI Applications are not required to support Offline Data Authentication.

Req T63: The POI Application supporting the Chip with Contact Acceptance Technology and Offline Data Authentication shall support the Offline Data Authentication methods as defined in [EMV] as follows:

- SDA is optional.
- DDA is mandatory.
- CDA is mandatory for newly installed POI.

For the POI Application supporting the Contactless Acceptance Technology, the Offline Data Authentication methods shall be supported as defined in the respective kernel specifications.

4.2.3.6.2 e- and m-commerce (Virtual POI)

Card Authentication is the Function by which Card Data or a Card Application is authenticated to the Issuer. However, some of the methods described below also facilitate cardholder authentication (e.g., OTP).

In addition, Passive Authentication may be used by the issuer as an additional method for risk management, as described in Book 4 section 2.3.2.4.

For e- and m-commerce transactions card authentication may be performed using static or dynamic authentication. This may involve a redirection from the Virtual POI to an authentication server in the Issuer domain.

Req T64: For recurring and instalment type transactions, static authentication shall only be performed on the initial transaction, since storage of the Card Security Code is prohibited.

4.2.3.6.3 MOTO (Physical POI and Virtual Terminal)

Req T65: All MOTO Applications shall support static authentication.

Req T66: For MOTO transactions, the card authentication is performed using static authentication whereby the Card Issuer verifies the Card Security Code.

- For recurring and instalment type transactions, Static Authentication can only be performed on the initial transaction because storage of the Card Security Code (CSC) is prohibited. Stored Card Data derived initially from manual entry as a result of a MOTO transaction, shall be processed as per the requirements described for Recurring or Instalment Payments (see Sections 4.3.7 and 4.3.8).

- For No-Show transactions, Static Authentication is not performed because the CSC cannot be stored, consequently is not available, when the No-Show is processed.

4.2.3.7 Cardholder Verification

Cardholder Verification is the Function used to verify whether the person using the Cardholder Environment is the legitimate cardholder.

4.2.3.7.1 Local Transactions (Physical POI)

On the Physical POI, Cardholder Verification is the Function by which a Cardholder Verification Method (CVM) is selected and performed. If Cardholder is not present, Cardholder Verification is not applicable.

The CVMs to be used are defined in the EMV specifications. The Acceptance Technologies with which they may be used are shown below:

- Offline Enciphered PIN, if the Acceptance Technology is Chip with Contact, Chip Contactless or Mobile Contactless,

  Note that the usage of Offline Enciphered PIN for the Contactless Acceptance Technology is currently not described in [EMV].

- Offline Plaintext PIN, if the Acceptance Technology is Chip with Contact,

- Online PIN, if the Acceptance Technology is Chip with Contact, Chip Contactless, Mobile Contactless or Magnetic Stripe,

- Offline Mobile Code, if the Acceptance Technology is Mobile Contactless,

- Signature for all Acceptance Technologies with the exception of the Contactless Acceptance Technology with form factors that do not allow signature comparison, e.g., Mobile phones,

- No CVM Required for all Acceptance Technologies.

4.2.3.7.1.1 General Requirements for Cardholder Verification

Req T67: All Physical 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 T68: For POIs that have a PIN Entry Device, the POI Application shall be able to support PIN as CVM.

Req T69: The POI Application shall offer PIN Bypass to the Cardholder if PIN entry is requested and PIN Bypass is allowed according to the Application Profile (see Req T24).

4.2.3.7.1.2 Cardholder Verification for the Chip with Contact Acceptance Technology

Req T70: POIs with a PIN Entry Device shall meet the following requirements:

- For POIs which are not ATMs:
  - 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.
  - Other CVMs as defined by [EMV], including Signature and No CVM Required, may be supported in addition to PIN.
  - Unattended POIs shall not support Signature CVM and Combined CVM containing Signature.
- For ATMs:
  - The POI Application shall support Online PIN.
  - The POI Application may in addition support Offline PIN.
  - ATMs shall not support No CVM Required, Signature CVM or Combined CVM containing Signature.

4.2.3.7.1.3 Cardholder Verification for the Contactless Acceptance Technology

Req T71: POIs supporting the Contactless Acceptance Technology shall support

- Online PIN
- Signature
- No CVM Required
- Offline Mobile Code

according to the requirements of the contactless kernels implemented in that POI.

4.2.3.7.1.4 Cardholder Verification for the Magnetic Stripe Acceptance Technology

Req T72: POIs with a PIN Entry Device shall meet the following requirements:

- 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.
- ATMs shall not support No CVM Required.

4.2.3.7.1.5 Cardholder Verification for the Manual Entry Acceptance Technology

Req T73: POIs with a PIN Entry Device shall meet the following requirements:

- Neither Online PIN nor Offline PIN shall be supported.
- Either No CVM Required, or Signature, or both CVMs shall be supported.

4.2.3.7.2 e- and m-commerce (Virtual POI)

On A Virtual POI, Cardholder Verification may be performed with one of the following Cardholder Verification Methods (CVM):

- Personal Code (offline or online),
- Mobile Code (offline or online) and
- No CVM Required.

The Virtual POI is only involved if online CVMs are used, in which case the Personal Code or Mobile Code is transferred via the card network or the internet.

Note that other CVMs may be used which do not involve the Virtual POI (e.g., a PIN entry via an additional authentication device may be used, see Book 4).To perform an online cardholder verification during an e- or m-commerce transaction, the cardholder may be redirected to the issuer, as the first step of the Authorisation process. The Issuer can then verify the cardholder using the previously registered personal or mobile code. The result of this verification is then passed by the Issuer to the Acceptor. This process is known as 3 Domain Security.

Req T74: The POI shall support at least one Cardholder Verification Method.

4.2.3.7.3 MOTO (Physical POI and Virtual Terminal)

For MOTO Cardholder Verification is not applicable. However, the address and Card Data provided by the Cardholder may be used for validation. "Signature on File", when available, may also be used for validation.

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 Acquirer according to Book 3 or processed offline by the Card Application.

4.2.3.8.1 Local Transactions (Physical POI)

Req T75: 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 T76: If the Authorisation Response Code indicates that the Online PIN entered did not verify correctly ("Wrong PIN"), for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology, the transaction shall be declined and Online PIN re-entry shall not be allowed within this same transaction.

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 Chip Card, without repeating Language Selection and Selection of the Application, but with repeating the complete EMV card process including Online PIN entry).

Req T77: For attended POIs, for all Card Services with exception of the Payment Service (see Req T117) and the Deferred Payment Service (see Req T186), the attendant shall not be allowed to force a declined transaction to be accepted.

Req T78: The DF Name [EMV] tag '84' and, if successfully read by the POI, the value for ID = '0001' of Application Selection Registered Proprietary Data [EMV] tag '9F0A' of the selected application shall be included in the authorisation messages.

4.2.3.8.2 e- and m-commerce (Virtual POI)

Req T79: For e- or m-commerce transaction if a dedicated (Mobile) Remote Application is not used, the POI shall perform an online authorisation exchange to the issuer. If a dedicated (Mobile) Remote Application is used, the transaction shall be authorised either offline by this Application or online.

Req T80: The Payment Brand and Product Type of the selected application shall be included in the authorisation messages.

4.2.3.8.3 MOTO (Physical POI or Virtual POI)

Req T81: MOTO transactions shall be sent online for authorisation.

Req T82: If it is not possible to perform an online authorisation, either Voice Authorisation shall be performed or the transaction shall be declined.

Req T83: The authorisation message shall identify that the transaction is MOTO.

Req T84: If available, the Payment Brand and Product Type shall be included in the authorisation messages.

4.2.3.9 Referral

Referral is the Function where a Card Service is completed with a verbal dialogue between the Acceptor and the Acquirer to obtain an approval code when the Authorisation response contains a referral response code. This Function is only performed for Local Transactions. It does not necessarily involve the Cardholder or the Cardholder Environment.

Req T85: Only attended POIs shall support referrals. If an unattended POI receives a request for referral it shall decline the transaction.

Req T86: 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 T87: If a Chip with Contact transaction is being processed and a request for referral is received then chip processing shall be terminated by requesting a decline from the Card Application and a message shall be displayed requesting the removal of the Chip Card.

