

SEPA ~~CARDS-PAYMENTS~~ STANDARDISATION (~~SPCS~~) "VOLUME"

STANDARDS' REQUIREMENTS

BOOK 2

FUNCTIONAL REQUIREMENTS

*Payments and Cash Withdrawals ~~with Cards~~ in SEPA
Applicable Standards and Conformance Processes*

© European ~~Cards-Payments~~ Stakeholders Group AISBL.

Any and all rights are the exclusive property of

EUROPEAN ~~CARDS-PAYMENTS~~ STAKEHOLDERS GROUP AISBL.

Abstract	This document contains the work on SEPA cards—payment standardisation to date
Document Reference	ECSG001-18
Issue	Book 2 – v10.5
Date of Version	27.11.2025
Reason for Issue	Public consultation
Reviewed by	EPSG Board – 25 November 2025
Produced by	EPSG Book 2 Expert Team
Owned and Authorised by	EPSG
Circulation	Public (draft for consultation release)

Change History of Book 2		
6.2.0	2012-2013	Working version of Book 2
7.2.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.2.1.0	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
8.2.40	22.11.2018	Board Approval version for Consultation as 8.5
8.2.50	17.12.2018	Public Consultation Release v8.5
8.5.3	26.06.2019	Working Version to v9.0
9.0	15.01.2020	ECSG Published version - Volume v9.0
9.1 – 9.4.7	15.09.2020 – 18.10.2021	Working Version 2020/2021
9.4.7	15.12.2021	Public Consultation Release v9.5
10.0	01.10.2022	ECSG Published version - Volume v10.0
<u>10.01- 10.28</u>	<u>2023-2025</u>	<u>Working Versions towards v10.5</u>
<u>10.5</u>	<u>27.11.2025</u> (published in December 2025)	<u>Public Consultation Release 10.5</u>

Table of Contents

1	GENERAL	5
1.1	Book 2 - Executive Summary	5
1.2	Description of Changes since the Last Version of Book 2	7
2	SCOPE	9
3	FUNCTIONAL REQUIREMENTS FOR PAYMENT DEVICES	23
3.1	Introduction	23
3.2	Electronic Product Identification	23
3.3	Local Customer Present Transactions	24
3.3.1	Chip with Contact	24
3.3.2	Chip and Mobile Contactless	25
3.3.3	Merchant-presented QR Code and Consumer-presented QR Code	27
3.4	Remote Customer Present Transactions	29
3.4.1	MOTO	29
3.4.2	e- and m-Commerce	29
4	POI FUNCTIONAL REQUIREMENTS	31
4.1	Introduction	31
4.2	Accessibility Requirements	33
4.3	General Requirements	34
4.3.1	POI Application	34
4.3.2	Configuration	40
4.3.3	Functions for Payment Service Processing	42
4.4	Basic Services	80
4.4.1	One-off Payment	80
4.4.2	Refund	87
4.4.3	Cancellation	90

4.4.4	Pre-Authorisation Services	94
4.4.5	Deferred Payment	103
4.4.6	No-Show	107
4.4.7	Instalment Payment	110
4.4.8	Recurring Payment	115
4.4.9	Quasi-Cash Payment	121
4.5	Cash Services	124
4.5.1	ATM Cash Withdrawal	124
4.5.2	Cash Advance (Attended)	127
4.6	Card Enquiry Services	131
4.6.1	Card Validity Check	131
4.6.2	Balance Enquiry	134
4.7	Card Electronic Transfer	137
4.7.1	Card Funds Transfer	137
4.7.2	Original Credit	141
4.7.3	Prepaid Card - Loading & Unloading	144
4.8	Additional Features	148
4.8.1	One-off Payment with Increased Amount	148
4.8.2	One-off Payment with Cashback	148
4.8.3	One-off Payment with Purchasing or Corporate Card Data	149
4.8.4	One-off Payment with Aggregated Amount	150
4.8.5	One-off Payment with Deferred Authorisation	150
4.8.6	Dynamic Currency Conversion (DCC)	152
4.8.7	Surcharging/Rebate	153
5	PROTOCOL FUNCTIONAL REQUIREMENTS FOR CARD TRANSACTIONS	155
	ANNEX 1 - FIGURES AND TABLES	159

1 GENERAL

1.1 Book 2 - Executive Summary

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

This book covers Local and Remote Card Transaction processing for all Payment Services as listed in Section 2.

In this version of the book, Local and Remote Instant Credit Transfer (ICT) Transaction processing is described based on published "Open Banking" standards and regulation (Model 1 according to Section 1.8 of Book 1) and for One-off Payment. ICT Transactions executed under the governance of an ICT Scheme (Model 2 according to Section 1.8 of Book 1) are not yet in scope for this version of the book, and Payment Services other than One-off Payment require extended "Open Banking" standards which are still under development.

These ~~Card-Payment~~ Services,

- ⇒ Involve, in general, a ~~Cardholder-Customer~~ and their ASPSP (called Issuer for Card based Payment Instruments), an Acceptor and their PSP (called Acquirer for Card based Payment Instruments), and, for ICT based Payment Instruments using Open Banking, the Acceptor's PISP;
- ⇒ Refer to Services where the ~~Cardholder-Customer~~ and the Acceptor interact using a particular Payment Device ~~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 Payment~~Physical-Card-or-Consumer~~ Device, in the Physical or Remote POI, in the Terminal to Acquirer/PISP Domain, and in the Acquirer/PISP to Issuer/Customer's ASPSP domain.

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

Table 2: Usage of Acceptance Environments and Payment Devices ~~Cardholder-Environments~~ for Local and Remote Transactions

Table 4: Book 2 Scope

Table 5: Mapping of Acceptance Technologies to Payment Devices~~Cardholder-Environments~~

Section 3 defines core functional requirements for Payment Devices~~Cardholder-Environments~~.

Section 4 defines core functional requirements for the POI.

Section 5 lists core functional requirements for Card Transaction protocols.

Details on security requirements may be found in Book 4.

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

Note: ~~Payment Device 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

In this new version of Book 2, functional descriptions and requirements for Payment Devices and POIs were adapted and extended to cover Instant Credit Transfer (ICT) Transaction processing based on published "Open Banking" standards and regulation for One-off Payment according to Section 1.8 of Book 1.

ICT Transaction processing for Payment Services other than One-off Payment is not yet in scope since it requires extended "Open Banking" standards which are still under development. One-off Payment is always performed with the participation of the Customer. Therefore, ICT-based processing of Acceptor Initiated Transactions (AIT) is not yet in scope either. In addition, in this version of Book 2, MOTO transactions are only described as Card Transactions. Although ICT-based MOTO transactions would theoretically be possible, MOTO transactions are excluded for ICT.

The more general terminology introduced in Book 1 to cover Card and ICT as Payment Instruments is used throughout almost the entire Book 2. However, in some requirements that are only applicable to Card Transaction processing, terms like "Cardholder" (instead of the more general term "Customer") may still be used in this version of Book 2.

In this Version of Book 2, Merchant-presented QR Code and Consumer-presented QR Code are introduced as new Acceptance Technologies, dedicated to ICT Transaction processing. Acceptance Technologies Chip with Contact, Chip Contactless and Mobile Contactless that are already in use for Card Transaction processing are also introduced for ICT Transaction processing. The Functions Technology Selection and Selection of the Application have been integrated into the more comprehensive Function Selection of the Payment Solution, facilitating selection of Acceptance Technology, Payment Brand and Payment Instrument for the Customer.

The more generic Function Authentication, i.e. is the Function to perform Strong Customer Authentication (SCA), applicable for Card and ICT Transaction processing, has replaced the Functions Card Authentication and Cardholder Verification in this version of Book 2. However, Card Authentication and Cardholder Verification are still described as technical functions to perform Authentication for EMV based transaction processing.

A clear distinction is now made between Acceptance Technology and methods for Account Data Retrieval and Authentication. In particular, in this version of Book 2, Manual Entry by Customer is no longer an Acceptance Technology for e- and m-Commerce. The Customer entering Account Data for a Remote Transaction is considered a method for Account Data Retrieval, using one of the Acceptance Technologies Consumer Device with Browser/Dedicated Application over Internet.

~~This new version of Book 2 was amended to incorporate the following:~~

- ~~• The following additions and clarifications were made in Book 2 due to the introduction of MIT and AIT, in particular the terminology and the structure has been adapted to better support these new concepts:~~
- ~~• Sections 2, 4.1, 4.3.3.9 have been updated.~~

- ~~Some subsection headings within sections 4.3 and 4.4 have been adapted.~~
- ~~Sections 4.4, 4.5, 4.6, 4.7 contain changes due to the restructuring.~~
- ~~Correction to clarify that Manual Entry is not applicable to AIT has been applied to Table 9, Table 11, and Table 18.~~
- ~~Reference to SRC has been included in sections 4.3.3.3.3 and 4.3.3.4.3.~~
- ~~References to offline authorisations of Remote Transactions have been removed from Requirements T82, T124, T140, T265.~~
- ~~Sections 4.4.4.1.1.1 and 4.4.4.1.2.1 have been updated for clarification regarding confirmation of the transaction amount.~~
- ~~Sections 4.4.4.1.1.3 and 4.4.4.1.2.2 have been added to clarify applicability of SCA for Pre-authorisation Services.~~
- ~~Recurring Payment (section 4.4.8) has been extended to include also Deferred Payments.~~
- ~~Correction to clarify that Manual Entry by Cardholder is applicable to e- and m-commerce for Quasi-Cash Payment, Card Funds Transfer, and Original Credit has been applied to Table 26, Table 36, and Table 38.~~
- ~~Integration of ECC-based protocols~~

2 SCOPE

This Volume differentiates between Local and Remote ~~Card~~ Transactions.

- A **Local ~~Card~~ Transaction** is a Card or ICT Transaction ~~conducted~~ initiated and completed¹ at the Acceptor's Physical POI which may be Attended (including Semi-Attended) or Unattended.

A Local Transaction is usually ~~initiated~~ performed with by the participation of Cardholder the Customer using a Payment Device. ~~Physical Card (Contact or Contactless) or an MCP Application on a Mobile Device in this~~ which case the Local Transaction is defined as a Local ~~Card Present~~ Customer Present Transaction.

When a transaction is ~~performed~~ initiated by the Acceptor based on ~~S~~ stored Card Account Data ~~without Customer participation~~, i.e. an MIT or a transaction where the Acceptor is the payer, then this is defined as an AIT (Acceptor Initiated Transaction). An AIT conducted at the Acceptor's Physical POI is defined as a Local AIT².

Local Card Transaction processing is described for all Payment Services listed in Table 3. Depending on the Service, Local Card Transactions are processed with the Customer present (i.e. as Local Customer Present Card Transaction) or without Customer participation (i.e. as Local Card AIT).

In this version of Book 2, Local ICT Transaction processing is only described for One-off Payment which is always performed with the participation of the Customer.

Therefore, in this version of Book 2, Local ICT Transactions with the Customer Present (i.e. Local Customer Present ICT Transactions) for processing Payment Services other than One-off Payment and all Local ICT Transactions without Customer participation (i.e. Local ICT AIT) are out of scope. Even if not stated explicitly, Local (Customer Present) ICT Transactions are only meant for processing One-off Payment, and Local AIT are only meant for processing Card Transactions based on Stored Card Data.

¹ Completed refers to the "Completion" Ffunction described in Section 4.3.3.8.

² Examples of ~~PaymentCard~~ Services that may be processed as Local or Remote AIT are

- Pre-Authorisation Services, No-Show, subsequent transactions of Instalment Payments and Recurring Payments (processed as MITs), or
- Refund and Original Credit (processed as AIT where the Acceptor is the Payer).

Currently, only One-off Payment and therefore no AIT are in scope for ICT Transactions.

Local Customer Present Card Transactions are processed based on EMV technology.

Usually, Local Customer Present ICT Transactions are non-EMV transactions processed as shown in Figures 5, 6 and 7 in Section 1.8 of Book 1 and are referred to as conventional Local ICT Transactions. However, there is an option to process Local Customer Present ICT Transactions based on EMV technology as shown in Figure 8 in Section 1.8 of Book 1, using an EMV Card Payment Application stored on the Payment Device.

Local Customer Present Card Transactions and Local Customer Present ICT Transactions based on EMV technology are called EMV based Local (Customer Present Card/ICT) Transactions.

- **A Remote ~~Card~~ Transaction** is a Card or ICT Transaction initiated and completed¹ conducted at the Acceptor's Virtual Remote POI or, only for MOTO, at a Virtual Terminal or Physical POI configured to perform MOTO transactions.

A Remote Transaction is usually initiated-performed with the participation of by the Cardholder-Customer (i.e. a Remote Customer Present Transaction). In this which case the Remote Transaction is e-Commerce, m-Commerce or MOTO:

- **e- and m-Commerce** Transactions are initiated by the Cardholder-Customer using a Consumer Device and are 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 ~~t~~** Transactions are conducted in the Acceptor's environment -using Manual Entry with the Cardholder-Customer interacting remotely for MOTO.

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

When a transaction is performed ~~initiated~~ by the Acceptor based on Stored Card Account Data without Customer Participation, i.e. an MIT or a transaction where the Acceptor is the payer, then this is defined as an AIT (Acceptor Initiated Transaction). An AIT conducted at the Acceptor's Remote POI is defined as a Remote AIT².

Remote Card Transaction processing is described for all Payment Services listed in Table 3. Depending on the Service, Remote Card Transactions are processed with the Customer present (i.e. as Remote Customer Present Card Transaction or, according to the definition above, as Card based e-Commerce, m-Commerce or MOTO) or without Customer participation (i.e. as Remote Card AIT).

In this version of Book 2, Remote ICT Transaction processing is only described for One-off Payment which is always performed with the participation of the Customer. In addition, in this version of Book 2, MOTO transactions are only described as Card Transactions. Although ICT based MOTO transactions would theoretically be possible, MOTO transactions are excluded for ICT.

Therefore, in this version of Book 2, Remote ICT Transactions with the Customer Present (i.e. Remote Customer Present ICT Transactions or, according to the definition above, ICT based e-Commerce, m-Commerce or MOTO) for processing Payment Services other than One-off Payment, ICT based MOTO transactions for processing One-off Payment and all Remote ICT Transactions without Customer participation (i.e. Remote ICT AIT) are out of scope. Even if not stated explicitly, Remote Customer Present ICT Transactions are only meant as e- and m-Commerce transactions for processing One-off Payment, and Remote AIT are only meant for processing Card Transactions based on Stored Card Data.

Note that for some Payment Services, a transaction may be conducted as AIT² or as may be initiated by the CustomerCardholder Present transaction, e.g. Refund and Pre-Authorisation Services.

An overview of the Acceptance Environments, the entity initiating the transaction at the POI in those environments and the Payment Devices and Acceptance Technologies used in the Acceptance Environments ~~and Cardholder Environments~~, is shown in the following **Table 1** for Local Transactions and **Table 2** for Remote Transactions. **Table 3** indicates for every Card Payment Service if it may be processed as a Customer Present transaction ~~initiated by the Cardholder Customer~~ or as an Acceptor Initiated Transaction (AIT) and, if so, whether it is an MIT.

Environment	Physical POI		
	Attended/ Semi-Attended POI ³		Unattended POI
Acceptance Environments:			
Initiated by:	Cardholder <u>Customer</u> ⁴	Acceptor ⁵ <u>6</u>	Cardholder <u>Customer</u>
Type of Transaction:	Local Card <u>Customer</u> Present	Local AIT	Local Card <u>Customer</u> Present
Cardholder Payment Devices:Environment:	Physical Card or Mobile <u>Consumer</u> Device ⁷	no Cardholder Environment <u>Payment Device</u> involved ⁵	Physical Card or Mobile <u>Consumer</u> Device ⁶
Acceptance Technologies for Card Transactions:	Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe, Manual Entry by Acceptor	Stored Card <u>Account</u> Data (stored by Acceptor) ⁵ <u>8</u>	Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe
Acceptance Technologies for ICT Transactions	<u>Conventional ICT Transaction:</u> <ul style="list-style-type: none"> Mobile NFC with Application Selection<u>Contactless</u> QR Code (Merchant-presented or Consumer-presented) <u>EMV based ICT Transaction:</u> <ul style="list-style-type: none"> Chip with Contact Chip Contactless Mobile Contactless 	<u>Stored Account Data (stored by Acceptor)⁵</u>	<u>Conventional ICT Transaction:</u> <ul style="list-style-type: none"> Mobile Contactless QR Code (Merchant-presented or Consumer-presented) <u>EMV based ICT Transaction:</u> <ul style="list-style-type: none"> Chip with Contact Chip Contactless Mobile Contactless

TABLE 1: USAGE OF ACCEPTANCE ENVIRONMENTS AND ~~CARDHOLDER-PAYMENT DEVICES~~ENVIRONMENTS FOR LOCAL TRANSACTIONS

³ According to the definition in Book 1, this Acceptance Environment also comprises Semi-Attended.