Req T88: If a request for referral is received and the attended POI supports referrals, the following process shall be followed:

- The contact number for voice authorisation shall be made available.
- If an approval code is received orally during voice authorisation it shall be manually entered in the POI.
    - If an approval code is entered, the transaction shall be approved.
    - If an approval code is not entered, the transaction remains declined.
    - The approval code shall be stored with the transaction data for data capture.

Req T89: The POI shall have mechanisms to ensure that only the authorised user can initiate the Referral Function.

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 Application
- Inform Cardholder, Attendant and/or Acquirer about the result of the transaction
- Deliver a receipt to Cardholder and/or Attendant

4.2.3.10.1 Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal)

Req T90: If the transaction (approved, declined or aborted) is not immediately online-captured, the transaction data shall be securely stored for data capture.

4.2.3.10.2 Local Transactions (Physical POI)

Req T91: 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 of the POI and, if offered by the Acceptor, in the Cardholder selected language. The transaction receipt may be combined with the sales receipt, if any.

The following are the minimum data that shall be printed on receipts.[29] 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)
- Transaction Reference, e.g., a sequence number or a sale reference number
- Transaction Amount[30] and Transaction Currency[31]
- Truncated PAN

[29] Provided these requirements are in line with the local laws and regulations

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

[31] For transactions with Dynamic Currency Conversion see Req. T311.

- DF Name (as returned by the Card Application) for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology
- Payment Brand name, e.g., Application Preferred Name or Application Label for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology, or as retrieved from the Application Profile for the Magnetic Stripe, Manual Entry or Stored Card Data Acceptance Technologies.
- Acceptor name and location
- The Card Service, e.g., "Payment"
- Transaction Result, e.g., "Approved"

4.2.3.10.3 e- and m-commerce (Virtual POI)

Req T92: The POI shall provide a transaction receipt to the Cardholder after a successful authorisation process. The transaction receipt may be combined with the sales receipt.

The following are the minimum data that shall be provided. The sequence of the data elements provided is not mandatory. Additional data may be provided but is out of scope of this document.

- Transaction Date and Transaction Time
- Transaction Amount and Transaction Currency
- Truncated PAN
- Payment Brand name
- Acceptor name and location
- Transaction Reference number
- The Card Service, e.g., 'Payment'
- Transaction Result, e.g., 'Approved'

Req T93: The transaction receipt shall be made available as confirmation to the Cardholder according to Cardholder's preference and communication channels available.

Req T94: In case of partial delivery the final amount shall be reduced and a new receipt shall be sent to the Cardholder.

Req T95: The POI shall receive from the Acceptor the final amount which may be lower than the authorised amount (in case of non-availability of goods or services). The clearing data shall always include the final amount.

4.2.3.10.4 MOTO (Physical POI or Virtual POI)

Req T96: For Telephone Order transactions, at least a transaction reference shall be provided to the Cardholder during the call.

Req T97: For MOTO transactions a transaction receipt shall be provided to the Cardholder with the delivery. The minimum data on the receipt is the same as listed in Req T92.

Req T98: In case of partial delivery, the final amount shall be reduced accordingly and a receipt reflecting the reduced amount shall be provided to the Cardholder.

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 Cardholder nor the Cardholder Environment. Reversal can be performed offline by removing the transaction data or by storing cancellation data for capture or online.

The following requirement applies to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T99: Reversal shall be performed online if Authorisation is performed online and if any of the following is true:

- A correct response is not received or no response (timeout) is received
- Or the transaction is declined/aborted after an online (full or partial) approval.

4.2.3.12 Data Capture

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

A requirement requesting specific data in Data Capture requires the POI to provide the respective data in the Data Capture Function, which is the first step in the clearing chain. However, this does

not mean that all data provided by the POI in the Data Capture function shall be used for clearing (or Financial Presentment).

If not specified elsewhere in the Volume, it is a Scheme/Acquirer decision, which of the data provided by the POI has to be provided by the Acquirer for clearing (or Financial Presentment).

4.2.3.12.1 Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal)

Req T100: One or more of the following methods 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.

4.2.3.12.2 Local Transactions (Physical POI)

Req T101: The DF Name [EMV] tag '84' and, if successfully read by the POI, the value for ID = '0001' of Application Selection Registered Proprietary Data [EMV] tag '9F0A' of the selected application shall be included in Data Capture.

4.2.3.12.3 e- and m-commerce (Virtual POI)

Req T102: The Payment Brand and Product Type shall be included in Data Capture.

4.2.3.12.4 MOTO (Physical POI and Virtual Terminal)

Req T103: The completion message shall identify that the transaction is MOTO.

Req T104: If available, the Payment Brand and Product Type shall be included in Data Capture.

4.3 Payment Services

4.3.1 Payment

Table 5 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Payment Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	✓	✓[32]
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	✓	×

TABLE 5: PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in Table 6 shows which Functions are not applicable (N/A) or which are, mandatory (M), optional (O) or conditional (C) for the Payment Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

[32] On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	M	M
Cardholder Verification	M	M	N/A
Authorisation	M	M	M
Referral	O	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	M	M	M

TABLE 6: FUNCTIONS USED FOR PAYMENT

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Payment Service for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.1.1 POI Application

4.3.1.1.1 Local Transactions, e- and m-commerce (Physical POI and Virtual POI) and MOTO (Physical POI or Virtual Terminal)

Req T105: The transaction amount shall be checked against a minimum allowed amount and/or a maximum allowed amount, if configured for the Application Profile. If the check fails, the transaction shall not proceed.

4.3.1.1.2 Local Transactions (Physical POI)

Req T106: For Payment, the cardholder shall be able to confirm the transaction amount and the selected Payment Brand when performing the CVM.

The only exceptions are where the CVM is No CVM Required or where the Cardholder Verification is performed on the Mobile Device before the transaction amount is known. In those cases, the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

Req T107: For unattended POIs, if the transaction amount is defined before the delivery of the goods or services, the amount used to process the transaction shall be the actual amount.

Req T108: If the POI supports partial approvals of online authorisations, then it shall support it for all Acceptance Technologies supported.

4.3.1.1.3 e- and m-commerce (Virtual POI)

Req T109: For e- and m-commerce transactions the Virtual POI shall inform the Cardholder about the transaction including the transaction amount prior to Card Data Retrieval.

4.3.1.1.4 MOTO (Physical POI and Virtual Terminal)

Req T110: For MOTO transactions it is the Card Acceptor that shall confirm the transaction, including the transaction amount.

4.3.1.2 Configuration

4.3.1.2.1 Local Transactions, and e- and m-commerce (Physical POI and Virtual POI) and MOTO (Physical POI or Virtual Terminal)

Req T111: 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.

4.3.1.2.2 Local Transactions (Physical POI)

Req T112: It shall be configured that the Chip with Contact Acceptance Technology and/or the Contactless Acceptance Technology shall be supported (see Req T18) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T22).

Req T113: 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 T114: For the specific Unable-to-go-online processing described in Req T124, 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 T115: For attended POIs that support partial approvals of online authorisations it shall be configurable per Application Profile whether partial approvals are activated.

Req T116: 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 T117: 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 T118: For unattended POIs, forcing a declined transaction to be accepted shall not be supported.

However, 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, it shall be possible to configure the POI Application to allow/not allow the transaction approval to be automatically forced.

4.3.1.2.3 MOTO (Physical POI and Virtual Terminal)

Req T119: For attended POIs (Physical POI or Virtual Terminal) that support partial approvals of online authorisations, it shall be configurable per Application Profile whether partial approvals are activated.

4.3.1.3 Transaction Initialisation

The following requirement applies to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T120: For Payment, the transaction amount (i.e. the amount to be authorised, which includes any additional amount) shall be available to the POI Application at Transaction Initialisation.

4.3.1.4 Authorisation

4.3.1.4.1 Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal)

Req T121: When a (Mobile) EMV Payment Application or (M)RP Application is not involved and if an online authorisation is required and it is not possible to perform the authorisation, the transaction shall be declined.

Req T122: For Authorisation, the transaction amount as defined in Req T120 shall be used.

Req T123: 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.

4.3.1.4.2 Local Transactions (Physical POI)

Req T124: For Chip with 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 Application approves the transaction, and the amount exceeds the POI floor limit, the POI Application shall be configurable per Application Profile whether to approve the transaction (or for attended POIs perform a voice authorisation according to scheme rules) or decline.

4.3.1.4.3 MOTO (Physical POI and Virtual Terminal)

Req T125: For MOTO, as online authorisation is required if it is not possible to perform an online or voice authorisation, the transaction shall be declined.

4.3.1.5 Completion

4.3.1.5.1 Local Transactions and e- and m-commerce (Physical POI and Virtual POI)

Req T126: Any POI which is integrated with the sale system shall send a message to the sale system to indicate the transaction result. In addition, it shall receive the final transaction amount if different from the authorised amount, from the sale system.

4.3.1.5.2 Local Transactions (Physical POI)

Req T127: The POI shall have mechanisms to ensure that only the authorised user can force a declined transaction to be accepted.

Req T128: To prevent the cardholder from leaving the Physical Card in the unattended POI, card removal shall always be prompted prior to goods or service delivery.

4.3.1.6 Reversal

These Requirements apply to Local Transactions, e- and m-commerce (Physical POI and Virtual POI) and MOTO:

Req T129: If the actual amount was authorised but goods or service could not 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 T130: 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 and capture is not performed immediately, the POI shall then perform a partial reversal. The captured data shall always include the final, reduced amount.

4.3.2 Refund

Table 7 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Refund Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	×	×	×
Magnetic Stripe	✓	×	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	×	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	✓	✓

TABLE 7: REFUND: 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 Refund Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	N/A	N/A	N/A
Cardholder Verification	N/A	N/A	N/A
Authorisation	O	O	O
Referral	N/A	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	M	M	M

TABLE 8: FUNCTIONS USED FOR REFUND

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Refund Service for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.2.1 POI Application

4.3.2.1.1 Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal)

Req T131: The Refund Service shall always be initiated by the Acceptor, never by the Cardholder.

Req T132: The transaction amount shall be checked against a maximum allowed amount if configured for the Application Profile. If the check fails, the transaction shall not proceed.

4.3.2.1.2 Local Transactions (Physical POI)

Req T133: If the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology is used, it is only for the purpose of retrieving the Card Data for the Refund transaction, not to perform a Card transaction. Therefore, EMV processing shall be followed until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the Expiry Date. If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the Card Application.

4.3.2.2 Configuration

The following requirements apply to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T134: In addition to Req T9, it shall be configurable for the Refund Service to further protect high value amounts using additional security e.g., a supervisor's password. The amount above which this additional security is required shall be configurable.

Req T135: It shall be configurable per Application Profile, whether the Refund is performed online or not.

4.3.2.3 Transaction Initialisation

The following requirement applies to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T136: 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

The following requirement applies to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T137: For Local Transactions, MOTO and e- and m-commerce, if required by the Application Profile, the Refund shall be processed online.

4.3.3 Cancellation

Table 9 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not

applicable (×) for the Cancellation Service. On the unattended Physical POI, the Cancellation Service is only initiated by the Acceptor based on original transaction data.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	×	×	×
Magnetic Stripe	✓	×	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	×	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	✓	✓

TABLE 9: CANCELLATION: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in Table 10 shows which Functions are not applicable (N/A) or which are, mandatory (M), optional (O) or conditional (C) for the Cancellation Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	N/A	N/A	N/A
Cardholder Verification	N/A	N/A	N/A
Authorisation	C	C[33]	M
Referral	N/A	N/A	N/A
Completion	M	M	M
(Partial) Reversal	O	C	C
Data Capture	C	C	C

TABLE 10: FUNCTIONS USED FOR CANCELLATION

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Cancellation Service for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.3.1 POI Application

4.3.3.1.1 Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal)

Req T138: The Cancellation Service shall always be initiated by the Acceptor, never by the Cardholder.

[33] When there is an (M)RP Application on the consumer device involved, online Authorisation is not mandatory.

Req T139: A Cancellation shall always be performed for the full amount of the original transaction.

Req T140: When performed for the Pre-Authorisation Services, the Cancellation Service shall cancel a Pre-Authorisation and all linked Update Pre-Authorisation(s).

Req T141: The Cancellation Service shall be supported to cancel a Payment Completion.

4.3.3.1.2 Local Transactions (Physical POI)

Req T142: If the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology is used, it is only for the purpose of retrieving the Card Data for the Cancellation transaction, not to perform a Card transaction. Therefore, EMV processing shall be followed until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the Expiry Date. If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the Card Application.

4.3.3.2 Configuration

The following requirements apply to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T143: It shall be configurable per Application Profile which of the Card Services can be cancelled.

Req T144: It shall be possible to configure for the POI whether Cancellations shall be restricted to the last transaction processed at the POI or may be extended to previous transactions.

Req T145: It shall be possible to configure per Application Profile, whether Cancellations shall be declined or processed online if the original transaction has already been captured to the Acquirer.

Req T146: It shall be possible to configure per Application Profile, whether Cancellations shall be declined or sent online, if the original transaction cannot be retrieved in the POI.

Req T147: 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

The following requirements apply to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T148: If the original transaction cannot be recognised by the POI or has been already captured to the Acquirer, the Cancellation shall either be aborted or be processed online according to the configuration of the Cancellation Service.

Req T149: 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

The following requirements apply to Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI and Virtual Terminal):

Req T150: Data Capture shall be performed according to the conditions described in T149.

Req T151: 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 are:

- Pre-Authorisation Service (see Section 4.3.4.1.1),
- Update Pre-Authorisation Service (see Section 4.3.4.1.2) and
- Payment Completion Service (see Section 4.3.4.2).

Update Pre-Authorisation may either:

- Increase the previously authorised amount(s) to reserve funds or,
- Decrease the previously authorised amount(s) to release funds.

Decreasing the previously authorised amount(s) may be achieved by a reversal or an authorisation adjustment.

As soon as the final amount is known, then Payment Completion is used to finalise the transaction using the final amount.

In the event that the amount(s) pre-authorised is not used, the previously authorised amount(s) are released by the Cancellation Service. In this case Payment Completion does not follow. Note that in an unattended environment the Cancellation Service would be initiated automatically by the POI application.

The Pre-Authorisation Services may either be performed as a "Card Present" or "Card Not Present" transaction.

It is recommended that at least one of the Pre-Authorisation Service(s) prior to Payment Completion is performed based on one of the following Acceptance Technologies:

- Chip with Contact,
- Contactless,
- Consumer Device with Payment Credentials and Authentication Application,
- Consumer Device with (M)RP Application.

Table 11 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (✗) for the Pre-Authorisation Services.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe	✓	✓	✗	✗
Manual Entry (by Acceptor)	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Cardholder)	✗	✗	✓	✗
Consumer Device with Payment Credentials	✗	✗	✓	✗
Consumer Device with Payment Credentials and Authentication Application	✗	✗	✓	✗
Consumer Device with (M)RP Application	✗	✗	✓	✗
Stored Card Data	✓	✗	✓	✓

TABLE 11: 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 12: shows which Functions are not applicable (N/A) or which are, mandatory (M), optional (O) or conditional (C) for the Pre-Authorisation and Update Preauthorisation Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and

Virtual Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	C	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	C	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	C	C
Cardholder Verification	C	C	N/A
Authorisation	M	M	M
Referral	O	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	N/A	N/A	N/A

TABLE 12: FUNCTIONS USED FOR PRE-AUTHORISATION AND UPDATE PREAUTHORISATION

4.3.4.1.1 Pre-Authorisation Service

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Pre-Authorisation Service for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.4.1.1.1 POI Application

Req T152: For Local Transactions, if the Cardholder is participating, the Cardholder shall be able to confirm the transaction amount and the Payment Brand when performing the CVM.

The only exception is when the CVM is No CVM Required, where the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

Req T153: 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 (no single unit currency), or be based on known or estimated expenditure.