⁴ For attended POI, the Attendant operates the POI on behalf of the ~~Cardholder~~Customer.

⁵ This concerns AIT transactions which are based on Stored ~~Card~~Account Data and therefore do not involve any ~~Cardholder Environment~~Payment Device, in particular MITs e.g., No-Show transactions, subsequent transactions of Instalment Payments and Recurring Payments.

⁶ Not applicable to ICT Transactions for this version of this book, because One-off Payment does not allow AIT. Will be applicable if ICT Transaction processing is added for Payment Services allowing AIT.

⁷ Using the Mobile Device for ~~Mobile Contactless~~.

⁸ Also referred to as Stored Card Data for Card Transactions.

Environment Acceptance Environments:	Physical POI		Remote POI			
	Attended POI		Virtual Terminal		Virtual POI	
Initiated by:	Cardholder Customer ^{4 9}	Acceptor ^{5 6}	Cardholder Customer ^{10 9}	Acceptor ^{5 6}	Cardholder Customer	Acceptor ^{5 6}
Type of Transaction:	MOTO in an Acceptor attended environment.	Remote AIT	MOTO	Remote AIT	e- & m-Commerce	Remote AIT
Cardholder Environment Payment Device:	Physical Card or Virtual Card	no Cardholder Environment Payment Device involved ⁵	Physical Card or Virtual Card	no Cardholder Environment Payment Device involved ⁵	Physical Card or Virtual Card or Consumer Device ¹¹	no Cardholder Environment Payment Device involved ⁵
Acceptance Technologies:	Manual Entry by Acceptor	Stored Card Account Data (Stored by Acceptor) ⁵	Manual Entry by Acceptor or by Cardholder Customer ¹⁰	Stored Card Account Data (Stored by Acceptor) ⁵	Manual Entry by Cardholder Customer, Payment Credentials on Consumer Device, Payment Credentials on Consumer Device with Authentication Application Browser over Internet ¹² , Consumer Device with Dedicated (M)RP Application over Internet or Consumer Device	Stored Card Account Data (Stored by Acceptor) ⁵

⁹ Not applicable to ICT Transactions for this version of this book, because MOTO is only described for Card Transactions.

¹⁰ The Attendant operates the POI on behalf of the ~~Cardholder~~Customer, except the ~~Cardholder~~Customer uses DTMF.

¹¹ Physical Card or Virtual Card may be used as carrier of Account Data to be entered on the Virtual POI via the Consumer Device. And, in some scenarios, an EMV ~~Card Payment~~ Application stored on a Physical Card, in combination with an Additional Authentication Device, may be used for authentication.

¹² Through this Acceptance Technology, a Merchant-presented QR Code may be used to provide Acceptor data. However, in this case, the Merchant-presented QR Code is not considered to be the Acceptance Technology but a means of data transfer.

TABLE 2: USAGE OF ACCEPTANCE ENVIRONMENTS AND ~~CARDHOLDER ENVIRONMENTS~~ PAYMENT DEVICES FOR REMOTE TRANSACTIONS

Services	AIT (MIT s)	AIT (Acceptor as Payer)	Initiated by the Cardholder <u>Initiated by the Customer</u> <u>Present Transaction</u> ⁴
One-off Payment Deferred Payment Instalment Payment - First transaction Recurring Payment - First transaction Quasi-Cash Payment ATM Cash Withdrawal Cash Advance (Attended) Balance Enquiry Card Funds Transfer Prepaid Card - Loading & Unloading	N	N	Y
Refund (partial or total) Cancellation Original Credit	N	Y	Y
Pre-Authorisation Services Card Validity Check	Y	N	Y
No-Show Instalment Payment - Subsequent transactions Recurring Payment - Subsequent transactions ¹³	Y	N	N

TABLE 3: CATEGORISATION OF SERVICES BY AIT AND CUSTOMER PRESENT TRANSACTION ~~INITIATED BY THE CARDHOLDER~~CUSTOMER

Table 4 below represents the scope of Book 2 and lists for Local and Remote Card and ICT Transactions which of the following items are covered and allowed (this is indicated by a "Y"), or are not covered or not allowed (this is indicated by a "N") by the Volume, or are not covered in this version but may be covered in future releases of the Volume (this is indicated by a "N/A" ~~or "N"~~ respectively):

⇒ Card Payment Services

⇒ ~~Cardholder Environments~~Payment Devices and Acceptance Environments

⇒ Acceptance Technologies

⇒ Authentication Methods ~~Cardholder Verification Methods and Card Authentication Methods~~

¹³ ~~The subsequent transactions may be Payments or Deferred Payments.~~

⇒ Functions

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

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

~~"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 Payment Services, Cardholder Environments Payment Devices, Acceptance Environments, Acceptance Technologies, Cardholder Verification Authentication Methods, Card Authentication Methods and Functions are provided in Book 1.

	<u>SCS-SPS</u> Volume Book 2 Scope			
	<u>Card</u> Transactions		<u>ICT</u> Transactions	
	Local	Remote	<u>Local</u>	<u>Remote</u>
CARD-PAYMENT SERVICES				
<u>BASIC SERVICES</u>				
<u>One-off</u> Payment	Y	Y	<u>Y</u>	<u>Y</u>
Refund (partial or total)	Y	Y	<u>N/A</u>	<u>N/A</u>
Cancellation	Y	Y	<u>N/A</u>	<u>N/A</u>
Pre-Authorisation Services <ul style="list-style-type: none"> Pre-Authorisation Update Pre-Authorisation Payment Completion 	Y	Y	<u>N/A</u>	<u>N/A</u>
Deferred Payment	Y	N	<u>N/A</u>	<u>N/A</u>
No-Show	Y	Y	<u>N/A</u>	<u>N/A</u>
Instalment Payment	Y	Y	<u>N/A</u>	<u>N/A</u>
Recurring Payment	Y	Y	<u>N/A</u>	<u>N/A</u>
Quasi-Cash Payment	Y	Y	<u>N/A</u>	<u>N/A</u>
<u>CASH SERVICES</u>				
ATM Cash Withdrawal	Y	N	<u>N/A</u>	<u>N/A</u>
Cash Advance (Attended)	Y	N	<u>N/A</u>	<u>N/A</u>
Cash Deposit	N/A	N/A	<u>N/A</u>	<u>N/A</u>
<u>CARD ENQUIRY SERVICES</u>				
Card Validity Check	Y	Y	<u>N/A</u>	<u>N/A</u>
Balance Enquiry	Y	N/A	<u>N/A</u>	<u>N/A</u>

	SCS-SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
CARD ELECTRONIC TRANSFER <u>OF FUNDS</u>				
Card Funds Transfer	Y	Y	<u>N/A</u>	<u>N/A</u>
Original Credit	Y	Y	<u>N/A</u>	<u>N/A</u>
Prepaid Card - Loading & Unloading	Y	Y	<u>N/A</u>	<u>N/A</u>
e-Purse - Loading/Unloading	N/A	N/A	<u>N/A</u>	<u>N/A</u>
ADDITIONAL FEATURES				
<u>One-off</u> Payment with Increased Amount	Y	N	<u>N/A</u>	<u>N/A</u>
<u>One-off</u> Payment with Cashback	Y	N	<u>N/A</u>	<u>N/A</u>
<u>One-off</u> Payment with Purchasing or Corporate Card Data	Y	Y	<u>N/A</u>	<u>N/A</u>
<u>One-off</u> Payment with Aggregated Amount	Y	Y	<u>N/A</u>	<u>N/A</u>
<u>One-off</u> Payment with Deferred Authorisation	Y	Y	<u>N/A</u>	<u>N/A</u>
Dynamic Currency Conversion (DCC)	Y	Y	<u>N/A</u>	<u>N/A</u>
Surcharging/Rebate	Y	Y	<u>N/A</u>	<u>N/A</u>
Payment with Deferred Clearing	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Payment with Loyalty Information	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Unsolicited Available Funds	N/A	N/A	<u>N/A</u>	<u>N/A</u>
CARD MANAGEMENT SERVICES				
PIN Change / Unlock	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Card Activation	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Return Card to Cardholder Request	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Card Pick-up Advice	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Return Card Advice	N/A	N/A	<u>N/A</u>	<u>N/A</u>
ACCEPTANCE TECHNOLOGIES				
Chip with Contact	Y	N	<u>Y¹⁴</u>	<u>N</u>
Magnetic Stripe	Y	N	<u>N</u>	<u>N</u>
Chip Contactless ¹⁵	Y	N	<u>Y¹⁴</u>	<u>N</u>

¹⁴ This Acceptance Technology may only be used for EMV based ICT Transactions using EMV technology.

¹⁵ If it is not necessary to distinguish the Payment Device/Cardholder Environment in use, Chip Contactless and Mobile Contactless are referred to as Contactless Acceptance Technology, because they are both implementations of [EMV L1 CL] and communication and behaviour are the same from the perspective of the POI.

	SCS-SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
Mobile Contactless ¹⁵	Y	N	<u>Y</u> ¹⁶	<u>N</u>
Manual Entry by Acceptor ¹⁷	Y	Y ¹⁸	<u>N</u>	<u>N</u>
Manual Entry by Cardholder Customer	N	Y ¹⁹	<u>N</u>	<u>N</u>
Stored Card Account Data (stored by the Acceptor)	Y ²⁰	Y ²⁰	<u>N/A</u> ²¹	<u>N/A</u> ²¹
Consumer Device with Payment Credentials	N	Y		
Consumer Device with Payment Credentials and Authentication Application Browser over Internet	N	Y	<u>N</u>	<u>Y</u>
Consumer Device with Dedicated (M)RP Application over Internet	N	Y	<u>N</u>	<u>Y</u>
Merchant-presented QR Code	<u>N/A</u>	<u>N</u> ²²	<u>Y</u>	<u>N</u> ²²
Consumer-presented QR Code	<u>N/A</u>	<u>N</u>	<u>Y</u>	<u>N</u>
Imprint	N/A	N/A	<u>N</u>	<u>N</u>
CARDHOLDER ENVIRONMENTS PAYMENT DEVICES				
Physical Card	Y	Y	<u>Y</u> ²³	<u>N</u>
Consumer Device	Y ²⁴	Y	<u>Y</u>	<u>Y</u>
Virtual Card	N	Y	<u>N</u>	<u>N</u>

¹⁶ This Acceptance Technology is used for Local ICT Transactions only in combination with Application Selection according to [EMV B], where the selected Application is an MCP Application supporting EMV based or conventional ICT Transactions.

¹⁷ Acceptor may also stand for an Attendant in the Acceptor's environment.

¹⁸ ~~Not applicable to e- and m-commerce~~Only applicable to MOTO ~~and AIT~~.

¹⁹ For MOTO only, if a touch-tone facility on a telephone handset is supported for Telephone Orders.

²⁰ This Acceptance Technology is used for AIT. It is also referred to as Stored Card Data for Card AIT processing.

²¹ N/A because One-off Payment does not allow AIT, will be Y if ICT Transaction processing is added for Payment Services allowing AIT.

²² A Merchant-presented QR Code may be used to provide Acceptor data when using the Acceptance Technology Consumer Device with Browser over Internet. However, in this case, the Merchant-presented QR Code is not considered to be the Acceptance Technology but a means of data transfer.

²³ This Payment Device may only be used for EMV based ICT Transactions.

²⁴ Using athe Mobile Device for Mobile Contactless.

		SCS-SPS Volume Book 2 Scope			
		Card Transactions		ICT Transactions	
		Local	Remote	Local	Remote
ACCEPTANCE ENVIRONMENTS					
Physical POI					
Attended ³²⁵		Y	Y ²⁶	Y	N/A ²⁷
Unattended		Y	N	Y	N
Remote POI					
Virtual POI		N	Y ²⁸	Y	Y
Virtual Terminal		N	Y ²⁶	N	N
AUTHENTICATION METHODS (SCA factor-based classification: K = Knowledge, P = Possession, I = Inherence)					
Offline Plaintext PIN ^{29, 30}	K	Y	YN	Y ³¹	N
Offline Enciphered PIN ^{29, 32}	K	Y	YN	Y ³¹	N
Online PIN	K	Y	N	Y ³¹	N
Signature	³³	Y	N ³⁴	N	N
No CVM Required ³⁵	²⁶	Y	Y ³⁵	Y ^{31, 35}	Y ³⁵
Offline Biometric Verification ²⁹	I	Y	YN	Y ³¹	N
Biometrics via Sensor on Card	I	Y	Y ³⁶	Y ³¹	Y ^{31 36}

²⁵ According to the definition in Book 1, this Acceptance Technology also comprises Semi-Attended.

²⁶ Only for MOTO and AIT, not applicable to e- and m-commerce.

²⁷ N/A because One-off Payment does not allow AIT, will be Y if ICT Transaction processing is added for Payment Services allowing AIT; will then be applicable to AIT, but not applicable to e- and m-commerce.

²⁸ Not applicable to MOTO.

²⁹ Where this Book refers to "Offline PIN", it is referring to both Offline Plaintext PIN and Offline Enciphered PIN.

³⁰ This method has been selected for sunseting by EMVCo (refer to [EMV GB60]), but is still listed here for legacy purposes.

³¹ This Cardholder Verification Method may only be used for EMV based ICT Transactions.

³² Offline Enciphered PIN encompasses all encryption methods based on RSA or ECC cryptography for the Contact Acceptance Technology as defined in [EMV B2].

³³ Still in use for Local Card Transactions, but not an SCA factor.

³⁴ However, a mail order form contains a cardholder signature.

³⁵ The No CVM Required covers is a the verification process defined CVM by for EMV technology, else it stands for "SCA Exemption allowed", e.g. based on Risk-Based Authentication and other cases where SCACardholder Verification is not required for transactions based on EMV technology (see Section 4.3.3.5 4.3.3.7.2).

³⁶ May be used if the Biometric Card is used for authentication, interfacing via NFC to the Consumer Device that communicates with the Issuer.

		SCS-SPS Volume Book 2 Scope			
		Card Transactions		ICT Transactions	
		Local	Remote	Local	Remote
Biometrics on Consumer Device (CDCVM) ^{37 38}	<u>I</u>	Y	Y	<u>Y</u>	<u>Y</u>
Offline Mobile Code (CDCVM) ^{37 38}	<u>K</u>	Y	Y	<u>Y</u>	<u>Y</u>
Online Mobile Code	<u>K</u>	N	Y	<u>Y</u>	<u>Y</u>
Offline Personal Code (CDCVM) ^{37 38}	<u>K</u>	N	Y	<u>N</u>	<u>Y</u>
Online Personal Code	<u>K</u>	N	Y	<u>N</u>	<u>Y</u>
SDA ²⁹	<u>P</u> ³³	Y	Y <u>N</u>	<u>N</u>	<u>N</u>
DDA	<u>P</u>	Y	Y <u>N</u>	<u>N</u>	<u>N</u>
CDA	<u>P</u>	Y	Y <u>N</u>	<u>Y</u> ³¹	<u>N</u>
fDDA ³⁹	<u>P</u>	Y	N	<u>N</u>	<u>N</u>
XDA	<u>P</u>	<u>Y</u> ⁴⁰	N	<u>Y</u> ³¹	<u>N</u>
BDHLA	<u>P</u>	<u>Y</u> ³⁹	N	<u>Y</u> ³¹	<u>N</u>
EMV Online Authentication	<u>P</u>	Y	<u>Y</u> ⁴¹	<u>Y</u> ³¹	<u>Y</u> ⁴¹
Static Authentication ⁴²	<u>P</u> ⁴³	Y	Y	<u>N</u>	<u>N</u>
Dynamic Authentication - One Time Password (OTP) ⁴⁴	<u>P</u>	N	Y	<u>Y</u>	<u>Y</u>
Dynamic Authentication - Challenge Response based on Additional Authentication Device ⁴⁵	<u>P</u>	N	Y	<u>N</u>	<u>Y</u>
Dynamic Authentication - Challenge Response based on Authentication/(Remote) Payment Application on a Consumer Device ^{42 44}	<u>P</u>	N	Y	<u>Y</u> (for Mobile Device)	<u>Y</u>
FUNCTIONS					

³⁷ Biometrics on Consumer Device, Offline Mobile Code and Offline Personal Code are the types of CDCVM defined in the Volume.

³⁸ This method may be supported in authentication protocols, e.g. [FIDO].

³⁹ Only applicable to the Contactless Acceptance Technologies.

⁴⁰ Only applicable to the Contact Acceptance Technology.

⁴¹ May be used if the Card is used for authentication, interfacing via NFC to the Consumer Device that communicates with the Issuer.

⁴² Typically the Card Security Code (CSC) is used.

⁴³ Still in use for Remote Card Transactions, but not an SCA factor.

⁴⁴ This ~~Card~~-Authentication Method is used for e- and m-commerce and for conventional Local ICT Transactions and may use EMV authentication methods.

⁴⁵ This ~~Card~~-Authentication Method is used for e- and m-commerce and may use EMV or FIDO authentication methods.

	SCS-SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
Configuration	Y	Y	<u>Y</u>	<u>Y</u>
Transaction Initialisation	Y	Y	<u>Y</u>	<u>Y</u>
Language Selection	Y	Y	<u>Y</u>	<u>Y</u>
Selection of the Payment Solution Technology Selection	Y	Y ^N	<u>Y</u>	<u>Y</u>
Account Data Retrieval	Y	Y	<u>Y</u>	<u>Y</u>
Authentication Card Authentication	Y	Y ⁴⁶	<u>Y</u>	<u>Y</u>
Authorisation	Y	Y	<u>Y</u> ⁴⁷	<u>Y</u> ⁴⁶
Referral	Y	N	<u>N</u>	<u>N</u>
Completion	Y	Y	<u>Y</u>	<u>Y</u>
Reversal	Y	Y	<u>N/A</u>	<u>N/A</u>
Data Capture	Y	Y	<u>Y</u> ⁴⁸	<u>Y</u> ⁴⁷
Financial Presentment	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Settlement	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Chargeback	N/A	N/A	<u>N/A</u>	<u>N/A</u>
Selection of the Application	¥	¥		
ADMINISTRATIVE SERVICE				
Reconciliation	N/A	N/A	<u>N/A</u>	<u>N/A</u>

TABLE 4: BOOK 2 SCOPE

⁴⁶ ~~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.~~

⁴⁷ ~~Currently, for One-off Payment performed as ICT Transaction, "Authorisation" stands for the initiation of the ICT.~~

⁴⁸ ~~Currently, for One-off Payment performed as ICT Transaction, Data Capture is performed in combination with Authorisation, i.e. the initiation of the ICT.~~

Table 5 shows which Acceptance Technologies can be used ~~to retrieve Card Data from~~ combination with the ~~Cardholder Environments~~ Payment Devices.

ACCEPTANCE TECHNOLOGIES	CARDHOLDER ENVIRONMENTS <u>PAYMENT DEVICES</u>		
	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
Manual Entry by Acceptor	Y ⁴⁹	N	N
Manual Entry by <u>Customer</u> Cardholder	Y ¹⁹	Y ¹⁹	N
Stored <u>Account</u> Card Data (stored by the Acceptor) ⁵⁰	N/A	N/A	N/A
Payment Credentials on Consumer Device	N	N	Y
Consumer Device with Payment Credentials on Consumer Device with Authentication Application <u>Browser over Internet</u>	N	N	Y
Consumer Device with Dedicated (M)RP Application on Consumer Device <u>over Internet</u>	N	N	Y
<u>Merchant-presented QR Code</u>	<u>N</u>	<u>N</u>	<u>Y</u>
<u>Consumer-presented QR Code</u>	<u>N</u>	<u>N</u>	<u>Y</u>

TABLE 5: MAPPING OF ACCEPTANCE TECHNOLOGIES TO ~~CARDHOLDER ENVIRONMENTS~~ PAYMENT DEVICES

⁴⁹ If used for Local Transactions or MOTO.

⁵⁰ For the Acceptance Technology Stored Account ~~Card~~ Data, Account Data, e.g. PAN and eExpiry dDate ~~for Card Transactions~~, will have been provided earlier. Therefore no Payment Device ~~Cardholder Environment~~ is involved, which is denoted as "N/A".

3 FUNCTIONAL REQUIREMENTS FOR PAYMENT DEVICES~~CARDHOLDER ENVIRONMENTS~~

3.1 Introduction

This section defines core functional requirements for Volume conformance for ~~the~~ Payment Devices~~Cardholder Environment~~ and Payment Applications.

A Payment Device is only used in Customer Present transactions. Therefore, only Customer Present Transactions are considered in Sections 3.3 and 3.4.

3.2 Electronic Product Identification

In the Application Selection Registered Proprietary Data (ASRPD, tag '9FOA', see [EMV B] and [EMV B1]), 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 '9FOA' with ID = '0001' indicates an EEA issued card used for Card Transactions.

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

3.3 Local Customer Present Transactions

The Payment Device used for Local Customer Present Transactions, the Cardholder Environments is a Physical Card or a Consumer Device⁵¹ are used. Functional requirements for Payment DeviceCard 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 and in Section 3.3.3 for the Acceptance Technologies Merchant-presented QR Code and Consumer-presented QR Code.

3.3.1 Chip with Contact

The Payment Device used for Local Customer Present Transactions with the Acceptance Technology Chip with Contact is a Physical Card carrying a Contact EMV Card Payment Application. Local ICT Transactions for the Acceptance Technology Chip with Contact are processed using a Contact EMV Card Payment Application and EMV technology (see Figure 8 in Section 1.8 of Book 1).

The following requirements apply to Physical Cards and Contact EMV Card Payment Applications, irrespective of whether they are used for Card Transactions or ICT Transactions using EMV technology.

Req C1: The Physical Card-to-Reader communication shall be compliant with [EMV L1 CT]. The functionality (commands and data structure) implemented by Contact EMV Card Payment Applications shall comply with the relevant requirements in [EMV B1].

Req C2: Physical Cards shall support Application Selection through PSE according to [EMV B1]⁵².

Req C3: PSE and Contact EMV Card Payment 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.

Req C28: For Contact EMV Card Payment Applications used for Card Transactions, the PSE and FCI shall include the Application Selection Registered Proprietary Data.

⁵¹ Using the Mobile Device for Mobile Contactless

⁵² 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.

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

- In the Directory Discretionary data (tag '73') within every ADF Directory Entry for Contact EMV Card Payment Application used for Card Transactions,
- AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of every such ADF.

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

Contact EMV Card Payment 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: Contact EMV Card Payment Card Applications shall support EMV Online Authentication.

Req C6: The following applies for Contact EMV Card Payment Card Applications that support RSA-based Offline Data Authentication:

- DDA is optional.
- CDA is mandatory.
- SDA is not permitted.

For Contact EMV Card Payment Card Applications that support ECC-based Offline Data Authentication, XDA is ~~226~~ mandatory.

3.3.2 Chip and Mobile Contactless

The Payment Device used for Local Transactions with the Acceptance Technology Chip Contactless is a Physical Card carrying a Contactless EMV Card Payment Application. Local ICT Transactions for the Acceptance Technology Chip Contactless are processed using a Contactless EMV Card Payment Application and EMV technology (see Figure 8 in Section 1.8 of Book 1).

The Payment Device used for Local Transactions with the Acceptance Technology Mobile Contactless is a Mobile Device carrying a Mobile Contactless Payment (MCP) Application. Local ICT Transactions for the Acceptance Technology Mobile Contactless are processed either as

conventional ICT Transactions using a Mobile Contactless ICT Payment Application (see Figure 7 in Section 1.8 of Book 1) or as EMV based ICT Transactions using a Mobile Contactless EMV Card Payment Application (see Figure 8 in Section 1.8 of Book 1).

If not stated otherwise, the following requirements apply to Physical Cards, Mobile Devices and (Mobile) Contactless Payment Applications, irrespective of whether they are used for Card Transactions or ICT Transactions.

For Mobile Contactless ~~Card-Payment~~ Applications and Mobile Devices additional guidance can be found in [EPC MCP IIG] and [EPC MSCT IG].

Req C7: The Physical Card or Mobile Device-to-Reader communication shall be compliant with [EMV L1 CL].

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

Req C9: ~~The~~ (Mobile) Contactless EMV Card Payment Applications used for Card Transactions 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] for all supported (Mobile) Contactless Payment Applications, including Mobile Contactless ICT Payment Applications.

In particular, Mobile Contactless ICT Payment Applications shall be identified and selectable by an Application identifier (AID) as defined in [ISO/IEC 7816-4].

Req C11: For the management of multiple Mobile Contactless ~~Card-Payment~~ Applications, Mobile Devices shall be compliant with [EMV CMP CM] and, if applicable, with [EMV CMP SE].

Req C12: For (Mobile) Contactless EMV Card Payment Applications used for Card Transactions, the PPSE Entries and the FCI 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') for (Mobile) Contactless EMV Card Payment Applications used for Card Transactions within the FCI of the PPSE,
- AND in the FCI Issuer Directory Discretionary data (tag 'BFOC') within the FCI of every ADF of such applications.

- Req C13: Contactless EMV Card Payment Applications on Physical Cards that support Biometrics via Sensor on Card shall indicate this CVM to the POI as CDCVM.
- Req C14: ~~A Mobile Contactless~~ EMV Card Payment Applications that supports Online Mobile Code shall indicate this CVM to the POI as CDCVM.
- Req C21: For (Mobile) Contactless EMV Card Payment Applications that support ECC-based Offline Data Authentication, BDHLA is mandatory.
- Req C29: Mobile Contactless ICT Payment Applications shall support processing as shown in Figure 7 (Open Banking-based ICT Transaction - Mobile Contactless with Mobile Contactless ICT Application) in Section 1.8 of Book 1.

3.3.3 Merchant-presented QR Code and Consumer-presented QR Code

3.3.3.1 Merchant-presented QR-Code

A Payment Device supporting Local ICT Transactions based on Merchant-presented QR Codes necessarily is a Mobile Device. Local ICT Transactions based on Merchant-presented QR Code are processed as conventional ICT Transactions (see Figure 5 in Section 1.8 of Book 1).

A Mobile Device supporting Local ICT Transactions based on Merchant-presented QR Code may be personalised with one or several Mobile QR Code ICT Payment Application(s) for processing ICT Transactions. Otherwise, the built-in camera app of the Mobile Device will be used to scan Merchant-presented QR Codes.

Irrespective of whether it carries one or more Mobile QR Code ICT Payment Application(s), the Mobile Device may be personalised with one or more Mobile Authentication Application(s).

As shown in Figure 5 in Section 1.8 of Book 1, Local ICT Transactions based on Merchant-presented QR Code are initiated and completed at the Acceptor's POI, but the intermediate steps are processed like for a Remote ICT Transaction, requiring an internet connection of the Mobile Device. In particular, the requirements regarding Customer authentication for Remote ICT Transactions (Req C23, Req C24, Req C25) are also applicable for Local ICT Transactions based on Merchant-presented QR Code.

Req C30: A Mobile Device supporting Local ICT Transactions based on Merchant-presented QR Codes, shall, at a minimum, support reading and decoding Merchant-presented QR Codes complying with [ISO/IEC 18004] and to use the PISP information (URL) retrieved from the QR Code to connect to the PISP remotely.

When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), a Mobile Device supporting Local ICT Transactions based on Merchant-presented QR Codes shall support reading Merchant-presented QR Codes which comply with that standard, preferably using a Mobile QR Code ICT Payment Application which is able to interpret the standardised payload and to act on its contents.

Req C31: If a Mobile QR Code ICT Payment Application opens the camera of the Mobile Device to read a Merchant-presented QR Code then it shall temporarily disable the contactless interface of the Mobile Device.

Req C32: If a Mobile QR Code ICT Payment Application supporting multiple ICT Payment Brands is used to scan a Merchant-presented QR Code with standardised QR Code, and if more than one Brand is mutually supported, the Mobile QR Code ICT Payment Application shall offer the choice among the mutually supported ICT Payment Brands to the Customer.

3.3.3.2 Consumer-presented QR Code

For this version of the Volume, a Payment Device supporting Local ICT Transactions based on Consumer-presented QR Codes is assumed to be a Mobile Device. Other options like a static printed Consumer-presented QR Code are currently out of scope. Local ICT Transactions based on Consumer-presented QR Code are processed as conventional ICT Transactions (see Figure 6 in Section 1.8 of Book 1).

A Mobile Device supporting Local ICT Transactions based on Consumer-presented QR Code may be personalised with one or several Mobile QR Code ICT Payment Application(s). Otherwise, Consumer-presented QR Codes will be shown on the display of the Mobile Device by other means.

Irrespective of whether it carries one or more Mobile QR Code ICT Payment Application(s), the Mobile Device may be personalised with one or more Mobile Authentication Application(s).

As shown in Figure 6 in Section 1.8 of Book 1, Local ICT Transactions based on Consumer-presented QR Code are initiated and completed at the Acceptor's POI. The intermediate steps may be processed like for a Remote ICT Transaction, requiring an internet connection of the Mobile Device. In this case, the requirements regarding Customer authentication for Remote ICT Transactions (Req C23, Req C24, Req C25) are also applicable for Local ICT Transactions based on Consumer-presented QR Code.

Alternatively, Local ICT Transactions based on Consumer-presented QR Code may be processed without an internet connection of the Mobile Device. This is possible, if Customer authentication may be performed via the PISP and if the PISP has established a secure interface to the Acceptor's POI to collect the Customer data needed for authentication (e.g. an Online Personal Code and an OTP).

Req C33: A Mobile Device supporting Local ICT Transactions based on Consumer-presented QR Codes shall, at a minimum, be able to present QR Codes complying with [ISO/IEC 18004].

When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), the QR Code presented by the Mobile Device shall comply with that standard.

preferably using a Mobile QR Code ICT Payment Application to retrieve or generate the standardised QR Code to be presented.

Req C34: If a Mobile QR Code ICT Payment Application supporting multiple ICT Payment Brands is used to generate a **standard** Consumer-presented QR Code, the Payment Application shall allow the Customer to pre-select one or several of the Brands and to assign priorities to the Brands and shall generate a Consumer-presented QR Code indicating the pre-selected Brand(s) ordered according to the Customer's priorities.

Req C35: If a Mobile QR Code ICT Payment Application displays the Consumer-presented QR Code, then it shall temporarily disable the contactless interface of the Mobile Device.

3.4 Remote Customer Present Transactions

3.4.3.4.1 MOTO

In MOTO transactions, the ~~Cardholder Environment~~Payment Device Physical Card or Virtual Card is used. MOTO transactions are always Card Transactions.

Req C22: Card Data shall be derived from either a Physical or a Virtual Card and shall include a PAN, ~~e~~Expiry date and Card Security Code (CSC).

3.5.3.4.2 e- and m-Commerce

The Payment Device used for e- and m-Commerce is, Card Data may be entered on a Consumer Device, where an Electronic Device is used for e-Commerce and a Mobile device is used for m-Commerce or may be derived from data stored on a Consumer Device. The Acceptance Technologies used for e- and m-Commerce are Consumer Device with **Dedicated Application** This may include a (Mobile) Remote Payment ((M)RP) Application over Internet and Consumer Device with Browser over Internet or ~~Cardholder~~ Payment Credentials. **Remote-ICT based e- and m-Commerce t**ransactions are processed as shown in Figure 4 in Section 1.8 of Book 1). This implies, that from the Customer's perspective on a the functional steps of level, Remote-ICT based e- and m-Commerce transactions and Remote-Card based e- and m-Commerce transactions are very similar~~processed in the same way.~~

The Payment Device may be personalised In addition, the Cardholder Payment Credentials may be combined with an (M)RP Application or with an Authentication Application. Entering **Card Account** Data on the Payment 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 C23: 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 C24: A (Mobile) Remote Payment Application or an Authentication Application shall support a Dynamic Authentication ~~M~~method listed in Table 4 and categorised as a possession factor.
- Req C25: A (Mobile) Remote Payment Application or an Authentication Application shall support one of the following ~~CVMs~~Authentication Methods listed in Table 4 and categorised as knowledge or inherence factors: "~~No CVM Required~~" or "Personal/Mobile Code" (online or offline) or "Biometrics on Consumer Device".
- If an Additional Authentication Device is used with an EMV Card Authentication Application on a Physical Card, "Offline PIN" (knowledge factor) or "Offline Biometric Verification" (inherence factor) shall be supported as ~~CVM~~Authentication Methods by the EMV Card Authentication Application.
- Req C26: Whether a Physical Card, a Virtual Card, Payment Credentials, or an Authentication / (M)RP Application is involved in a the Remote Card Transaction shall be identifiable by the ~~i~~ssuer.
- Req C27: Card Data entered f~~For a Remote-Card based e- or m-Commerce t~~ransaction, Card Data entered manually by the Customer used for Manual Entry shall include PAN, ~~e~~Expiry date and Card Security Code (CSC).
- Req C36: Account Data entered for an ICT based e- or m-Commerce transaction, shall include the identity of the Customer's ASPSP and, depending on how Customer authentication is performed (see Figure 4 in Section 1.8 of Book 1), also the identity of the Customer.

4 POI FUNCTIONAL REQUIREMENTS

4.1 Introduction

This section defines accessibility requirements and 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 PaymentCard Services, Functions and Additional Features, as listed in Section 2.

Section 4.2 contains accessibility requirements that apply to all Payment Services for Local Transactions (Physical POI) and for Remote Transactions (Virtual POI, Physical POI and Virtual Terminal).