Req T154: If the cardholder is participating, the cardholder display shall clearly indicate that the amount to be confirmed is an estimated amount and is a Pre-Authorisation.

Req T155: A Pre-Authorisation shall be identified as such in authorisation messages and transaction data.

Req T156: Data from approved Pre-Authorisations (e.g., PAN and Expiry Date, amount, authorisation code and unique reference) shall be stored for performing subsequent steps (i.e. Update Pre-Authorisation, Payment Completion).

Req T157: If a Card Application is used, the appropriate Card Application data elements from both the Pre-Authorisation request and response must be retained for the Payment Completion Service, including the EMV Application Cryptogram(s) (ARQC and, if generated, TC), because all fields needed to validate the cryptogram must be included in the Payment Completion record.

4.3.4.1.1.2 Configuration

Req T158: The POI Application shall be configurable to allow the Pre-Authorisation amount to be received or to be a configurable default amount.

4.3.4.1.1.3 Authorisation

Req T159: A Pre-Authorisation shall be authorised online in order to reserve the funds.

Req T160: For Pre-Authorisation, the authorisation response message shall contain the Transaction Lifecycle Identifier (as defined in Book 3) or corresponding element, which is the unique reference to be used to link any subsequent Update Pre-Authorisation(s) and the Payment Completion to the Pre-Authorisation.

4.3.4.1.1.4 Data Capture

Req T161: Approved Pre-Authorisations shall not be captured.

4.3.4.1.2 Update Pre-Authorisation Service

In addition to the general requirements listed in section 4.2, the following specific requirements apply to the Update Pre-Authorisation Service for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.4.1.2.1 POI Application

Acceptance Technology for Update Pre-Authorisation may be different from the Pre-Authorisation (or previous Update Pre-Authorisation) Acceptance Technology mainly because the card or cardholder are normally not present when Up-date Pre-Authorisations are being performed.

Note:

If the Update Pre-Authorisation is performed based on Stored Card Data obtained in the Pre-Authorisation, then the Card Data for an Update Pre-Authorisation will not contain the CSC, because it is not allowed to store the CSC after authorisation.

Req T162: For Local Transactions, if the cardholder is participating, the display shall clearly indicate that the amount to be confirmed is an increment or decrement amount. In addition the cardholder shall be able to confirm the transaction amount and the Payment Brand when performing the CVM.

The only exception is when the CVM is No CVM Required, where the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

Req T163: An Update Pre-Authorisation shall be identified as such in authorisation messages and transaction data and shall contain the unique reference from the original linked Pre-Authorisation.

Req T164: An approved Update Pre-Authorisation shall increment or decrement the amount of the previously linked Pre-Authorisation and Update Pre-Authorisation(s).

Req T165: Data from approved Update Pre-Authorisations (e.g., amount and authorisation code) shall be stored for future use as needed.

If the Update Pre-Authorisation is performed using a Card Application then the relevant Card Application data shall be stored for subsequent steps.

Req T166: An Update Pre-Authorisation shall include the increment or decrement amount to be authorised.

Req T167: If the cardholder is participating, the cardholder display shall clearly indicate that the amount to be confirmed is the increment or decrement amount.

Req T168: If the Update Pre-Authorisation is declined, the previously linked Pre-Authorisation (or Update Pre-Authorisation(s)) shall remain unchanged and valid.

Req T169: As soon as it is known that a Pre-Authorisation and any Update Pre-Authorisation linked to it will not be used, the previously authorised amount(s) must be released by a Cancellation. In this case Payment Completion shall not follow.

4.3.4.1.2.2 Authorisation

Req T170: An Update Pre-Authorisation shall be processed online.

4.3.4.1.2.3 Completion

Req T171: The transaction receipt, if any, shall clearly show that this is an Update Pre-Authorisation and shall indicate the increment or decrement amount.

4.3.4.1.2.4 Data Capture

Req T172: Approved Update Pre-Authorisations shall not be captured.

4.3.4.2 Payment Completion Service

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 Completion Service for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	C	N/A	N/A
Transaction Initialisation	M	M	M
Technology Selection	C	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	N/A	N/A	N/A
Cardholder Verification	N/A	N/A	N/A
Authorisation	N/A	N/A	N/A
Referral	N/A	N/A	N/A
Completion	M	M	M
(Partial) Reversal	N/A	N/A	N/A
Data Capture	M	M	M

TABLE 13: 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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and/or MOTO (Physical POI or Virtual Terminal).

4.3.4.2.1 POI Application

The Payment Completion may be performed in a different Acceptance Environment and Acceptance Technology to that used for the Pre-Authorisation and Update Pre-Authorisation(s).

Req T173: When the final amount is known and not zero, a Payment Completion shall be performed, provided the final amount does not exceed the accumulated authorised amount(s).

The accumulated authorised amount can only be exceeded by the configurable overspent percentage, if allowed by scheme rules.

If the accumulated authorised amount is exceeded by the configurable overspent percentage allowed by scheme rules, an Update Pre-Authorisation shall be performed for the difference, before the Payment Completion Service is performed.

Req T174: If the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology is used, it is only for the purpose of retrieving the Card Data for the Payment Completion transaction, not to perform a Card transaction. Therefore, EMV processing shall be followed until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the Expiry Date. If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the Card Application.

Req T175: A Payment Completion shall be identified as such in transaction data and shall contain the unique reference from the original linked Pre-Authorisation.

Req T176: A Payment Completion shall include the final amount.

Req T177: 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 T178: 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.

4.3.4.2.3 Data Capture

Req T179: If a Card Application was used in one of the Pre-Authorisation Service(s), the Card Data to be used for the Payment Completion Service shall be the Card Application data retained from the Pre-Authorisation Service.

4.3.5 Deferred Payment

Only Local Card Transactions (Physical POI) are allowed for processing the Deferred Payment Service.

TABLE 14 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Deferred Payment Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	×
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	×	×

TABLE 14: DEFERRED PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 15 shows which Functions are not applicable (N/A) or which are either mandatory (M), optional (O) or conditional (C) for the Deferred Payment Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	N/A	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	N/A	N/A
Card Data Retrieval	M	N/A	N/A
Card Authentication	C	N/A	N/A
Cardholder Verification	M	N/A	N/A
Authorisation	M	N/A	N/A
Referral	O	N/A	N/A
Completion	M	N/A	N/A
(Partial) Reversal	C	N/A	N/A
Data Capture	M	N/A	N/A

TABLE 15: 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 for Local Transactions (Physical POI).

4.3.5.1 POI Application

Req T180: 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 T181: The transaction amount for authorisation shall be checked against a maximum allowed amount if configured for the Application Profile. If the check fails, the transaction shall not proceed.

Req T182: The cardholder shall be able to confirm the transaction amount for authorisation and the Payment Brand 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 Physical Card or Mobile Device or explicit with a confirmation display, if confirmation of the transaction amount is configured for the Application Profile.

4.3.5.2 Configuration

Req T183: It shall be configured that the Chip with Contact Acceptance Technology and/or the Contactless Acceptance Technology shall be supported (see Req T18) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T22).

Req T184: It shall be possible to configure per Application Profile, if the transaction amount shall be checked against a maximum allowed amount.

Req T185: For Deferred Payment, it shall be possible to configure per Application Profile, if the transaction amount shall be confirmed by the cardholder.

Req T186: 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 T187: 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 T188: Deferred Payment shall be authorised online.

Req T189: 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 T190: 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 T192.

4.3.5.5 Completion

Req T191: The POI shall receive the delivery result from the sale system, including the final amount which may be a zero amount.

Req T192: A notification of the final amount that shall not exceed the authorised 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 T193: The POI shall send a message to the sale system to indicate the transaction result.

4.3.5.6 Data Capture

Req T194: Data Capture shall be performed either as online capture through a completion message sent after each transaction (referred to as notification message in T192) 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 "Card Not present" Service, which can only be performed using recorded Card Data information including PAN and Expiry Date, because the reservation process (e.g., of a hotel room or a rental car) does not normally involve the Cardholder Environment being present or the Card Application being read. This data would have been previously received:

- By phone, via a secure fax or from a letter in which case the PAN and Expiry could be recorded on a manual folio or on a paper booking schedule.
- Electronically from a booking agent or via a web service, in which case it would be regarded as "Stored Card Data", which is commonly thought of as electronically stored.