Section 4.3~~4.2~~ contains general requirements that apply to ~~all Card Services for~~ Local Transactions (Physical POI) and for ~~or for~~ Remote Transactions (Virtual POI, Physical POI and Virtual Terminal):

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

If not stated otherwise in Section 4.3, the general requirements for Local Transactions and, e- and m-Commerce transactions apply to Card Transactions for all Payment Services and to ICT Transactions for One-off Payment. General requirements for MOTO transactions and for Local and Remote AIT only apply to Card Transactions.

Section 4.3 is followed by sections detailing the specific functional requirements for each individual PaymentCard Service. The functional requirements for the individual Payment Services cover Card Transactions for all Payment Services and ICT Transactions for One-off Payment.

The sections on the individual PaymentCard Services are grouped according to Section 2 as follows:

- Basic Services (Section 4.4),
- Cash Services (Section 4.5),
- Card Enquiry Services (Section 4.6) and
- Card Electronic Transfer (Section 4.7).

These sections contain the following for Local Transactions (Physical POI) and for Remote Transactions (Virtual POI, Physical POI and Virtual Terminal):

- Allowed combinations of Acceptance Technologies and Acceptance Environments for each PaymentCard Service.
- Applicability of the Functions for each PaymentCard Service in the different Acceptance Environments.
- PaymentCard Service dependent requirements for the POI Application and for Configuration, if any.
- PaymentCard Service dependent requirements for the Functions that are applicable for processing the PaymentCard Service as appropriate.

Section 4.8 contains requirements that apply to the Additional Features. These requirements only apply to Card Transactions.

Where necessary in the following sections, it is distinguished whether requirements for Remote Transactions apply to:

- all Acceptance Environments for Remote Transactions, i.e. to Virtual POI, Physical POI and Virtual Terminal,
- only to the Acceptance Environment Virtual POI,
- only to the Acceptance Environments Physical POI and Virtual Terminal.

This distinction is mainly made due to the different ways of using the respective Acceptance Environment when the CustomerCardholder is participating in a Remote Transaction:

- A Virtual POI is used for e- or m-Commerce.
- A Physical POI or a Virtual Terminal is used for MOTO.

In the following sections, most of the requirements for Remote Transactions defined for the Acceptance Environment Virtual POI apply to e- and m-Commerce, and most of the requirements defined for the Acceptance Environments Physical POI and Virtual Terminal apply to MOTO. But for all these Acceptance Environments, each section may also contain requirements which apply to Remote AIT.

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

In requirements that are only applicable to Card Transactions, e.g. in requirements regarding MOTO or regarding Payment Services other than One-off Payment, terms like "Cardholder"

(instead of the more general term "Customer") and "Card Data" (instead of the more general term "Account Data") may still be used in this version of Book 2.

If it is not necessary to distinguish the ~~Payment Device 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 L1 CL] 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 Accessibility Requirements

It is the responsibility of each stakeholder to be aware of the requirements of the 'European Accessibility Act' [EAA] and the impact on their implementation. In particular, it is their responsibility to check the documents available, e.g. the EN 301 549 V3.2.1 (2021-03) standard of Accessibility requirements for Information and Communication Technology products and services [EN AR].

Annex I of [EAA] gives detailed information on accessibility requirements for products and services (cited here for informative purposes only):

In Section 2 (o) of the Annex I of [EAA], the following Sectors' specific requirements are provided for self-service terminals:

- "shall provide for text-to-speech technology;
- shall allow for the use of personal headsets;
- where a timed response is required, shall alert the user via more than one sensory channel;
- shall give the possibility to extend the time given;
- shall have an adequate contrast and tactilely discernible keys and controls when keys and controls are available;
- shall not require an accessibility feature to be activated in order to enable a user who needs the feature to turn it on;
- when the product uses audio or audible signals, it shall be compatible with assistive devices and technologies available at Union level, including hearing technologies such as hearing aids, telecoils, cochlear implants and assistive listening devices;"

As guidelines to help the reader in the analysis of accessibility requirements defined in the [EN AR] document, it is recommended to analyse sections 5, 8 and 11 of [EN AR] for Local Payment

Transactions with ~~Customer~~ interactions and sections 5, 9 and 11 of [EN AR] for Remote Payment Transactions with ~~Customer~~ interactions. These guidelines are in no way exhaustive but only indications to what sections of the document are likely to be applicable.

[EAA] implementation guidance is also provided in Book 6.

4.24.3 General Requirements

This section contains requirements that apply to Card Transactions for all or several ~~PaymentCard~~ Services and to ICT Transactions for One-off Payment. These requirements are grouped in requirements for the POI Application (Section 4.3.1), for the Configuration Function (Section 4.3.2) and for the Functions used for ~~PaymentCard~~ Service Processing (Section 4.3.3).

4.2.14.3.1 POI Application

The POI Application is an application consisting of software and data used to perform ~~PaymentCard~~ Services. Depending on the architecture of the POI, the POI Application may be implemented on one component or distributed on several components.

4.2.1.14.3.1.1 Local Transactions and Remote Transactions (all Acceptance Environments)

Req T1: The POI Application shall support processing with multiple ~~A~~acquirers/~~PISPs~~.

Req T2: The POI Application shall increment the Transaction Sequence Counter for each transaction.

4.2.1.24.3.1.2 Local Transactions (Physical POI)

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

- POI parameters configure the POI Application independently of the ~~PaymentCard~~ Services, e.g., define which of the supported Acceptance Technologies, Acceptance Environments, ~~PaymentCard~~ Services and Functions are available for transaction processing and which Payment Brands and Payment Instruments are supported per Acceptance Technology.
- ~~PaymentCard~~ Service parameters configure the ~~PaymentCard~~ Service, e.g., define which of the available Acceptance Technologies, Payment Brands and Payment Instruments are allowed for a ~~PaymentCard~~ Service.
- Application Profile parameters configure the Application Profile for a ~~PaymentCard~~ Service, for example:

- define the limits to be used;
- restrict functionality for accepting EEA issued cCards, e.g. CVM supported.

The Application Profile to be used for a transaction is selected based on the Payment Service to be performed and primarily on the Payment Brand selected for the transaction (see ~~The way Application Profiles are referenced is described in~~ Req T54, and T56 ~~and~~ T57.

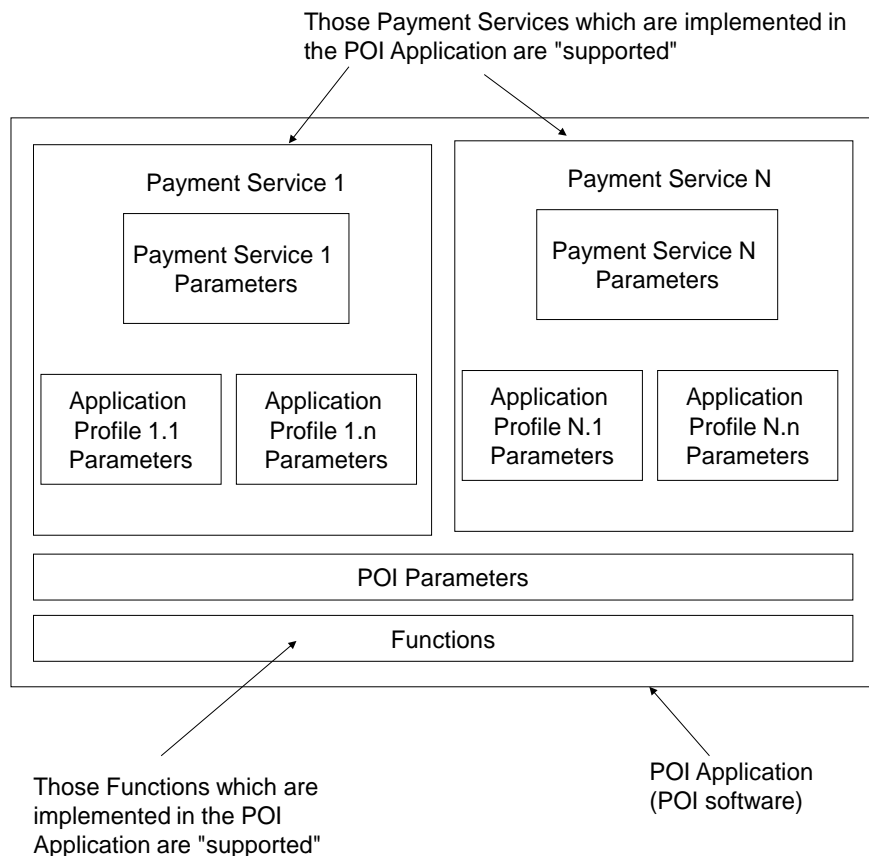


FIGURE 6: POI APPLICATION - LOGICAL STRUCTURE AND CONFIGURATION PARAMETERS

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

Req T3: The POI Application supporting the Chip with Contact Acceptance Technology for EMV based Transactions (i.e. Card Transactions and/or EMV based ICT Transactions) shall be compliant with [EMV B1] to [EMV B4] and [EMV L1 CT].

- Req T4: For the Chip with Contact Acceptance Technology, the POI Application shall support Application Selection through PSE ("Payment System Environment") according to [EMV B1].
- Req T329: The POI Application supporting the Chip with Contact Acceptance Technology for EMV based ICT Transactions shall support transaction processing according to Figure 8 in Section 1.8 of Book 1.
- Req T5: The POI Application supporting the Contactless Acceptance Technology shall support and accept any contactless form factor according to [EMV L1 CL].
- Req T6: The POI Application supporting the Contactless Acceptance Technology for EMV based Transactions (i.e. Card Transactions and/or EMV based ICT Transactions) shall support and comply with [EMV A] and [EMV B] ~~and [EMV L1 CL]~~.
- In particular, the POI Application supporting the Contactless Acceptance Technology for EMV based Transactions shall support Combination Selection through PPSE according to [EMV B] and at least one contactless kernel that complies with [EMV A] and [EMV B] to accept at least one (Mobile) Contactless EMV Card Payment Application.
- Req T330: The POI Application supporting the Contactless Acceptance Technology for EMV based ICT Transactions shall support transaction processing according to Figure 8 in Section 1.8 of Book 1.
- Req T331: The POI Application supporting the Contactless Acceptance Technology for conventional ICT Transactions shall support Combination Selection through PPSE according to [EMV B] and at least one contactless kernel performing the communication with the Payment Application on the Payment Device according to steps 2. and 3. in Figure 7 in Section 1.8 of Book 1 to accept at least one Mobile Contactless ICT Payment Application.
- Req T332: The POI Application supporting the Contactless Acceptance Technology for conventional ICT Transactions shall support transaction processing according to Figure 7 in Section 1.8 of Book 1.
- Req T333: The POI Application supporting the Contactless Acceptance Technology for both, conventional ICT Transactions and EMV based Transactions shall support Combination Selection through PPSE in a uniform way for (Mobile) Contactless EMV Card Payment Applications and for Mobile Contactless ICT Payment Applications.
- Req T334: The POI Application supporting the Merchant-presented QR Code Acceptance Technology (only for conventional ICT Transactions) shall support Selection of the Payment Brand as described in Section 4.3.3.3.2.3 and transaction processing according to Figure 5 in Section 1.8 of Book 1.

Req T335: The POI Application supporting the Consumer-presented QR Code Acceptance Technology (only for conventional ICT Transactions) shall support Selection of the Payment Brand as described in Section 4.3.3.3.2.3 and transaction processing according to Figure 6 in Section 1.8 of Book 1.

Req T7: The POI Application shall support at least a local language and English for the Customer~~cardholder~~ display. English only is allowed if English is the local language.

Req T8: The POI Application shall support updating of displayable messages for Customer~~cardholder~~ display languages.

Req T9: All POIs, attended and unattended, shall have mechanisms to ensure that only the authorised user can initiate the Payment~~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 for a Card Transaction, 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 T24).

Req T42: For attended POI, the messages for the Attendant shall be displayed in a local language.

4.2.1.34.3.1.3 Remote Transactions at the Virtual POI

For e- and m-Commerce, an ~~Card~~-Acceptor website is involved which typically includes the following components:

- The "shopping" pages;
- The checkout page, where the ~~Customer~~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 ~~Customer~~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/~~PISP~~.

The Virtual POI may also facilitate redirection services to support "direct" remote authentication of the ~~Customer~~Cardholder by the ~~Customer's ASPSP~~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 ~~Customer~~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 T336: The Virtual POI Application supporting Remote ICT Transactions shall support transaction processing according to Figure 4 in Section 1.8 of Book 1.

Req T12: All Virtual POI Applications shall support at least one method of authenticating the ~~Customer~~cardholder. Supported method(s) may be static or dynamic, and may include a redirection to the ~~Customer's ASPSP~~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 ~~Customer~~cardholder.

- Req T14: The Virtual POI Application shall use the Acceptor Name⁵³ on CustomerCardholder displays.
- Req T15: Refund, Original Credit and Cancellation Services shall be initiated by the Card Acceptor. These Payment Services shall never be initiated by the CustomerCardholder.
- Req T16: Refund, Original Credit and Cancellation Services shall have mechanisms to ensure that only the authorised user can initiate these Services.

4.2.1.44.3.1.4 Remote Card Transactions at 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.

⁵³ [Detailed guidance on the usage of Acceptor Name can be found within Book 6.](#)

- 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 T17: The Acceptor shall be able to confirm the transaction including the transaction amount to execute the transaction.

4.2.24.3.2 Configuration

Configuration is the act and result of setting the parameters for [PaymentCard](#) Services and Functions within a POI Application or MOTO Application.

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

4.2.2.14.3.2.1 Local Transactions and Remote Transactions (all Acceptance Environments)

Req T18: It shall be possible to configure the [PaymentCard](#) Services, the Application Profiles and the Functions. In particular it shall be possible to configure the POI Application to activate or deactivate specific [PaymentCard](#) Services and/or Functions.

Req T19: It shall be possible to configure which of the supported Acceptance Technologies are activated per [Payment Card](#) Service. Activation of the Contactless Acceptance Technology shall mean both, activation of Chip Contactless and Mobile Contactless.

Req T337: It shall be possible to configure which Payment Brands and Payment Instruments are supported per Payment Service and Acceptance Technology.

Req T20: 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.

4.2.2.24.3.2.2 Local Transactions (Physical POI) and Remote Transactions at the Virtual POI

Req T21: It shall be possible to configure the supported [Authentication Methods CVMs](#) per Application Profile.

4.2.2.34.3.2.3 Local Transactions (Physical POI)

Req T22: For POIs with a ~~Customer~~~~cardholder~~ display it shall be possible to configure the default language for the ~~Customer~~~~cardholder~~ display and there shall always be one language set to be the default language.

Req T338: For each Payment Brand supported for the Chip with Contact Acceptance Technology it shall be possible to configure an Application identifier (AID) as defined in [ISO/IEC 7816-4] corresponding to the Payment Brand.

Req T339: For each Payment Brand supported for the Contactless Acceptance Technology it shall be possible to configure a corresponding Application identifier (AID) as defined in [ISO/IEC 7816-4] and one or more Kernel ID(s) identifying the contactless kernel(s) that may be used for transaction processing with the respective AID.

Note that this requirement applies not only to Payment Brands which support Local EMV based Transaction processing but also to Payment Brands which support conventional Local ICT Transaction processing for the Contactless Acceptance Technology.

Req T23: As a default configuration, for Card Transactions, the Chip with Contact Acceptance Technology shall have priority over the Magnetic Stripe Acceptance Technology. However, it shall be possible to configure per ~~Payment Card~~ Service if the Chip with Contact Acceptance Technology is not required to have priority over the Magnetic Stripe Acceptance Technology.

Req T24: 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 for a Card Transaction 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 T25: It shall be configurable per Application Profile whether PIN Bypass is allowed.

- Req T26: For attended POIs that support referrals [for Card Transactions](#) it shall be configurable per Application Profile whether referrals are activated.
- Req T27: It shall be configurable per transaction result (approved, declined or aborted) and per [PaymentCard](#) Service whether a [Customercardholder](#) receipt shall be printed or delivered electronically, either never, always or on request.⁵⁴
- Req T28: Data identifying an unattended POI used for the purposes of paying a transport fare or parking fees shall be configurable per Application Profile.

4.2.2.4.3.2.4 Remote [Card](#) Transactions at Physical POI and Virtual Terminal

- Req T29: It shall be configurable per transaction result (approved, declined or aborted) and per [PaymentCard](#) Service, whether a [Cardholder](#) receipt shall be printed or delivered electronically either never, always or on request.

4.2.3.3.3 Functions for [PaymentCard](#) Service Processing

The following sections contain the Function specific requirements which are not only applicable to an individual [PaymentCard](#) Service but to all or to several [PaymentCard](#) Services [for Card Transactions and to One-off-Payment for ICT Transactions](#).

4.2.3.1.4.3.3.1 Transaction Initialisation

Transaction Initialisation is the Function which allows selection of the [PaymentCard](#) Service for the next transaction and where the transaction amount is set, transaction data is initialised and processing of the [PaymentCard](#) Service is started.