In the event the Card and Cardholder are physically present at time of the reservation, only PAN and Expiry Date would be taken, for the purposes of the guaranteed reservation, in the event a No-Show needs to be processed.

Therefore, Stored Card Data or Manual Key Entry are the only Acceptance Technologies used for this Service. In addition, this Service is restricted to the Acceptance Environments Attended Physical POI or Virtual Terminal.

TABLE 16 shows which combination of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO is allowed (✓) or not allowed/not applicable (×) for the No-Show Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	×	×	×	×
Magnetic Stripe	×	×	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	×	×	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	✓	×	×	✓

TABLE 16: NO-SHOW: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS

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 No-Show Service and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	N/A	N/A	N/A
Transaction Initialisation	M	N/A	M
Technology Selection	N/A	N/A	N/A
Selection of the Application	M	N/A	M
Card Data Retrieval	M	N/A	M
Card Authentication	N/A	N/A	N/A
Cardholder Verification	N/A	N/A	N/A
Authorisation	M	N/A	M
Referral	O	N/A	N/A
Completion	M	N/A	M
(Partial) Reversal	C	N/A	C
Data Capture	M	N/A	M

TABLE 17: 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 for Local Transactions (Attended Physical POI) and MOTO (Attended Physical POI or Virtual Terminal).

4.3.6.1 Authorisation

Req T195: No-Show transactions shall be authorised online and shall be identified as No-Show.

4.3.6.2 Data Capture

Req T196: 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 "Card Not present" transactions where the Card Data used is extracted from Stored Card Data or is manually entered. In addition,

subsequent transactions of an Instalment Payment are not necessarily initiated by the POI that performed the first Instalment Payment transaction.

In particular, for the first transaction Card Authentication and Cardholder Verification may be performed whereas in subsequent transactions these Functions will not be performed.

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 18 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the first transaction of an Instalment Payment.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	✓	✓[34]
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

TABLE 18: INSTALMENT PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION

The column "Requirement" in TABLE 19 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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual

[34] On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	M	M
Cardholder Verification	M	M	N/A
Authorisation	M	M	M
Referral	O	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	M	M	M

TABLE 19: 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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal)

4.3.7.1.1 POI Application

Req T197: 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 T198: The allowed maximum total Instalment amount shall be configurable.

4.3.7.1.3 Authorisation

Req T199: 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 T200: 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 transactions shall be made in the payment plan (e.g., 1:6 to indicate the first of 6 transactions).

4.3.7.2 Subsequent Transactions

Regardless what Acceptance Technology or Acceptance Environment was used for the first transaction, subsequent transactions will use Stored Card Data and may be processed by the Acceptor or entirely in the environment of the PSP. The Cardholder will not be involved.

The column "Requirement" in Table 20 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 for all Acceptance Environments. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

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

TABLE 20: 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 T201: Subsequent Instalment Payment transactions shall be authorised online using only PAN and Expiry Date and shall include the information which identifies the instalment number being processed from the payment plan (e.g., 3:6 to indicate the third of 6 Instalment Payments).

4.3.7.2.2 Data Capture

Req T202: 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 the third of 6 Instalment Payments).

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 "Card Not present" transactions where the Card Data used is extracted from Stored Card Data or is manually entered. In addition, subsequent transactions of a Recurring Payment are not necessarily initiated by the POI that performed the first Recurring Payment transaction.

In particular, for the first transaction Card Authentication and Cardholder Verification may be performed whereas in subsequent transactions these Functions will not be performed.

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 21 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the first transaction of a Recurring Payment.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	✓	✓
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

TABLE 21: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION

The column "Requirement" in TABLE 22 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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual

Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	M	M
Cardholder Verification	M	M	N/A
Authorisation	M	M	M
Referral	O	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	M	M	M

TABLE 22: 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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

4.3.8.1.1 POI Application

Req T203: 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 T204: 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 T205: The data captured for clearing of the first transaction of a Recurring Payment shall additionally contain specific information which identifies it as a Recurring Payment transaction.

4.3.8.2 Subsequent Transactions

Regardless what Acceptance Technology or Acceptance Environment was used for the first transaction, subsequent transactions will use Stored Card Data and may be processed by the Acceptor or entirely in the environment of the PSP. The Cardholder will not be involved.

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 for all Acceptance Environments. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement
Language Selection	N/A
Transaction Initialisation	M
Technology Selection	N/A
Selection of the Application	M
Card Data Retrieval	M
Card Authentication	N/A
Cardholder Verification	N/A
Authorisation	M
Referral	N/A
Completion	M
(Partial) 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 T206: Subsequent Recurring Payment transactions shall be authorised online using only PAN and Expiry Date and shall contain specific information which identifies it as a Recurring Payment transaction.

4.3.8.2.2 Data Capture

Req T207: 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 used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Quasi-Cash Payment Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	×	✓[35]
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The

[35] On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	M	M
Cardholder Verification	M	M	N/A
Authorisation	M	M	M
Referral	O	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	M	M	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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

4.3.9.1 POI Application

Req T208: 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 T209: 'No CVM Required' shall not be supported for Quasi-Cash Payment transactions.

4.3.9.3 Authorisation

Req T210: The Quasi-Cash Payment shall be authorised online and it shall be identified as a Quasi-Cash Payment.

4.3.9.4 Reversal

Req T211: 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 T212: 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 T213: The data captured for clearing of a Quasi-Cash Payment shall identify it as a Quasi-Cash Payment.

4.4 Cash Services

Only Local Card Transactions (Physical POI) are allowed for processing the 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 used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the ATM Cash Withdrawal Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	×	✓	×	×
Magnetic Stripe	×	✓	×	×
Manual Entry (by Acceptor)	×	×	×	×
Contactless (Chip and Mobile)	×	✓	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The

condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	N/A	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	N/A	N/A
Card Data Retrieval	M	N/A	N/A
Card Authentication	C	N/A	N/A
Cardholder Verification	M	N/A	N/A
Authorisation	M	N/A	N/A
Referral	N/A	N/A	N/A
Completion	M	N/A	N/A
(Partial) Reversal	M	N/A	N/A
Data Capture	M	N/A	N/A

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 for Local Transactions (Physical POI).

4.4.1.1 Configuration

Req T214: It shall be configured that the Chip with Contact Acceptance Technology shall be supported (see Req T18) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T22).

4.4.1.2 Transaction Initialisation

Req T215: The Welcome Screen shall be shown initially in the default language and English (or in the default language only if it is English).

Req T216: Transactions on the ATM shall be initiated by insertion of a Physical Card or by Cardholder interaction.

4.4.1.3 Authorisation

Req T217: ATM Cash Withdrawal transactions shall be authorised online. Otherwise ATM transactions shall be declined.

4.4.1.4 Completion

Req T218: To minimise the risk of the cardholder leaving the Physical 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 T219: If the Physical Card is inserted in the reader of an ATM with card capture capability and if the Cardholder does not retrieve the Card, the Card shall be retained.

Req T220: If the Physical Card is retained in response to the authorisation response message, an appropriate message shall be displayed to inform the Cardholder.

Req T221: An ATM shall not allow a declined transaction to be accepted.

Req T222: For ATM Cash Withdrawal transactions using the Contactless Acceptance Technology further transactions after the Cash Withdrawal are not allowed without new presentment of the Physical Card or Mobile Device.

4.4.1.5 Reversal

Req T223: If the actual amount was authorised but cash could not be delivered, a reversal shall be performed to nullify the original authorisation.

Req T224: 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 used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Cash Advance Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	×	×	×
Magnetic Stripe	✓	×	×	×
Manual Entry (by Acceptor)	✓	×	×	×
Contactless (Chip and Mobile)	✓	×	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	N/A	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	N/A	N/A
Card Data Retrieval	M	N/A	N/A
Card Authentication	C	N/A	N/A
Cardholder Verification	M	N/A	N/A
Authorisation	M	N/A	N/A
Referral	O	N/A	N/A
Completion	M	N/A	N/A
(Partial) Reversal	C	N/A	N/A
Data Capture	M	N/A	N/A

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 for Local Transactions (Physical POI).