4.2.3.1.1.4.3.3.1.1 Local Transactions (Physical POI)

- Req T30: The attendant, [Customercardholder](#) or sale system shall be able to select the required [PaymentCard](#) Service from the list of [PaymentCard](#) Services that are activated. If [PaymentCard](#) Service selection is not performed, then the default [PaymentCard](#) Service is the selected [PaymentCard](#) Service.
- Req T31: For [Transaction](#) [Initialisation](#) the [Customercardholder](#) display shall always display a message, called Welcome Message, to the [Customercardholder](#), the contents of which will depend on the selected [PaymentCard](#) Service.

⁵⁴ If there is a legal requirement to print a receipt, the POI shall be configured to do so.

- Req T32: 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 T33: 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 T34: 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 T35: 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~~Customer that a receipt cannot be printed and offer the choice to continue or abort the transaction.

~~4.2.3.1.24.3.3.1.2~~ Remote Transactions at the (Virtual POI)

- Req T36: If more than one ~~PaymentCard~~ Service is available for the transaction, the ~~cardholder~~Customer shall be able to select the ~~PaymentCard~~ Service from the list of ~~PaymentCard~~ Services that are available. If only one ~~PaymentCard~~ Service is available, this ~~PaymentCard~~ Service shall be selected by default.

~~4.2.3.1.34.3.3.1.3~~ Remote ~~Card~~ Transactions at Physical POI and Virtual Terminal

- Req T37: All transactions shall be initiated by the ~~Card~~-Acceptor only.

Requirements T30, T31, T32 and T33 defined above for Physical POIs also apply for MOTO, albeit it is the Acceptor that is interfacing with the POI.

- Req T38: The default Service on a Virtual Terminal shall be the One-off Payment.

~~4.2.3.24.3.3.2~~ Language Selection

Language Selection is the Function which allows selecting one of the languages supported by the POI for the ~~Customer~~cardholder display.

Language Selection is only performed for Customer Present Transactions.

4.2.3.2.14.3.3.2.1 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~~Customer the option to select one of the languages supported by the POI.

POI based Language Selection is applicable for all Local Transactions and for all Acceptance Technologies supported by a Physical POI.

For the Card based Language Selection, the POI automatically selects one of the supported languages, without ~~cardholder~~Customer or Attendant interaction, by retrieving and evaluating the card data element Language Preference.

Card based Language Selection is only applicable for EMV based Local Transactions processed with the Chip with Contact Acceptance Technology or the Contactless Acceptance Technology~~y~~.

Req T39: 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 T40 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~~Customer the option to override the default language for the ~~cardholder~~Customer display (see Req T22) and to select one of the languages supported by the POI for the ~~cardholder~~Customer 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 T41: If all of the following are true:

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

then the selection of the language for the ~~cardholder~~Customer 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.

Note:

For the Contactless Acceptance Technology, if a display shall be shown to the ~~cardholder~~Customer in the context of [IFR] according to Req T53 before the card data element Language Preference can be retrieved regularly, then a specific process may be applied as described in ~~Book 6~~Section 2.3 of Book 6 to retrieve the card data element Language Preference.

~~Req T42: For attended POI, the messages for the attendant shall be displayed in a local language.~~

~~4.2.3.2.24.3.3.2.2~~ Remote Transactions at the Virtual POI

Req T43: If the language selected on the ~~Acceptormerchant~~'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 T44: If the language selected on the ~~Acceptormerchant~~'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.

~~4.2.3.2.34.3.3.2.3~~ Remote Card Transactions at Physical POI and Virtual Terminal

Language Selection is not performed for MOTO

4.3.3.3 Selection of the Payment Solution and of the Application Profile

Selection of the Payment Solution is the Function which allows for the selection of the combination of Payment Instrument (Payment Card or Instant Credit Transfer, abbreviated as

ICT), Acceptance Technology (e.g., Contactless, QR Code) and Payment Brand to be used for transaction processing.

Therefore, this Function may be considered as consisting of three (Sub-)Functions, processed in any order:

- Selection of the Payment Instrument,
- Selection of the Acceptance Technology (also called Technology Selection),
- Selection of the Payment Brand.

Selection of the Application Profile is the Function which allows for the selection of the Application Profile containing Payment Solution specific configuration data to be used for transaction processing.

For Customer Present transactions, the selection of the Payment Solution results from interactions - verbal or not - between Customer and Acceptor where the starting points are

- The range of Payment Instruments and Payment Brands accepted by the Acceptor,
- The range of Payment Instruments and Payment Brands supported by the Payment Device of the Customer,

while taking into account the mutually supported Acceptance Technologies between Payment Device of the Customer and POI of the Acceptor, where each Acceptance Technology may support one or several Payment Brands for Card and/or ICT based Payment Instruments.

Several ways of selecting the final Payment Solution exist. These may vary depending on whether the transaction is a Local Transaction or a Remote Transaction, and, for Local Transactions, whether the POI is attended or unattended, whether the Acceptor is a large merchant and queues may form, whether language barriers may be a factor (for example in tourist areas), etc.

For example, the Customer may be asked to make consecutive decisions to select the Payment Instrument ("Payment Card, or Instant Credit Transfer") and/or the Acceptance Technology ("contact, contactless, QR Code") and/or the Payment Brand in any order.

For Local Transactions at an attended POI, this may be triggered by verbal questions of the Attendant. In other environments, this may be prompted by showing on the screen the available options. Alternatively, for Local Transactions, an Acceptor could avoid verbal interactions with the Customer by opening on the POI all the supported Acceptance Technologies in parallel for the Customer to choose, allowing for technical processes on POI and/or Consumer Device to select the final Payment Solution.

Each selection made, may reduce the options for the subsequent selection step. In particular, since a Payment Brand is either a Card based Payment Brand or an ICT based Payment Brand, but never both, Selection of the Payment Brand is an implicit Selection of the Payment Instrument.

Requirements for the Selection of the Payment Brand for Card Transactions contained in the IF Regulation IFR 715/2015 ([IFR]) together with derived requirements for the POI, partly extended to ICT Transactions, are listed in Section 4.3.3.3.1.

POI requirements regarding Selection of the Payment Solution are contained in

- Section 4.3.3.3.2 for Local Card and ICT Transactions (always at the Physical POI).
- Section 4.3.3.3.3 for Remote Card and ICT Transactions at the Virtual POI.
- Section 4.3.3.3.4 for Remote Card Transactions at Physical POI and Virtual Terminal

Some examples of selection flows can be found in Book 6.

POI requirements regarding Selection of the Application Profile are contained in Section 4.3.3.3.5.

4.2.3.2.4.3.3.1 IF Regulation Article 8.6 and Article 10.5 Requirements for Selection of the Payment Brand

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

4.2.3.2.4.14.3.3.1.1 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.

4.2.3.2.4.24.3.3.1.2 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 ~~P~~ayment ~~B~~rand or ~~P~~ayment ~~A~~pplication (including overriding) occurs when there are multiple mutually supported ~~Payment B~~brands or ~~P~~ayment ~~A~~pplications in the ~~CustomerCardholder's P~~ayment ~~Device~~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 IFR Req T2 - IFR Req T5 shall be met. For the purposes of this Volume, requirements IFR Req T2 and IFR Req T3 are extended to also cover ICT Transactions. Requirements IFR Req T4 and IFR Req T5 only cover Card Transactions.

IFR Req T2: The option to have a priority selection of a particular ~~P~~ayment ~~B~~rand or ~~P~~ayment ~~A~~pplication by the Acceptor shall only be allowed if the priority ~~P~~ayment ~~B~~rand or ~~P~~ayment ~~A~~pplication is displayed to the ~~CustomerCardholder~~ and the ~~CustomerCardholder~~ 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 ~~CustomerCardholder~~ to override a priority selection (e.g., Environment with no screen and /or no Pin/touch/key Pad ...).
- The priority ~~P~~ayment ~~B~~rand or ~~P~~ayment ~~A~~pplication shall be displayed on the POI or at the POS, e.g. together with the accepted ~~P~~ayment ~~B~~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 CustomerCardholder can be achieved through various mechanisms. It may include early CustomerCardholder 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 CustomerCardholder shall be informed of their ability to override the Acceptor's priority selection and how to override it so that the CustomerCardholder 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 Card T 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 Card T transactions, ~~a the Card resident~~ data element, [EMV] tag '9FOA' with ID = '0001' (see Section 3.2), shall be used as the target solution. If this data element is not available, solutions based on BIN tables may be used.
- For Remote Card T 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.

4.2.3.2.54.3.3.2 Selection of the Payment Solution for Local Transactions (Physical POI)

4.3.3.3.2.1 Selection of the Payment Instrument

For Local Customer Present Transactions, Selection of the Payment Instrument is a Function, which allows selection of one of the Payment Instruments, Card or ICT, in several ways:

- If a Physical POI supports only one of the Payment Instruments (Card or ICT), then Selection of the Payment Instrument is the first step of Selection of the Payment Solution, implicitly performed by the Customer by using this POI.
- If a Physical POI supports both Payment Instruments, then:
 - Selection of the Payment Instrument may be the first step of Selection of the Payment Solution. In this case, Selection of the Payment Solution has to be performed explicitly.
 - Selection of the Payment Instrument may be a subsequent step of the Selection of the Payment Solution. In this case, Selection of the Payment Solution is always performed implicitly:
 - If Selection of the Payment Brand is the first step of the Selection of the Payment Solution, then the Payment Instrument is selected implicitly since a specific Payment Brand is either Card based or ICT based.
 - If Technology Selection is the first step of the Selection of the Payment Solution, then:
 - Selecting Chip with Contact, Chip Contactless or Mobile Contactless will lead to Application Selection or Combination Selection, selecting an AID and the corresponding Payment Brand and therefore implicitly selecting the Payment Instrument,
 - Selecting a QR Code based Acceptance Technology implicitly selects ICT as Payment Instrument since QR Code is only supported for ICT,
 - Selecting Magnetic Stripe or Manual Entry by Acceptor implicitly selects Card as Payment Instrument since these Acceptance Technologies are only supported for Card.

Req T340: Explicit Selection of the Payment Instrument shall only be performed at a POI that supports both Payment Instruments, Card and ICT, and only if both Payment Instruments are supported for the Service to be performed.

Req T341: If explicit Selection of the Payment Instrument is performed, it shall be performed as first step of the Selection of the Payment Solution.

If Technology Selection or Selection of the Payment Brand is performed as first step of the Selection of the Payment Solution, then explicit Selection of the Payment Instrument shall not be performed, and the Payment Instrument shall be selected implicitly as described in Sections 4.3.3.3.2.2 and 4.3.3.3.2.3.

Req T342: If Selection of the Payment Instrument is the first step of Selection of the Payment Solution, then both Payment Instruments shall be offered to the Customer to be chosen from, either by a verbal communication with the Attendant at an attended POI or by making a selection from a menu shown on the display of the attended or unattended POI.

In this version of Book 2, Local AITs are always Card Transactions. Therefore, Selection of Card as Payment Instrument is implicitly performed for Local AITs.

4.2.3.2.5.14.3.3.2.2 Technology Selection

For Local Customer Present Transactions, 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 (Card and ICT Transactions),
- Contactless (Card and ICT Transactions),
- Magnetic Stripe (Card Transactions), or
- Manual Entry by Acceptor (Card Transactions),
- Merchant-presented QR Code (ICT Transactions),
- Consumer-presented QR Code (ICT Transactions).

For Local AITs, Technology Selection is implicitly performed since Local AITs are always processed based on Stored Account Data.

Req T45: For if a Local AIT transaction is processed based on Stored Card Data, Stored Account Data shall be used as Acceptance Technology without performing Technology Selection shall not be performed.

Req T46: Technology Selection shall be based on the configuration of the Payment Card Service to be performed i.e., which Acceptance Technologies are activated for the Service, which Payment Brand(s) and Payment Instrument(s) are supported per Payment Service and Acceptance Technology, and, for Card as Payment

Instrument, whether Chip with Contact has priority over Magnetic Stripe for this Service (see Reqs T19 and T23).

Req T343: If Technology Selection is the first step of the Selection of the Payment Solution, then all Acceptance Technologies activated for the Service to be performed shall be available in parallel for the Customer to choose for Technology Selection ("open-to-all" scenario in Book 6).

Req T344: If Selection of the Payment Instrument is performed before Technology Selection, then only the Acceptance Technologies which are activated for the Payment Service to be performed and for which the selected Payment Instrument is supported shall be available for the Customer to choose for Technology Selection.

Req T345: If Selection of the Payment Brand is performed before Technology Selection, then only the Acceptance Technologies which are activated for the Payment Service to be performed and for which the selected Payment Brand is supported shall be available for the Customer to choose for Technology Selection.

Req T346: A POI supporting Merchant-presented QR Code as Acceptance Technology shall, at a minimum, be able to present QR Codes complying with [ISO/IEC 18004] and providing the PISP information (URL) needed to connect to the PISP remotely.

When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), the QR Code presented by the POI shall comply with that standard.

Req T347: If the POI supports one or more ICT Payment Brand(s) based on the standard Merchant-presented QR Code, then, for Technology Selection, the POI shall present a standard Merchant-presented QR Code indicating in the standardised payload all available Payment Brand(s), which, if several Payment Brands are available, may be ordered according to the Acceptor's priorities.

Req T348: A POI supporting Consumer-presented QR Code as Acceptance Technology shall, at a minimum, be able to read and decode QR Codes complying with [ISO/IEC 18004].

When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), the POI shall support reading Consumer-presented QR Codes which comply with that standard and shall be able to interpret the standardised payload and to act on its contents. In particular, the POI shall be able to decode which Payment Brand(s) are indicated as supported in the QR Code.

Req T349: The POI shall be able to detect, which of the Acceptance Technologies made available for the Customer is selected by the Customer.

For the Merchant-presented QR Code Acceptance Technology, this may require that Customer or Attendant enter on the POI an additional selection or confirmation of this Acceptance Technology.

- Req T47: 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 T48: 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, [implicitly selecting Card as Payment Instrument](#),
 - 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 [and the Payment Instrument Card is supported for this Acceptance Technology](#) (see Req T19 [and Req T337](#)),
 - and the Chip with Contact Acceptance Technology is configured to have priority (see Req T23).
- Req T49: 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 T50: 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 T51: If a Physical Card is inserted in the chip reader, [and if the Payment Instrument Card is activated for the Chip with Contact Acceptance Technology, and if the Payment Instrument ICT is not activated for the Chip with Contact Acceptance Technology or has not \(yet\) been selected](#), 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 T24.

4.2.3.2.5.24.3.3.2.3 Selection of the Payment BrandApplication

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.~~

For Local Customer Present Transactions, Selection of the Payment Brand is a Function which allows the selection of a Payment Brand in several ways according to the following requirements:

Req T350: The Acceptor shall display to the Customer the accepted Payment Brands in a clear way.

Req T351: If Selection of the Payment Brand is performed before Technology Selection, Selection of the Payment Brand shall be performed explicitly, either by a verbal communication with the Attendant at an attended POI or by making a selection from a menu shown on the display of the attended or unattended POI. In addition, only the Acceptance Technologies for which the selected Payment Brand is supported shall available for Technology Selection (see Req T345).

Req T352: If Technology Selection is performed before Selection of the Payment Brand, and if the Acceptance Technology Chip with Contact is selected, then:

- Application Selection according to [EMV B1] shall be performed, resulting in selection of an AID supported by both the Payment Device and the POI,
- And the Payment Brand corresponding the selected AID (see Req T338) shall implicitly be selected.

Req T353: If Technology Selection is performed before Selection of the Payment Brand, and if the Contactless Acceptance Technology is selected, then:

- Combination Selection according to [EMV B] shall be performed, resulting in selection of a Combination of AID and Kernel ID supported by both the Payment Device and the POI,
- And the Payment Brand corresponding the selected AID (see Req T339) shall implicitly be selected.

Req T354: If Technology Selection is performed before Selection of the Payment Brand, and if the Merchant-presented QR Code Acceptance Technology is selected, then:

- The Selection of the Payment Brand shall be performed by the Customer, selecting a Payment Brand from a list on the PISP website according to Reg T55,
- Or Selection of the Payment Brand shall be performed by the Customer on their Payment Device, selecting one of the Payment Brand(s) mutually supported by POI and Mobile QR Code ICT Application on the Payment Device, if the QR Code is a standard QR Code indicating in the standardised payload the ICT based Payment Brands supported by the POI for the Payment Service to be performed and if the QR Code is read through a Mobile QR Code ICT Application on the Payment Device supporting such a selection and communicating its result to the PISP.