4.4.2.1 POI Application

Req T225 The Cash Advance Service shall follow the same process as the Payment Service for all available Acceptance Technologies, but using its own configuration.

4.4.2.2 Configuration

Req T226: For Cash Advance, it shall be configured that the Chip with Contact Acceptance Technology and/or the Contactless Acceptance Technology shall be supported (see Req T18) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T22).

Req T227: 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 T228: 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 T229: No CVM Required shall not be supported for the Cash Advance Service.

4.4.2.5 Authorisation

Req T230: Cash Advance transactions shall be authorised online. If the Referral Function is activated and a Referral is received in the Authorisation Response message, the Voice Authorisation process shall be followed. Otherwise Cash Advance transactions shall be declined.

4.4.2.6 Reversal

Req T231: If the actual amount was authorised but cash could not 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 used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Card Validity Check Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	✓	×
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	✓

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	C	N/A
Cardholder Verification	O	O	N/A
Authorisation	M	M	M
Referral	N/A	N/A	N/A
Completion	M	M	M
(Partial) Reversal	N/A	N/A	N/A
Data Capture	N/A	N/A	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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

4.5.1.1 POI Application

Req T232: 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 T233: For Card Validity Check, the authorised amount sent to the Card Application shall be set to zero.

4.5.1.3 Authorisation

Req T234: Card Validity Check transactions shall be authorised online. Otherwise Card Validity Check transactions shall be declined.

Req T235: Card Validity Check transactions shall be identified as such in the online authorisation request.

4.5.1.4 Data Capture

Req T236: Card Validity Check transactions shall not be captured for "Financial Presentment".

4.5.2 Balance Inquiry

Only Local Card Transactions (Physical POI) are allowed for processing the Balance Inquiry Service.

TABLE 32 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Balance Inquiry Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	×
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	×	×
Consumer Device with Payment Credentials and Authentication Application	×	×	×	×
Consumer Device with (M)RP Application	×	×	×	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	N/A	N/A
Transaction Initialisation	M	N/A	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	N/A	N/A
Card Data Retrieval	M	N/A	N/A
Card Authentication	C	N/A	N/A
Cardholder Verification	M	N/A	N/A
Authorisation	M	N/A	N/A
Referral	N/A	N/A	N/A
Completion	M	N/A	N/A
(Partial) Reversal	N/A	N/A	N/A
Data Capture	N/A	N/A	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 for Local Transactions (Physical POI).

4.5.2.1 POI Application

Req T237: 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 T238: For Balance Inquiry, the authorised amount sent to the Card Application shall be set to zero.

4.5.2.3 Authorisation

Req T239: Balance Inquiry transactions shall be authorised online. Otherwise Balance Inquiry transactions shall be declined.

Req T240: Balance Inquiry transactions shall be identified as such in the online authorisation request.

Req T241: The balance of the Card Account shall only be retrieved from a positive authorisation response.

4.5.2.4 Completion

Req T242: 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 T243 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 by the Cardholder of the Card Account to be credited. Such an account is called Funding Account. There may be more than one Funding Account for a Card Account. If several Funding Accounts are defined for a Card Account, one of these accounts shall be defined as default. The entity that processes authorisations for the Card Account shall know the Funding Account(s) defined for the Card Account 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 Card Present transaction. The 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.

Only Local Card Transactions (Physical POI) and e- and m-commerce (Virtual POI) are allowed for processing the Card Funds Transfer Service.

TABLE 34 shows which combinations of Acceptance Technologies for the funding card and used in Local Transactions, e- and m-commerce and MOTO Acceptance Environments are allowed (✓) or not allowed/not applicable (×) for the Card Funds Transfer Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	×
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	N/A
Card Data Retrieval	M	M	N/A
Card Authentication	C	M	N/A
Cardholder Verification	M	M	N/A
Authorisation	M	M	N/A
Referral	N/A	N/A	N/A
Completion	M	M	N/A
(Partial) Reversal	C	C	N/A
Data Capture	C	C	N/A

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 for Local Transactions (Physical POI) and e- and m-commerce (Virtual POI).

4.6.1.1 POI Application

Req T244: 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 T245: 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 T246: The cardholder shall be able to select the transaction amount to be credited to or debited from the Card Account.

Req T247: In the case of a (Mobile) EMV Payment Application based or (M)RP Application based Card Funds Transfer transaction, the application shall only be used for the purpose of retrieving the Card Data, not to perform a Payment transaction.

4.6.1.3 Card Data Retrieval

Req T248: 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. If a (Mobile) EMV Payment Application or (M)RP Application is used to process the Card Funds Transfer transaction, this information may be retrieved from the Card Application.

Req T249: 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 T250: After the Card Data Retrieval Function has obtained either the relevant Card Data (e.g., 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 T251: Card Funds Transfer transactions shall be authorised online and shall be identified as Card Funds Transfer.

Req T252: 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 T253: 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

Only Local Card Transactions (Physical POI) and e- and m-commerce (Virtual POI) are allowed for processing the Original Credit Service.

TABLE 36 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Original Credit Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	×	×	×
Magnetic Stripe	✓	×	×	×
Manual Entry (by Acceptor)	✓	×	×	×
Contactless (Chip and Mobile)	✓	×	×	×
Manual Entry (by Cardholder)	×	×	×	×
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	N/A
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	N/A
Card Data Retrieval	M	M	N/A
Card Authentication	N/A	N/A	N/A
Cardholder Verification	N/A	N/A	N/A
Authorisation	O	O	N/A
Referral	N/A	N/A	N/A
Completion	M	M	N/A
(Partial) Reversal	C	C	N/A
Data Capture	M	M	N/A

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 for Local Transactions (Physical POI) and e- and m-commerce (Virtual POI).

4.6.2.1 POI Application

Req T254: The Original Credit Service shall always be initiated by the Acceptor, never by the Cardholder.

Req T255: If the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology is used, it is only for the purpose of retrieving the Card Data for the Original Credit transaction, not to perform a Card transaction. Therefore, EMV processing shall be followed until the Card Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the Expiry Date. If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the card.

In the case of an (M)RP Application based Original Credit transaction, the (M)RP Application process shall be terminated after the Card Data Retrieval Function has obtained either the relevant card data (e.g., the Track 2 equivalent data), or the PAN together with the Expiry Date.

If the Card Application requires entry of an amount, the amount given to the Card Application during the Original Credit should be zero to avoid unnecessary Card Risk Management.

Req T256: The transaction amount shall be checked against a maximum allowed amount if configured for the Application Profile. If the check fails, the transaction shall not proceed.

4.6.2.2 Configuration

Req T257: 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 T258: It shall be configurable per Application Profile, whether the Original Credit is performed online or not.

4.6.2.3 Transaction Initialisation

Req T259: The Original Credit amount shall be available to the POI Application at Transaction Initialisation.

4.6.2.4 Authorisation

Req T260: 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 has provided funds to the issuer of the Prepaid Card which is subsequently used to fund the load transaction. The Prepaid Card

Unloading Service requires that the issuer of the prepaid card has agreed which cardholder account shall be used to unload the prepaid Card Account.

The 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 used in Local Transactions, e- and m-commerce and MOTO are allowed (✓) or not allowed/not applicable (×) for the Prepaid Card - Loading & Unloading Service.

Acceptance Technologies	Local Transactions Physical POI		e- and m-commerce Virtual POI	MOTO Physical POI or Virtual Terminal
	Attended	Unattended		
Chip with Contact	✓	✓	×	×
Magnetic Stripe	✓	✓	×	×
Manual Entry (by Acceptor)	✓	×	×	✓
Contactless (Chip and Mobile)	✓	✓	×	×
Manual Entry (by Cardholder)	×	×	✓	×
Consumer Device with Payment Credentials	×	×	✓	×
Consumer Device with Payment Credentials and Authentication Application	×	×	✓	×
Consumer Device with (M)RP Application	×	×	✓	×
Stored Card Data	×	×	×	×

TABLE 38: PREPAID 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 and for Local Transactions, e- and m-commerce and MOTO using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual

Terminal. The condition (C) for conditional Functions is described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions Physical POI	**e- and m-commerce Virtual POI**	**MOTO Physical POI or Virtual Terminal**
Language Selection	M	O	N/A
Transaction Initialisation	M	M	M
Technology Selection	M	N/A	N/A
Selection of the Application	M	M	M
Card Data Retrieval	M	M	M
Card Authentication	C	M	M
Cardholder Verification	M	M	M
Authorisation	M	M	M
Referral	N/A	N/A	N/A
Completion	M	M	M
(Partial) Reversal	C	C	C
Data Capture	C	C	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 for Local Transactions (Physical POI), e- and m-commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

4.6.3.1 POI Application

Req T261: 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 T262: The cardholder shall be able to select whether the prepaid card shall be loaded or unloaded.

Req T263: The cardholder shall be able to select the transaction amount to be loaded to or unloaded from the prepaid Card Account.

Req T264: In the case of a Prepaid Card - Loading & Unloading transaction based on a (Mobile) EMV Payment Application or an (M)RP Application the amount given to the Card Application 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 T265: After the Card Data Retrieval Function has obtained either the relevant card data (e.g., 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 T266: Prepaid Card - Loading & Unloading transactions shall be authorised online and shall be identified as Prepaid Card - Loading & Unloading.

Req T267: 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 T268: 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 T269: Payment with Increased Amount shall be restricted to the Payment Service at the attended Physical POI.

Req T270: Any extra amount shall be included in the transaction amount before or during Transaction Initialisation.

Req T271: The extra amount shall be displayed separately for transaction confirmation and printed on the receipt, if any.

4.7.2 Payment with Cashback

Req T272: 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.

Req T273: Payment with Cashback shall be restricted to the Payment Service at the attended Physical POI.

Req T274: For a Payment with Cashback, the transaction amount shall be the sum of the payment amount and the Cashback amount.

Req T275 The Cashback amount shall be identified separately in the authorisation and settlement messages.

Req T276: For a Payment with Cashback transaction, the Cashback amount to be confirmed shall be displayed 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 the display size permits.
- Cashback amount and (total) transaction amount shall be displayed.

Req T277: Cardholder confirmation of the Cashback amount shall be implicit with the confirmation of the transaction amount.

Req T278: 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 T279: For attended POIs that support Payment with Cashback, it shall be possible to configure per Application Profile a maximum Cashback amount.

Req T280: 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 T281: Payment with Cashback transactions shall be authorised online.

Req T282: The POI Application shall support handling of an authorisation response indicating the payment part is authorised but the Cashback is not.

Req T283: If a receipt is printed for a Payment with Cashback transaction, then in addition to the data listed in Req T91 the following data shall also be printed:

- Payment amount
- Cashback amount

4.7.3 Payment with Purchasing or Corporate Card Data

Req T284: 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 T285: 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 distinguish a purchasing or corporate Card Data, from Card Data of other products in that scheme.

Req T286: If a Payment transaction is performed with Card Data 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 T287: 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 T288: When online capture methods are used, if allowed by scheme rules, only the Acquirer may aggregate the Payment transactions.

Req T289: The maximum amount of the aggregated Payment transactions shall be defined by Scheme rules.

Req T290: (Mobile) EMV Payment Application and (M)RP Application based Payment transactions shall be aggregated separately from Payment transactions based on other Acceptance Technologies.

Req T291: For aggregated (Mobile) EMV Payment Application or (M)RP Application based Payment transactions, the cryptogram of the last aggregated transaction shall be sent together with the data elements used to calculate it.

Req T292: 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.

4.7.5 Payment with Deferred Authorisation

Req T293: 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.

Req T294: Payment with Deferred Authorisation shall be restricted to the Payment Service at the Physical or Virtual POI.

Req T295: It shall be configurable which of the Acceptance Technologies supported for Payment are allowed for Deferred Authorisation.

Req T296: It shall be configurable whether Deferred Authorisation is initiated automatically or only on request of an attendant.

Req T297: It shall be possible to activate/deactivate Deferred Authorisation for Payment per Application Profile.

Req T298: A minimum and a maximum amount for Payment with Deferred Authorisation shall be configurable per Application Profile.

Req T299: 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 T300: It shall be configurable per Application Profile whether Deferred Authorisation shall only be allowed for Card Application based transactions if Offline Data Authentication was successfully performed.

Req T301: For 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 authorised offline by a Card Application.

If necessary according to the Application Profile configuration, confirmation of an attendant shall be requested for Deferred Authorisation.

Req T302: If Deferred Authorisation cannot be performed according to the Application Profile configuration the transaction shall be declined, and Completion and Data Capture for a declined Payment transaction shall be performed. Note that if configured for the Completion function this process may include forcing acceptance by an attendant.

Req T303: If Deferred Authorisation can be performed according to the Application Profile configuration, Completion of an approved transaction shall be performed for the cardholder (display and receipt, if any).

Req T304: If Deferred Authorisation can be performed according to the Application Profile configuration, the transaction shall be stored in the POI and authorised online when the POI is again able to go online. In case of a (Mobile) EMV Payment Application or (M)RP Application based transaction, the cryptogram of the original transaction together with the data elements used for its calculation shall be stored and used for the deferred online authorisation.

Req T305: If Deferred Authorisation has been performed for a (Mobile) EMV Payment Application or (M)RP Application based transaction, the cryptogram of the original transaction together with the data elements used for its calculation shall also be used for Data Capture.

4.7.6 Dynamic Currency Conversion (DCC)

DCC is an additional feature which may be used for Payment and Cash Services.

Req T306: It shall be configurable per Application Profile, whether DCC is supported.

Req T307: To perform DCC, the POI or attendant shall give the cardholder the choice of currency to be used, the cardholder billing 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 billing currency and
- The conversion rate (ratio) used to calculate the amount in the cardholder billing currency.

Req T308: If the POI is used to offer the choice to the cardholder 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 billing 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 T309: If the cardholder selects the transaction amount in the cardholder billing currency, then the total transaction amount and, if applicable, a Cashback amount shall be in the cardholder billing currency. Cash obtained from the card acceptor in the process of Cashback shall be in the card acceptor's currency.

Req T310: If the cardholder has selected the transaction amount in the cardholder billing currency, the amounts shall be conveyed to the cardholder in both the cardholder billing currency and the card acceptor's currency. The conversion rate used shall also be included.

Req T311: If the cardholder has selected the transaction amount in the cardholder billing currency and if a transaction receipt is being produced, the amounts shown on the receipt shall be expressed in the cardholder billing currency and in the card acceptor's currency. The conversion rate used shall also be included.

Req T312: If for a Contact EMV Payment Application or (M)RP Application based transaction data from the Contact EMV Payment Application or (M)RP Application are needed to determine the cardholder billing 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 billing currency,

then the Contact EMV Payment Application or (M)RP application based transaction shall be re-started without further cardholder interaction with the previously selected application.

4.7.7 Surcharging/Rebate

Surcharging/Rebate is an additional feature which may be used for Payment and Cash Services.

Req T313: For Payment Services, any kind of surcharge/rebate shall be part of the agreed total sales amount.[36]

Req T314: 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 T315: For a Cash Withdrawal with surcharge/rebate, the transaction amount shall be the total of the withdrawal amount and the surcharge/rebate amount.

[36] Note that surcharging/rebate is subject to scheme or legal regulations.

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 P7 below).