Req T355: If Technology Selection is performed before Selection of the Payment Brand, and if the Consumer-presented QR Code Acceptance Technology is selected, then:

- The Selection of the Payment Brand shall be performed by the Customer on the POI where the selection is made from all ICT based Payment Brands supported by the POI,
- Or Selection of the Payment Brand shall be performed by the Customer on the POI, selecting one of the ICT based Payment Brand(s) mutually supported by POI and the Payment Device, if the QR Code is a standard QR Code indicating in the standardised payload more than one ICT based Payment Brands supported by the Payment Device and if the standard QR Code is interpreted by the POI to identify the Payment Brand(s) supported by Payment Device and POI.

Req T356: If Technology Selection is performed after Selection of the Payment Brand, and if one of the Acceptance Technologies Chip with Contact or Contactless is selected, then Application Selection (Chip with Contact) or Combination Selection (Contactless) shall be performed after Technology Selection:

- To determine whether the AID corresponding to the selected Payment Brand is supported by the Payment Device,
- And to select the Payment Application on the Payment Device with the AID corresponding to the selected Payment Brand.

Req T52: For Selection of the Payment BrandApplication 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 and Contact EMV Card

Payment Applications used for ICT Transactions, in line with the IFR Requirements in Section 4.3.3.3.1.2:

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 Customercardholder 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 CustomerCardholder 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 CustomerCardholder choice. The POI display ergonomics shall be designed such that the CustomerCardholder is able to choose from the mutually supported applications in a convenient way.

- The Acceptor may put their prioritised application on top.
- Once the CustomerCardholder decides which application to be used for that specific transaction, the Acceptor shall not override that decision.

4. The CustomerCardholder 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 CustomerCardholder 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 Customercardholder preference mechanism.

If the CardholderCustomer 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 T53: For Selection of the [Payment Brand Application](#) for the Contactless Acceptance Technology, Combination Selection shall follow [EMV B].

For EEA issued cards, [for Contactless EMV Card Payment Applications used for ICT Transactions and for Mobile Contactless ICT Payment Applications the following rules apply:](#)

- ~~The~~ the following modifications are allowed for building the list of mutually supported combinations described in [EMV B]:
 - If the POI successfully reads [EMV] tag '9FOA' 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~~ the following modification applies for [EMV B] Final Combination Selection: If the list of mutually supported combinations contains only one application and the [Customer](#)~~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~~[Customer](#) shall have the means to select the application of their choice. If the ~~Cardholder~~[Customer](#) makes a choice, then the chosen application shall be used in Final Combination Selection.
 - If the ~~Cardholder~~[Customer](#) 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~~[Customer](#) 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~~.

Reg T357: For Selection of the Payment Brand for the Consumer-Presented QR Code Acceptance Technology the following rules apply:

- When building the list of (mutually supported) Payment Brands, the Acceptor may put their prioritised Payment Brand on top.
- If the list of (mutually supported) Payment Brands contains only one entry and the Customer has expressed the wish to make a choice, then this single Payment Brand shall be shown to the Customer for confirmation.
- If the list of (mutually supported) Payment Brands contains more than one entries, then:
 - The Customer shall have the means to select the Payment Brand of their choice. If the Customer makes a choice, then the chosen Payment Brand shall be used for the transaction.
 - If the Customer does not wish to make a choice, or if it is not technically feasible to allow the Customer to select the Payment Brand of their choice (e.g., Environment with no screen and /or no Pin/touch/key Pad ...), then the Payment Brand on top of the list of (mutually supported) Payment Brands shall be selected and used for the transaction.

For Local AITs, the Acceptor has to store the Payment Brand to be used together with the Account Data to be used. Therefore, selection of the Payment Brand for a Local AIT is performed according to the following requirement:

Reg T358: For processing a Local AIT, the Acceptor shall select and use the Payment Brand stored together with the Account Data to be used for the Local AIT.

4.2.3.2.64.3.3.3 Selection of the Payment Solution for Remote Transactions at the 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 Customercardholder) or automatically (without Customercardholder 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.~~

4.3.3.3.1 Selection of the Payment Instrument

For Remote Customer Present Transactions, i.e. for e- and m-Commerce transactions, Selection of the Payment Instrument is a Function, which allows selection of one of the Payment Instruments, Card or ICT as follows:

- If a Virtual POI supports only one of the Payment Instruments (Card or ICT), then Selection of the Payment Instrument is the first step of Selection of the Payment Solution, implicitly performed by the Customer by using this POI.
- If a Virtual POI supports both Payment Instruments, then:
 - Selection of the Payment Instrument may be the first step of Selection of the Payment Solution. In this case, Selection of the Payment Solution has to be performed explicitly.
 - If Selection of the Payment Brand is the first step of the Selection of the Payment Solution, then the Payment Instrument is selected implicitly since a specific Payment Brand is either Card based or ICT based.

Req T359: Explicit Selection of the Payment Instrument shall only be performed at a Virtual POI that supports both Payment Instruments, Card and ICT, and only if both Payment Instruments are supported for the Service to be performed.

Req T360: If explicit Selection of the Payment Instrument is performed, it shall be performed as first step of the Selection of the Payment Solution.

If Selection of the Payment Brand is performed without performing explicit Selection of the Payment Instrument before, then explicit Selection of the Payment Instrument shall not be performed, and the Payment Instrument shall be selected implicitly as described in Section 4.3.3.3.3.

Req T361: If Selection of the Payment Instrument is the first step of Selection of the Payment Solution, then both Payment Instruments shall be offered to the Customer to be chosen from a menu displayed to the Customer.

In this version of Book 2, Remote AITs are always Card Transactions. Therefore, Selection of Card as Payment Instrument is implicitly performed for Remote AITs.

4.3.3.3.2 Technology Selection

For Remote Customer Present Transactions, i.e. for e- and m-Commerce transactions, Technology Selection is implicitly performed by the Customer when choosing on their Consumer Device a browser or a dedicated application for the access over the internet.

For Remote AITs, Technology Selection is implicitly performed since Remote AITs are always processed based on Stored Account Data.

4.3.3.3.3 Selection of the Payment Brand

For Remote Customer Present Transactions, Selection of the Payment Brand is a Function which allows the selection of a Payment Brand according to the following requirement:

Req T55: The Payment Brands⁵⁵ and, for Card based Payment Brands, Product Types accepted by the Acceptor for the transaction shall be displayed so the CardholderCustomer can choose the Payment Brandapplication to be used to perform the transaction. The Acceptor may determine the method and the order in which the Payment Brands and, for Card based Payment Brands, Product Types are displayed to the CardholderCustomer. If not all Payment Brands and Product Types are displayed at once for selection, the Acceptor shall inform the CardholderCustomer how to select the other supported Payment Brands and Product Types.

For Remote AITs, the Acceptor has to store the Payment Brand to be used together with the Account Data to be used. Therefore, selection of the Payment Brand for a Remote AIT is performed according to the following requirement:

Req T362: For processing a Remote AIT, the Acceptor shall select and use the Payment Brand stored together with the Account Data to be used for the Remote AIT.

4.2.3.2.74.3.3.3.4 Selection of the Payment Solution for Remote Card Transactions at Physical POI and Virtual Terminal

In this version of Book 2, MOTO transactions are always Card Transactions. Therefore, Selection of Card as Payment Instrument is implicitly performed for MOTO transactions.

For MOTO transactions, the Acceptance Technology is implicitly selected. It is determined by the process used for MOTO, whether the Acceptance Technology is Manual Entry by the Acceptor or Manual Entry by the Customer.

⁵⁵ The Click to Pay Icon may be used in this context.

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

Req T363: The POI shall select the Payment Brand based on the PAN that is manually entered for the MOTO transaction.

4.3.3.3.5 Selection of the Application Profile

Req T54: For Local Customer Present Transactions, The Application Profile shall be selected for a transaction based on the Payment Card Service to be performed and primarily on the following:

- The selected AID for a Card or ICT Transaction if the Chip with Contact Acceptance Technology is used,
- The selected Combination for a Card or ICT Transaction if a the Contactless Acceptance Technology is used,
- The PAN for a Card Transaction if the Magnetic Stripe, Manual Entry or Stored Card Data Acceptance Technology is used,
- The selected Payment Brand for an ICT Transaction if the Merchant-presented QR Code or Consumer-presented QR Code Acceptance Technology is used.

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

Req T56: For Remote Transactions, ~~t~~The Application Profile shall be selected for a transaction based on the Payment Card Service to be performed and on the selected Payment Brand. In addition, for a Card based Payment Brand, the Application Profile may be selected based on the Product Type.

~~Req T57: 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.~~

4.2.3.3.4 Account ~~Card~~ Data Retrieval

Account ~~Card~~ Data Retrieval is the Function which allows retrieval of the ~~Card~~ Data identifying the Customer's account to be used for the transaction. The method to retrieve this data depends on to be retrieved according to the Acceptance Technology.

For Card Transactions, this Function is used to retrieve Card Data.

4.2.3.3.14.3.3.4.1 Local Transactions and Remote Transactions (all Acceptance Environments)

Req T58: For Card Transactions, aAll authorisation and completion messages shall identify the method~~Acceptance Technology~~ used to retrieve Card Data.

4.2.3.3.24.3.3.4.2 Local Transactions (Physical POI)

Req T59: For Local Customer Present Card Transactions at a Physical POI, the Acceptance Technology shall be Chip with Contact, Chip Contactless, Mobile Contactless, Magnetic Stripe, or~~and~~ Manual Entry by Acceptor.

For Local Customer Present ICT Transactions at a Physical POI, the Acceptance Technology shall be Chip with Contact, Chip Contactless, Mobile Contactless, Merchant-presented QR Code or Consumer-presented QR Code.

For EMV based Local Card or ICT Transactions using Acceptance Technology Chip with Contact, Chip Contactless, or Mobile Contactless, and for Local Card Transactions using Acceptance Technology Magnetic Stripe or Manual Entry by Acceptor, Account Data to be retrieved is Card Data, i.e. PAN and expiry date. Depending on the Acceptance Technology, Card Data shall be read by the Physical POI Application from the EMV Card Payment Application selected for the transaction or from the magnetic stripe of the Card used for the transaction, or Card Data shall be entered to the POI by the Acceptor.

For conventional ICT Transactions using Acceptance Technology Mobile Contactless, Account Data consisting of Customer's ASPSP identification and Customer identification, shall be retrieved by the Physical POI Application from the Mobile Contactless ICT Payment Application selected for the transaction (see step 3. in Figure 7 in Section 1.8 of Book 1).

For conventional ICT Transactions using Acceptance Technology Merchant-Presented QR Code, Account Data is not retrieved by the Physical POI Application, but by the PISP (see step 3. in Figure 5 in Section 1.8 of Book 1).

For conventional ICT Transactions using Acceptance Technology Consumer-presented QR Code, Account Data consisting of the Customer's ASPSP

identification and, if not entered or retrieved later during the transaction, of the Customer identification, shall be retrieved by the Physical POI Application from the Consumer -presented QR Code (see step 2. in Figure 6 in Section 1.8 of Book 1).

read by the Physical POI Application from the EMV Card Payment Application selected for the transaction or from the magnetic stripe of the Card used for the transaction, or Card Data shall be entered to the POI by the Acceptor.

For Local AIT at a Physical POI, the Acceptance Technology shall be ~~or~~ Stored AccountCard Data.

Req T60: When Manual Entry by Acceptor is supported, the Physical POI Application shall facilitate entering the PAN, the eExpiry date and, when appropriate, the Card Security Code.

4.2.3.3.4.3 *Remote Transactions at the Virtual POI*

Req T61: 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 Browser over InternetAuthentication Application, or (M)RP Application on Consumer Device with Dedicated Application over Internet~~or Stored Card Data~~.

For any of these Acceptance Technologies~~Therefore,~~ the Virtual POI shall display a payment page to the CustomerCardholder.

For Remote-Card based e- and m-Commerce t~~r~~ansactions, t~~t~~his page shall facilitate for the Customer either the entry or retrieval of the PAN, the eExpiry date, and the Card Security Code or the retrieval of s~~s~~Stored PAN and expiry date~~Card Data~~⁵⁶, 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.

For Remote-ICT based e- and m-commerce t~~t~~ransactions, this page shall facilitate for the Customer the entry or retrieval of the Customer's ASPSP identification and, if not entered or retrieved later during the transaction, of the Customer identification (see step 3. in Figure 4 in Section 1.8 of Book 1).

For Remote AIT at the Virtual POI, the Acceptance Technology shall be Stored Account Data.

⁵⁶ SRC may be offered in this context to retrieve Card Data, previously stored in a secure way.

4.2.3.3.44.3.3.4.4 Remote Card Transactions at Physical POI and Virtual Terminal

Req T62: For MOTO transactions, the Acceptance Technology shall be Manual Entry by AcceptorAttendant or Manual Entry by Customer.~~or For Remote AIT at Physical POI and Virtual Terminal, the Acceptance Technology shall be~~ Stored Card Data.

For MOTO transactions, tThe 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 eExpiry 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 T63: The MOTO Application shall also support the entry and transmission of Address Data if address validation is supported.

4.3.3.5 Authentication

Authentication is the Function to perform Strong Customer Authentication (SCA) according to [PSD2] and the [RTS SCA/CSC], including the decision whether any exemption applies.

Authentication is only applicable for Customer Present Transactions.

4.3.3.5.1 EMV Based Local Transactions (Physical POI)

For EMV based Local Transactions, Authentication consists of two sub-functions: Card Authentication, and Cardholder Verification as defined by EMV.

4.2.3.3.4.14.3.3.5.1.1 Card Authentication

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

Card Authentication for EMV based Local Transactions using a Contactless Acceptance Technology may contain additional steps to detect relay attacks. These mechanisms are specific to each contactless EMV Kernel⁵⁷ and are out of scope of this document.

Req T64: Online-only POI Applications are not required to support Offline Data Authentication.

Req T65: The following applies for POI Applications supporting the Chip with Contact Acceptance Technology and RSA-based Offline Data Authentication:

- DDA is mandatory.
- CDA is mandatory.
- SDA is no longer supported.

For POI Applications supporting the Chip with Contact Acceptance Technology and ECC-based Offline Data Authentication, XDA is mandatory.

For POI Applications supporting Chip and Mobile Contactless, the Offline Data Authentication methods shall be supported as defined in the respective kernel specifications (in particular BDHLA, when supporting Kernel 8 [EMV C8]).

4.2.3.3.4.24.3.3.5.1.2 Cardholder Verification

~~On the Physical POI,~~ Cardholder Verification is a the Function for EMV based Local Transactions defined by EMV by which a Cardholder Verification Method (CVM) is selected and performed. ~~Cardholder is not present, Cardholder Verification is not applicable.~~

⁵⁷ E.g. Relay Resistance Protocol in [EMV C8].

The CVMs to be used are listed in Table 4. 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 Biometric Verification, if the Acceptance Technology is Chip with Contact,
- Biometrics via Sensor on Card, if the Acceptance Technology is Chip Contactless,

Note that Biometrics via Sensor on Card may also be used with the Acceptance Technology Chip with Contact,

- CDCVM, i.e. Offline Mobile Code or Biometrics on Consumer Device⁵⁸, 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.

4.2.3.3.4.2.14.3.3.5.1.2.1 General Requirements for Cardholder Verification

Req T69: All Physical POI shall have a PIN Entry Device; with the exception of environments where the interaction with the Customer~~Cardholder~~ must be minimized for Customer~~Cardholder~~ or Acceptor convenience (e.g., low value payments, transaction speed, highway tolls). The Physical POI may in addition have a Biometric Capture Device.

Req T70: For POIs that have a PIN Entry Device, the POI Application shall be able to support PIN as CVM.

⁵⁸

A POI that supports CDCVM implicitly supports Biometrics via Sensor on Card and Online Mobile Code (see Req C13 and Req C14).

Req T71: The POI Application shall offer PIN Bypass to the ~~Customer~~**Cardholder** if PIN entry is requested and PIN Bypass is allowed according to the Application Profile (see Req T25).

4.2.3.3.4.2.24.3.3.5.1.2.2 *Cardholder Verification for the Chip with Contact Acceptance Technology*

Req T72: 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, No CVM Required and Offline Biometric Verification, 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 and Offline Biometric Verification.
 - ATMs shall not support No CVM Required, Signature CVM or Combined CVM containing Signature.

~~4.2.3.3.4.2.3~~4.3.3.5.1.2.3 *Cardholder Verification for the Contactless Acceptance Technology*

Req T73: POIs supporting the Contactless Acceptance Technology shall support

- Online PIN
- Signature
- No CVM Required
- CDCVM

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

~~4.2.3.3.4.2.4~~4.3.3.5.1.2.4 *Cardholder Verification for the Magnetic Stripe Acceptance Technology*

Req T74: POIs with a PIN Entry Device shall meet the following requirements:

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

Note:

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.

~~4.2.3.3.4.2.5~~4.3.3.5.1.2.5 *Cardholder Verification for the Manual Entry Acceptance Technology*

Req T75: 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.

4.3.3.5.2 Conventional Local ICT Transactions (Physical POI)

4.3.3.5.2.1 Merchant-Presented QR Code

Authentication is performed by the Customer's ASPSP either directly (re-directed or decoupled Authentication) or through the PISP (embedded Authentication).

Req T364: Authentication shall be performed as shown in steps 5. and 6. in Figure 5 in Section 1.8 of Book 1.

The following Authentication Methods may be used:

- Dynamic Authentication - One Time Password (OTP)
- Dynamic Authentication - Challenge Response based on Authentication/Remote Payment Application on a Consumer Device
- Biometrics on Consumer Device (CDCVM)
- Offline Mobile Code (CDCVM)
- Online Mobile Code
- No CVM Required, if an SCA Exemption is allowed, e.g. based on Risk-Based Authentication or cases where SCA is not required

4.3.3.5.2.2 Consumer-Presented QR Code

Authentication is performed by the Customer's ASPSP either directly (re-directed or decoupled Authentication) or through the PISP (embedded Authentication) or via the Acceptor's POI.

If Authentication is performed via the Acceptor's POI, an interface would have been established between PISP and Acceptor's POI to collect the Customer data needed for authentication (e.g. an Online Personal Code and an OTP).

Req T365: Authentication shall be performed as shown in steps 5. and 6. in Figure 6 in Section 1.8 of Book 1.

The following Authentication Methods may be used:

- Dynamic Authentication - One Time Password (OTP)
- Dynamic Authentication - Challenge Response based on Authentication/Remote Payment Application on a Consumer Device
- Biometrics on Consumer Device (CDCVM)

- Offline Mobile Code (CDCVM)
- Online Mobile Code
- No CVM Required, if an SCA Exemption is allowed, e.g. based on Risk-Based Authentication or cases where SCA is not required

4.3.3.5.2.3 *Mobile Contactless*

Authentication is performed via an e-signed/authorised payment request with support of the Customer's bank app.

Req 366: Authentication shall be performed as shown in steps 2. and 3. in Figure 7 in Section 1.8 of Book 1 with support of the Customer's bank app, acting as a Mobile Contactless ICT Payment Application.

The following Authentication Methods may be used:

- Biometrics on Consumer Device (CDCVM)
- Offline Mobile Code (CDCVM)
- Dynamic Authentication - Challenge Response based on Authentication/(Remote) Payment Application on a Consumer Device
- No CVM Required, if an SCA Exemption is allowed, e.g. where SCA is not required

~~4.2.3.3.4.3~~ *Local Transactions (Physical POI)*

~~4.2.3.3.4.4~~ 4.3.3.5.3 *Remote Transactions at the Virtual POI*

~~Card~~ Authentication is the Function by which Strong Customer Authentication (SCA) Card Data or a Card Application is authenticated is performed to the Customer's ASPSP/Issuer. ~~However, some of the methods described below also facilitate cardholder authentication (e.g., OTP).~~

~~In addition,~~ Risk Based Authentication may be used by the Customer's ASPSP/Issuer to decide, whether an exemption for SCA applies as an additional method for risk management, as described in (see Book 4 Section 2.3.2.4 of Book 4).

For Remote Customer Present Transactions, i.e. e- and m-Commerce transactions, ~~Authentication~~ 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 [Customer's ASPSP/Issuer](#) domain.

~~Req T66: 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.~~

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

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

Req T76: The [Virtual](#) POI shall support at least [two of the following Authentication ~~one~~ Cardholder Verification Methods](#) of different SCA factors:.

- [Dynamic Authentication - One Time Password \(OTP\)](#)
- [Dynamic Authentication - Challenge Response based on Authentication/Remote Payment Application on a Consumer Device](#)
- [Dynamic Authentication - Challenge Response based on Additional Authentication Device](#)
- CDCVM, i.e. Biometrics on Consumer Device, Offline Personal Code or Offline Mobile Code,
- Online Personal Code or Online Mobile Code,
- No CVM Required, [if an exemption for SCA applies](#).
- [No CVM Required if an SCA Exemption is allowed, e.g. based on Risk-Based Authentication or cases where SCA is not 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 (Offline PIN, Offline Biometric Verification, Biometrics via Sensor on Card) 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 [Authentication ~~an online cardholder verification~~](#) during an [Card based](#) 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. It is highly recommended to support [EMV 3DS] for 3 Domain Security.

For ICT based e- and m-Commerce transactions, Authentication is performed by the Customer's ASPSP either directly (re-directed or decoupled Authentication) or through the PISP (embedded Authentication) as shown in steps 5. and 6. in Figure 4 in Section 1.8 of Book 1.

4.2.3.3.4.54.3.3.5.4 Remote Card Transactions at Physical POI and Virtual Terminal

Req T67: All MOTO Applications shall support Static Authentication.

Req T68: For MOTO transactions, ~~the card authentication is performed using Static Authentication~~ is performed 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 4.4.7 and 4.4.8).
- 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.

For MOTO, ~~no other Authentication Method 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.

4.2.3.44.3.3.6 Authorisation

Authorisation is the Function performed by the POI to get information whether ~~help the Acceptor to make a decision to proceed with a~~ PaymentCard Service has a positive or negative result~~not~~.

For Card Transactions, ~~this Function~~ can be processed online to the Acquirer according to Book 3 or processed offline by the EMV Card Payment Application.

For ICT Transactions, this Function is currently only described for One-off Payment. It is processed as shown in Figures 4 to 8 in Section 1.8 of Book 1. According to these Figures, Authorisation is initiated at the POI either by providing the payment details (step 0 in Figures 4 and 5 in Section 1.8 of Book 1) or by sending a payment request (step 3 in Figure 6, step 1 in Figure 7, step 2 in Figure 8 in Section 1.8 of Book 1).

At the latest, the POI receives the Authorisation result when the PISP informs about success or failure of the payment execution (step 11 in Figures 4 to 6, step 9 in Figures 7 and 8 in Section 1.8

of Book 1). However, if delays are allowed for payment execution and/or confirmation of success or failure, delivery of this information may take several seconds.

A faster delivery of the Authorisation result may be achieved if the PISP communicates success or failure of payment initiation by the Customer's ASPSP to the POI (see optional communication in step 9 in Figures 4 to 6, step 5 in Figures 7 and 8 in Section 1.8 of Book 1). Failure of the payment initiation always means a negative result for the One-off Payment. Successful payment initiation implies that the Customer's ASPSP has made a positive decision regarding the payment. Therefore, this information may be considered as the positive result of the Authorisation, provided error solutions are in place in case a payment execution is initiated but is finally not successful.

4.2.3.4.14.3.3.6.1 Local Card Transactions (Physical POI) and Remote Card Transactions at the Virtual POI

Req T77: If the authorisation response message includes a response code indicating that SCA is required, then the POI shall take appropriate action to obtain Cardholder Verification or, if this is not possible, decline the transaction.

Note:

There are several methods to obtain Cardholder Verification:

- SWITCH INTERFACE
- RE-PRESENT CARD AND ENTER PIN
- ENTER PIN WITHOUT A SECOND TAP

4.2.3.4.24.3.3.6.2 Local Card Transactions (Physical POI)

Req T78: 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 T79: 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 CustomerCardholder 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 T80: For attended POIs, for all [PaymentCard](#) Services with exception of the [One-off Payment Service](#) (see Req T120) and the Deferred Payment Service (see Req T191), the attendant shall not be allowed to force a declined transaction to be accepted.

Req T81: 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.

~~4.2.3.4.34.3.3.6.3~~ Remote [Card](#) Transactions at the Virtual POI

Req T82: For e- or m-[Commerce](#) transaction, the POI shall perform an online authorisation exchange to the [Issuer](#).

Req T83: The Payment Brand and Product Type of the selected application shall be included in the authorisation messages.

~~4.2.3.4.44.3.3.6.4~~ Remote [Card](#) Transactions at Physical POI or Virtual Terminal

Req T84: MOTO transactions shall be sent online for authorisation.

Req T85: If it is not possible to perform an online authorisation, either Voice Authorisation shall be performed or the transaction shall be declined.

Req T86: The authorisation message shall identify that the transaction is MOTO.

Req T87: If available, the Payment Brand and Product Type shall be included in the authorisation messages.

~~4.2.3.54.3.3.7~~ Referral

Referral is the Function where a [PaymentCard](#) 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 [Card Transactions](#). It does not necessarily involve the Cardholder or the [Payment DeviceCardholder Environment](#).

Req T88: Only attended POIs shall support referrals. If an unattended POI receives a request for referral it shall decline the transaction.

Req T89: 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 T90: 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 T91: 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 T92: The POI shall have mechanisms to ensure that only the authorised user can initiate the Referral Function.

4.2.3.6-14.3.3.8 Completion

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

- Complete the transaction for the PaymentCard Application
- Inform CustomerCardholder, Attendant and/or Acquirer/PISP about the result of the transaction
- Deliver a receipt to CustomerCardholder and/or Attendant

4.2.3.6-14.3.3.8.1 Local Card Transactions and Remote Card Transactions (all Acceptance Environments)

- Req T93: If the transaction (approved, declined or aborted) is not immediately online-captured, the transaction data shall be securely stored for data capture.

4.2.3.6.24.3.3.8.2 Local Transactions (Physical POI)

Req T94: If the POI is capable of printing receipts and/or of providing electronic receipts, a transaction receipt shall be provided for the Customer~~Cardholder~~ if configured for the Application Profile. The receipt for the Cardholder~~Customer~~ shall be printed/provided in a local language of the POI and, if offered by the Acceptor, in the Cardholder~~Customer~~ selected language. The transaction receipt may be combined with the sales receipt, if any.

The following are the minimum data that shall be present~~printed~~ on receipts.⁵⁹ The sequence of the data elements shown is not mandatory for the receipt. Additional data may be present~~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 Amount⁶⁰ and Transaction Currency⁶¹
- Truncated PAN or truncated or tokenised Account Reference
- DF Name (as returned by the Payment ~~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 Name⁶²
- The Payment ~~Card~~ Service, e.g., "One-off Payment"
- Transaction Result, e.g., "Approved"

⁵⁹ Provided these requirements are in line with the local laws and regulations.

⁶⁰ For Pre-Authorisation and Update Pre-Authorisation, this is the estimated amount that has been authorised.

⁶¹ For transactions with Dynamic Currency Conversion see Req- T324.

⁶² Detailed guidance on the usage of Acceptor Name can be found within Book 6.

~~4.2.3.6.34.3.3.8.3~~ Remote Transactions at the Virtual POI

Req T95: The POI shall provide a transaction receipt to the ~~Cardholder~~Customer 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 or truncated or tokenised Account Reference
- Payment Brand name
- Acceptor Name⁶²
- Transaction Reference number
- The ~~PaymentCard~~ Service, e.g., "One-off Payment"
- Transaction Result, e.g., "Approved"

Req T96: The transaction receipt shall be made available as confirmation to the ~~Cardholder~~Customer according to ~~Cardholder~~Customer's preference and communication channels available.

Req T97: In case of partial delivery the final amount shall be reduced and a new receipt shall be sent to the ~~Cardholder~~Customer.

Req T98: 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.

~~4.2.3.6.44.3.3.8.4~~ Remote Card Transactions at Physical POI or Virtual Terminal

Req T99: For Telephone Order transactions, at least a transaction reference shall be provided to the Cardholder during the call.

Req T100: 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 T95.

Req T101: 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.

4.2.3.74.3.3.9 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 is only performed for Local Card Transactions. It involves neither the Cardholder nor the Payment DeviceCardholder 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 and Remote Transactions (all Acceptance Environments):

Req T102: 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.

4.2.3.84.3.3.10 Data Capture

Data Capture is the Function to transfer data captured at a POI to the Acquirer/PISP 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/PISP decision, which of the data provided by the POI has to be provided by the Acquirer/PISP for ~~clearing (or Financial Presentment)~~.

~~4.2.3.8.14~~4.3.3.10.1 *Local Transactions and Remote Transactions (all Acceptance Environments)*

Req T103: 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.

Req T367: For Open Banking based ICT Transactions, Online capture through the authorisation message, i.e., according to Section 4.3.3.6, when providing the payment details (step 0 in Figures 4 and 5 in Section 1.8 of Book 1) or by sending a payment request (step 3 in Figure 6, step 1 in Figure 7, step 2 in Figure 8 in Section 1.8 of Book 1), shall be performed.

~~4.2.3.8.24~~4.3.3.10.2 *Local Transactions (Physical POI)*

Req T104: For Card Transactions, 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 '9FOA' of the selected application shall be included in Data Capture.

~~4.2.3.8.34~~4.3.3.10.3 *Remote Transactions at the Virtual POI*

Req T105: The Payment Brand and, for Card Transactions, Product Type shall be included in Data Capture.

~~4.2.3.8.44~~4.3.3.10.4 *Remote Card Transactions at Physical POI and Virtual Terminal*

Req T106: The completion message shall identify that the transaction is MOTO.

Req T107: If available, the Payment Brand and Product Type shall be included in Data Capture.

4.34.4 Payment-Basic Services

4.3.14.4.1 One-off Payment

For One-off Payment, Local Transactions are always Local Customerard Present. Remote Transactions are always e- or m-Ceommerce if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal.

Table 7 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote Transactions are allowed (✓) or not allowed/not applicable (✗) for the One-off Payment Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- <u>Ceommerce</u>)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local <u>Customerard</u> Present)	Unattended (always Local <u>Customerard</u> Present)		
Chip with Contact	✓ ⁶³	✓ ⁶³	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓ ⁶⁵	✓ ⁶⁵	✗	✗
Manual Entry (by <u>CustomerCardholder</u>)	✗	✗	✗/✓	✓ ⁶⁶
Consumer Device with Payment Credentials	✗	✗	✗/✓	✗
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✓	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✓	✗
<u>Merchant-presented QR Code</u> ⁶⁷	✓	✓	✗	✗
<u>Consumer-presented QR Code</u> ⁶⁷	✓	✓	✗	✗

⁶³ For ICT Transactions, this Acceptance Technology may only be used for those using EMV technology.

⁶⁴ This Acceptance Technology is only allowed for Card Transactions.

⁶⁵ For ICT Transactions, Chip Contactless may only be used for those using EMV technology.

⁶⁶ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

⁶⁷ This Acceptance Technology is not allowed for Card Transactions.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local Customer Card Present)	Unattended (always Local Customer Card Present)		
Stored <u>Account Card</u> Data ⁶⁸	x	x	x✓	x

TABLE 7: ONE-OFF PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in Table 8 shows which Functions are not applicable (-) or which are mandatory (M), optional (O) or conditional (C) for the One-off Payment Service and for Local and Remote Transactions 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	Remote Transactions	
	Physical POI (always Local Customer Card Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
Language Selection	M	O	-
Transaction Initialisation	M	M	M
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Selection of the Payment Instrument</u>	<u>C</u>	<u>C</u>	<u>C</u>
• <u>Technology Selection</u>	M	-	-
• <u>Selection of the Payment Brand</u>	M	M	M
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Card Authentication</u> ⁶⁹	C	M	M
• <u>Cardholder Verification</u> ⁶⁹	M	M	-

⁶⁸ This Acceptance Technology may be called Stored Card Data for Card Transactions.

⁶⁹ The distinction of Card Authentication and Cardholder Authentication is only relevant for EMV based Local Card and ICT Transactions.

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local Customer ard Present)	Virtual POI (always e- or m- C ommerce)	Physical POI or Virtual Terminal (always MOTO)
Authorisation	M	M	M
Referral ⁷⁰	O	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 8: FUNCTIONS USED FOR [ONE-OFF](#) PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the [One-off](#) Payment Service for Local Transactions and Remote Transactions (all Acceptance Environments).

[4.3.1.14.4.1.1](#) POI Application

[4.3.1.1.14.4.1.1.1](#) Local [and Remote Card and ICT](#) Transactions ~~and Remote Transactions~~ (all Acceptance Environments)

Req T108: 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.

[4.3.1.1.24.4.1.1.2](#) Local [Card](#) Transactions (Physical POI)

Req T109: ~~For Payment, the~~ [Customer](#)~~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 Physical Card or Mobile Device before the transaction amount is known. In those cases, the [Customer](#)~~Cardholder~~ shall be

⁷⁰ [This Function is only performed for Local Card Transactions.](#)

⁷¹ [This Function is only performed for Card Transactions.](#)

informed of the transaction amount so that the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

- Req T110: 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 T111: If the POI supports partial approvals of online authorisations, then it shall support it for all Acceptance Technologies supported.

4.4.1.1.3 Local ICT Transactions (Physical POI)

Req T368: The Customer shall be able to confirm the transaction amount prior to Account Data Retrieval (see Figures 5 to 8 in Section 1.8 of Book 1).

4.3.1.1.34.4.1.1.4 Remote Transactions at the Virtual POI

- Req T112: For e- and m-Commerce transactions the Virtual POI shall inform the CustomerCardholder about the transaction including the transaction amount prior to Account Card Data Retrieval.