POI connected directly to an acquirer host:

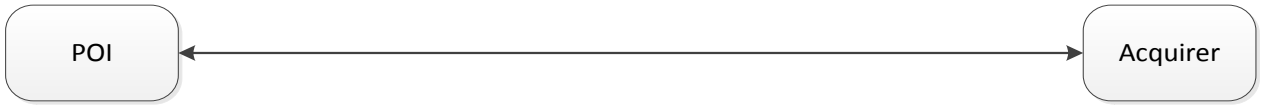

FIGURE 40: POI CONNECTED DIRECTLY TO AN ACQUIRER HOST

POI directly connected to several acquirers:

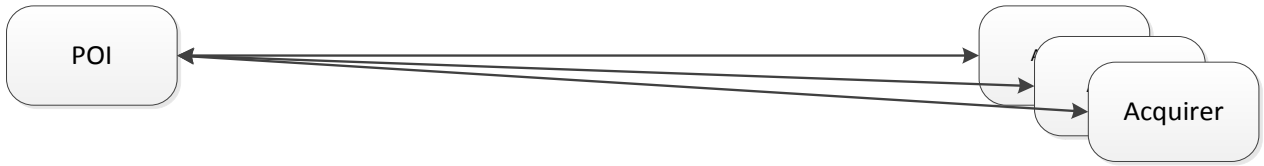

FIGURE 41: POI DIRECTLY CONNECTED TO SEVERAL ACQUIRERS

Environment of large retailer:

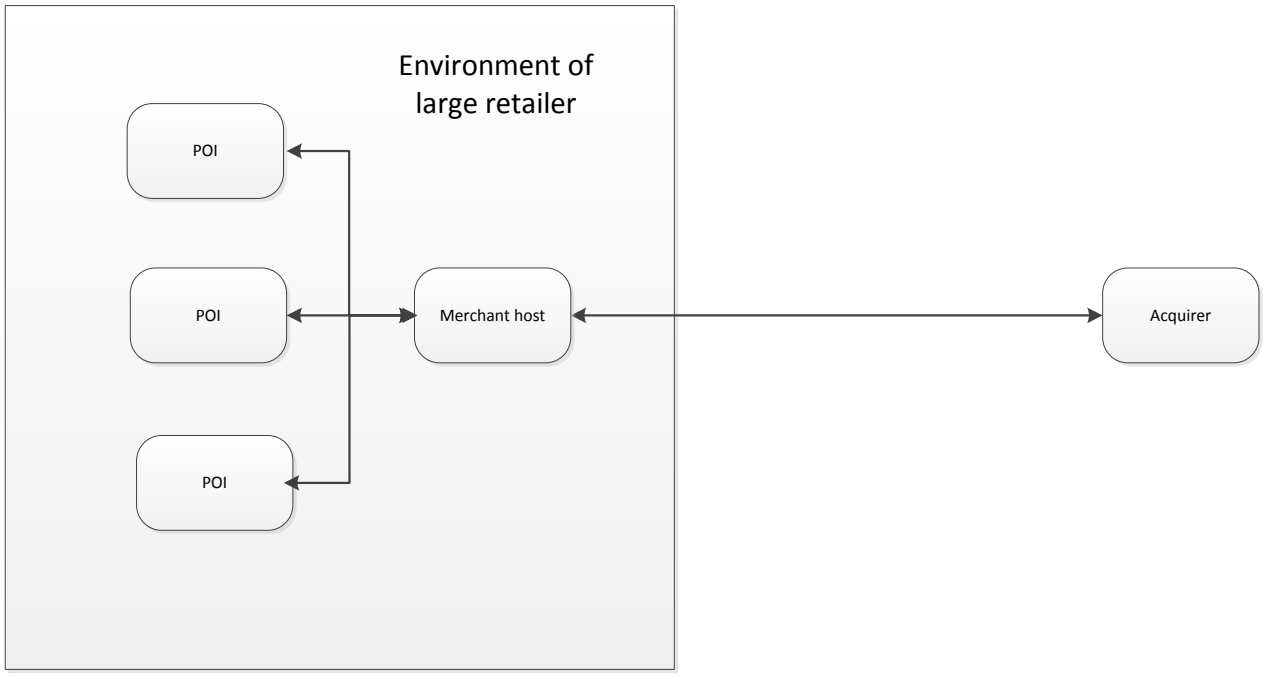

FIGURE 42: ENVIRONMENT OF LARGE RETAILER

Environment of a terminal provider:

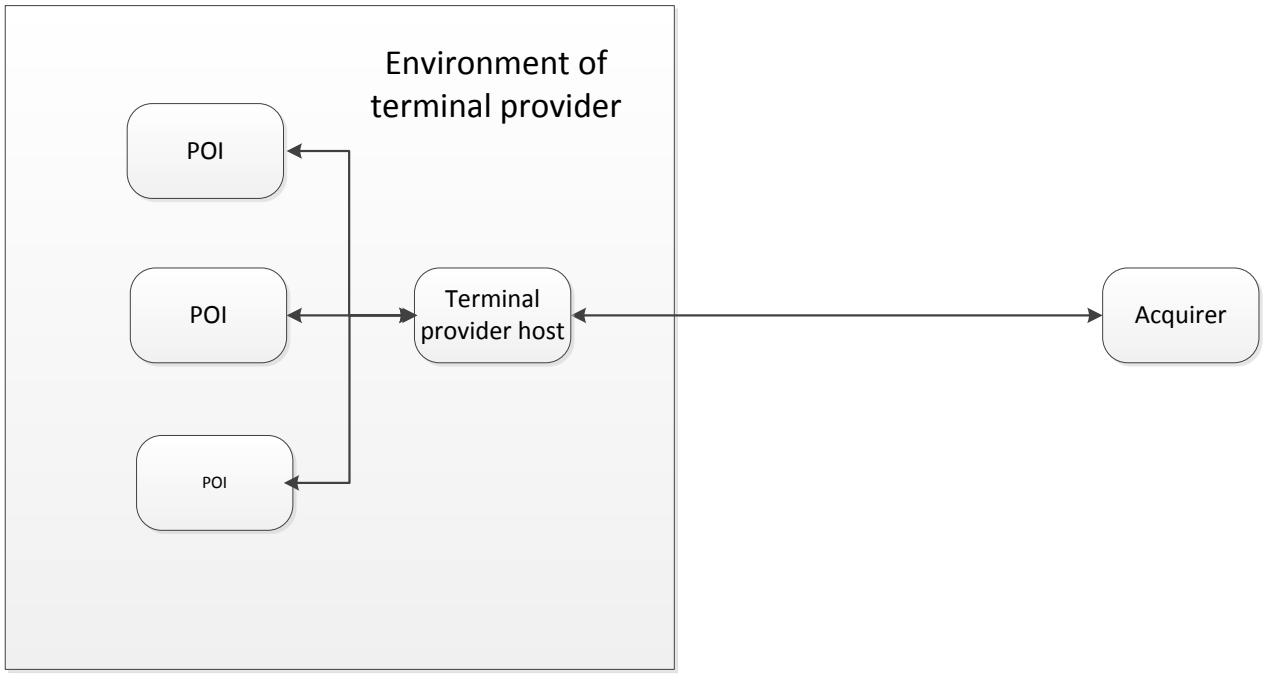

FIGURE 43: ENVIRONMENT OF A TERMINAL PROVIDER

Environment with an intermediate agent:

FIGURE 44: ENVIRONMENT WITH AN INTERMEDIATE AGENT

Intermediate host connected to several acquirers:

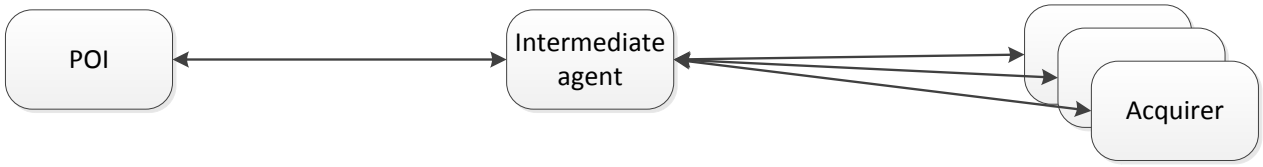

FIGURE 45: INTERMEDIATE HOST CONNECTED TO SEVERAL ACQUIRERS

Req P1: The T2A protocols shall support the Card Services as described 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 T2A protocols shall be designed to accommodate all types of POI architectures relevant to the Acceptance Environment.

Req P8: 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 P9: The T2A protocols shall support sending 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 P10: The T2A protocols shall be designed to allow POIs to process transactions with different acquirers.

ANNEX 1 - FIGURES AND TABLES