4.3.1.1.44.4.1.1.5 Remote Transactions at Physical POI and Virtual Terminal

- Req T113: For MOTO transactions it is the Card-Acceptor that shall confirm the transaction, including the transaction amount.

4.3.1.24.4.1.2 Configuration

4.3.1.2.14.4.1.2.1 Local Transactions and Remote Transactions (all Acceptance Environments)

- Req T114: 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.

4.3.1.2.24.4.1.2.2 Local Card Transactions (Physical POI)

- Req T115: It shall be configured that the Chip with Contact Acceptance Technology and/or the Contactless Acceptance Technology shall be supported (see Req T19) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T23).

- Req T116: For attended POIs that support [One-off](#) 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 [Customercardholder](#).
- Req T117: For the specific Unable-to-go-online processing described in Req T127, 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 T118: For attended POIs that support partial approvals of online authorisations it shall be configurable per Application Profile whether partial approvals are activated.
- Req T119: 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 T120: For attended POIs, if the POI is offline 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 T121: For unattended POIs, forcing a declined transaction to be accepted shall not be supported.

However, for unattended environments where the interaction with the [Customercardholder](#) 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.

[4.3.1.2.34.4.1.2.3](#) Remote [Card](#) Transactions at Physical POI and Virtual Terminal

- Req T122: 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.

[4.3.1.34.4.1.3](#) Transaction Initialisation

The following requirement applies to Local Transactions and Remote Transactions (all Acceptance Environments):

- Req T123: For [One-off](#) 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.

4.3.1.44.4.1.4 Authorisation

4.3.1.4.14.4.1.4.1 Local and Remote Card Transactions ~~and Remote Transactions~~ (all Acceptance Environments)

- Req T124: If an online authorisation is required and it is not possible to perform the authorisation, the transaction shall be declined.
- Req T125: For Authorisation, the transaction amount as defined in Req T123 shall be used.
- Req T126: 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.

4.3.1.4.24.4.1.4.2 Local Card Transactions (Physical POI)

- Req T127: 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.

4.3.1.4.34.4.1.4.3 Remote Card Transactions at Physical POI and Virtual Terminal

- Req T128: For MOTO, as online authorisation is required if it is not possible to perform an online or voice authorisation, the transaction shall be declined.

4.3.1.54.4.1.5 Completion

4.3.1.5.14.4.1.5.1 Local Transactions (Physical POI) and Remote Transactions at the Virtual POI

- Req T129: Any POI which is integrated with the sale system shall send a message to the sale system to indicate the transaction result.

In addition, [for Card Transactions](#), the POI ~~it~~ shall receive the final transaction amount if different from the authorised amount, from the sale system.

~~4.3.1.5.2~~ [4.4.1.5.2](#) *Local Transactions (Physical POI)*

Req T130: [For Card Transactions](#), the POI shall have mechanisms to ensure that only the authorised user can force a declined transaction to be accepted.

Req T131: [For Card and ICT Transactions using a Physical Card](#), ~~to~~ prevent the [Customer 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~~ [4.4.1.6](#) *Reversal*

These Requirements apply to Local [and Remote Card](#) Transactions ~~and Remote Transactions~~ (all Acceptance Environments):

Req T132: 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 T133: 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.

4.3.24.4.2 Refund

For Refund, Local Transactions are Local [Customer Card](#) Present or Local AIT and are always attended. Remote Transactions are always Remote AIT.

Table 9 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Refund Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
	Attended (Local Customer Card Present / Local AIT)	Unattended (not allowed)		
Chip with Contact	✓/✗	✗	✗	✗
Magnetic Stripe ⁶⁴	✓/✗	✗	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓/✗	✗	✗	✗
Contactless (Chip and Mobile)	✓/✗	✗	✗	✗
Manual Entry (by Customer Cardholder)	✗	✗	✗	✗
Consumer Device with Payment Credentials	✗	✗	✗	✗
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored Account Card Data ⁶⁸	✗/✓	✗	✓	✓

TABLE 9: REFUND: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **Table 10** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Refund Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	M/-	-	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M/-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	-	-	-
• Card Authentication ⁶⁹	-	-	-
• Cardholder Verification ⁶⁹	-	-	-
Authorisation	O	O	O
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 10: FUNCTIONS USED FOR REFUND

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Refund Service for Local [Card](#) Transactions (Physical POI) [and for Remote Card Transactions](#), ~~e-and m-commerce~~ (Virtual POI, ~~)and/or MOTO~~ (Physical POI or Virtual Terminal).

~~4.3.2.14.4.2.1~~ POI Application

~~4.3.2.14.4.2.1.1~~ Local Transactions and Remote Transactions (all Acceptance Environments)

Req T134: 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.

~~4.3.2.14.4.2.1.2~~ Local Transactions (Physical POI)

Req T135: For Local [CustomerCard](#) Present transactions the Refund Service shall not be initiated by the [CustomerCardholder](#) without the Acceptor being involved.

Req T136: 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 [complete EMV based](#) Card Transaction. Therefore, EMV processing shall be followed until the [AccountCard](#) Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the [eExpiry dDate](#). If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the [EMV Card Payment](#) Application.

~~4.3.2.24.4.2.2~~ Configuration

The following requirements apply to Local Transactions and Remote Transactions (all Acceptance Environments):

Req T137: 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 T138: It shall be configurable per Application Profile, whether the Refund is performed online or not.

4.3.2.34.2.3 Transaction Initialisation

The following requirement applies to Local Transactions and Remote Transactions (all Acceptance Environments):

Req T139: The Refund amount shall be available to the POI Application at Transaction Initialisation. The way to link the Refund transaction to a previous [One-off Payment](#) is out of scope.

4.3.2.44.2.4 Authorisation

The following requirement applies to Local Transactions and Remote Transactions (all Acceptance Environments):

Req T140: If authorisation is required by the Application Profile, then the Refund shall be processed online.

4.3.34.3 Cancellation

For Cancellation, Local Transactions are Local [CustomerCard](#) Present or Local AIT and are always attended. Remote Transactions are always Remote AIT.

Table 11 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the [CancellationRefund](#) Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
	Attended (Local CustomerCard Present / Local AIT)	Unattended (not allowed)		
Chip with Contact	✓/✗	✗	✗	✗
Magnetic Stripe ⁶⁴	✓/✗	✗	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓/✗	✗	✗	✗
Contactless (Chip and Mobile)	✓/✗	✗	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗	✗
Consumer Device with Payment Credentials	*	*	*	*

	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
	Attended (Local CustomerCard Present / Local AIT)	Unattended (not allowed)		
Acceptance Technologies				
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗/✓	✗	✓	✓

TABLE 11: CANCELLATION: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in Table 12 shows which Functions are not applicable (-) or which are, mandatory (M), optional (O) or conditional (C) for the Cancellation Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	M/-	-	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M/-	-	-
• Selection of the Payment Brand	M	M	M

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	-	-	-
• <u>Card Authentication</u> ⁶⁹	-	-	-
• <u>Cardholder Verification</u> ⁶⁹	-	-	-
Authorisation	C	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	C	C	C

TABLE 12: FUNCTIONS USED FOR CANCELLATION

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Cancellation Service for Local Card Transactions and Remote Card Transactions (all Acceptance Environments).

4.3.3.14.4.3.1 POI Application

4.3.3.1.14.4.3.1.1 Local Transactions and Remote Transactions (all Acceptance Environments)

- Req T141: A Cancellation shall always be performed for the full amount of the original transaction.
- Req T142: When performed for the Pre-Authorisation Services, the Cancellation Service shall cancel a Pre-Authorisation and all linked Update Pre-Authorisation(s).
- Req T143: The Cancellation Service shall be supported to cancel a Payment Completion.

4.3.3.1.24.4.3.1.2 Local Transactions (Physical POI)

- Req T144: For Local CustomerCard Present transactions the Cancellation Service shall not be initiated by the ~~Cardholder~~Customer without the Acceptor being involved.

Req T145: 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 [complete EMV based](#) Card Transaction. Therefore, EMV processing shall be followed until the [AccountCard](#) Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the [eExpiry dDate](#). If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the [EMV](#) Card [Payment](#) Application.

4.3.3.24.4.3.2 Configuration

The following requirements apply to Local Transactions and Remote Transactions (all Acceptance Environments):

- Req T146: It shall be configurable per Application Profile which of the [PaymentCard](#) Services can be cancelled.
- Req T147: 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 T148: 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 T149: 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 T150: 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.

4.3.3.34.4.3.3 Authorisation

The following requirements apply to Local Transactions and Remote Transactions (all Acceptance Environments):

- Req T151: 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 T152: 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 (only applicable to Local [CustomerCard](#) Present Transactions), 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.

4.3.3.44.3.4 Data Capture

The following requirements apply to Local Transactions and Remote Transactions (all Acceptance Environments):

Req T153: Data Capture shall be performed according to the conditions described in T152.

Req T154: Every captured Cancellation transaction shall include a (set of) data element(s) uniquely referencing the original transaction.

4.3.44.4.4 Pre-Authorisation Services

Pre-Authorisation Services are:

- Pre-Authorisation Service (see Section 4.4.4.1.1),
- Update Pre-Authorisation Service (see Section 4.4.4.1.2) and
- Payment Completion Service (see Section 4.4.4.2).

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.

For Pre-Authorisation Services, Local Transactions are Local [CustomerCard](#) Present, which are attended or unattended, or Local AIT, which are attended. At least one of the Pre-Authorisation Service(s) prior to Payment Completion shall be Local [CustomerCard](#) Present. A Remote (Update) Pre-Authorisation transactions are e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal, or Remote AIT. At least one of the Pre-Authorisation Service(s) prior to Payment Completion performed at the Virtual POI shall be e- or m-[Commerce](#). Remote Payment Completion transactions are always Remote AIT.

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 [Browser over Internet](#)~~Payment Credentials and Authentication Application~~,
- Consumer Device with [Dedicated \(M\)RP Application](#) [over Internet](#).

Table 13 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Pre-Authorisation Services.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
	Attended (Local CustomerCard Present / Local AIT)	Unattended (Local CustomerCard Present)		
Chip with Contact	✓/✗	✓	✗	✗
Magnetic Stripe ⁶⁴	✓/✗	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓/✗	✗	✗	✓/✗
Contactless (Chip and Mobile)	✓/✗	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗/✗	✓ ⁷² /✗
Consumer Device with Payment Credentials	✗	✗	✗/✗	✗
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✓/✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✓/✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗/✓	✗	✗/✓	✗/✓

TABLE 13: PRE-AUTHORISATION SERVICES: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

4.3.4.14.4.1 Pre-Authorisation Service and Update Pre-Authorisation Service

The column "Requirement" in **TABLE 14:** shows which Functions are not applicable (-) or which are, mandatory (M), optional (O) or conditional (C) for the Pre-Authorisation and Update Preauthorisation Service and for Local and Remote [Card](#) Transactions using the respective Acceptance Environments Physical POI (attended and unattended), Virtual POI and Virtual

⁷² 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	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
Language Selection	M/-	O/-	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M/-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	C/-	C/-	C/-
• Card Authentication ⁶⁹	C/-	C/-	C/-
• Cardholder Verification ⁶⁹	C/-	C/-	-
Authorisation	M	M	M
Referral ⁷⁰	O/-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	-	-	-

TABLE 14: FUNCTIONS USED FOR PRE-AUTHORISATION AND UPDATE PREAUTHORISATION

4.3.4.1.14.4.1.1 Pre-Authorisation Service

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Pre-Authorisation Service for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

4.3.4.1.1.14.4.1.1.1 POI Application

Req T155: 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 T156: If the [CustomerCardholder](#) is participating, the [CustomerCardholder](#) shall be informed of the transaction amount and shall be able to confirm the transaction amount and the [CustomerCardholder](#) display shall clearly indicate that the amount to be confirmed is an estimated amount and is a Pre-Authorisation.

Req T157: For Local [Customer Present](#) Transactions, ~~if the Cardholder is participating~~, the [CustomerCardholder](#) shall be informed of the transaction amount and shall be able to confirm the transaction amount and the Payment Brand when performing the CVM.

The only exceptions are when the CVM is No CVM Required or when the Cardholder Verification is performed on the Physical Card or Mobile Device before the transaction amount is known. In those cases, the [CustomerCardholder](#) shall be informed of the transaction amount so that the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

Req T158: A Pre-Authorisation shall be identified as such in authorisation messages and transaction data.

Req T159: Data from approved Pre-Authorisations (e.g., PAN and ~~e~~Expiry ~~d~~ate, amount, authorisation code and unique reference) shall be stored for performing subsequent steps (i.e. Update Pre-Authorisation, Payment Completion).

Req T160: If an [EMV](#) Card [Payment](#) Application is used, the appropriate [EMV](#) Card [Payment](#) 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.

4.3.4.1.1.24.4.1.1.2 Configuration

Req T161: The POI Application shall be configurable to allow the Pre-Authorisation amount to be received or to be a configurable default amount.

4.3.4.1.1.34.4.1.1.3 Card Authentication and Cardholder Verification

Req T162: The Pre-Authorisation or at least one of the subsequent Update Pre-Authorisations shall be performed with Cardholder Verification and, if necessary for SCA, with Card Authentication.

4.3.4.1.1.44.4.1.1.4 Authorisation

Req T163: A Pre-Authorisation shall be authorised online in order to reserve the funds.

Req T164: 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.

4.3.4.1.1.54.4.1.1.5 Data Capture

Req T165: Approved Pre-Authorisations shall not be captured.

4.3.4.1.24.4.1.2 Update Pre-Authorisation Service

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Update Pre-Authorisation Service for Local Transactions and Remote Transactions (all Acceptance Environments).

4.3.4.1.2.14.4.1.2.1 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 Payment Device~~card~~ or Customer~~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 T166: 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 T167: An approved Update Pre-Authorisation shall increment or decrement the amount of the previously linked Pre-Authorisation and Update Pre-Authorisation(s).

Req T168: 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 an [EMV Card Payment Application](#) then the relevant [EMV Card Payment Application](#) data shall be stored for subsequent steps.

Req T169: An Update Pre-Authorisation shall include the increment or decrement amount to be authorised.

Req T170: If the [CustomerCardholder](#) is participating, the [CustomerCardholder](#) shall be informed of the transaction amount and shall be able to confirm the transaction amount and the [CustomerCardholder](#) display shall clearly indicate that the amount to be confirmed is the increment or decrement amount.

Req T171: For Local [Customer Present](#) 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 [CustomerCardholder](#) 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 or when the Cardholder Verification is performed on the Physical Card or Mobile Device before the transaction amount is known. In those cases, the [CustomerCardholder](#) shall be informed of the transaction amount so that the confirmation of the transaction amount shall be implicit by presenting the Physical Card or Mobile Device.

Req T172: If the Update Pre-Authorisation is declined, the previously linked Pre-Authorisation (or Update Pre-Authorisation(s)) shall remain unchanged and valid.

Req T173: 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~~ [4.4.1.2.2](#) *Card Authentication and Cardholder Verification*

Req T174: If the Pre-Authorisation was not performed with Cardholder Verification and with Card Authentication, then at least one of the subsequent Update Pre-Authorisations shall be performed with Cardholder Verification and, if necessary for SCA, with Card Authentication.

~~4.3.4.1.2.3~~ [4.4.1.2.3](#) *Authorisation*

Req T175: An Update Pre-Authorisation shall be processed online.

4.3.4.1.2.44.4.1.2.4 Completion

Req T176: The transaction receipt, if any, shall clearly show that this is an Update Pre-Authorisation and shall indicate the increment or decrement amount.

4.3.4.1.2.54.4.1.2.5 Data Capture

Req T177: Approved Update Pre-Authorisations shall not be captured.

4.3.4.24.4.2 Payment Completion Service

The column "Requirement" in **TABLE 15** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Payment Completion Service for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	M/-	-	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M/-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	-	-	-
• Card Authentication ⁶⁹	-	-	-
• Cardholder Verification ⁶⁹	-	-	-

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Authorisation	-	-	-
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	-	-	-
Data Capture	M	M	M

TABLE 15: FUNCTIONS USED FOR PAYMENT COMPLETION

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Payment Completion Service for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

[4.3.4.2.14.4.4.2.1](#) 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 T178: 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 T179: 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 [complete EMV based Card Transaction](#). Therefore, EMV processing shall be followed until the [AccountCard](#) Data Retrieval Function has obtained either the Track 2 equivalent data, or the PAN together with the [eExpiry dDate](#). If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the [EMV Card Payment](#) Application.

Req T180: A Payment Completion shall be identified as such in transaction data and shall contain the unique reference from the original linked Pre-Authorisation.

Req T181: A Payment Completion shall include the final amount.

Req T182: If the [CustomerCardholder](#) is participating, the POI display shall clearly indicate that the amount is the final amount.

[4.3.4.2.24.4.4.2.2](#) Configuration

Req T183: 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.

[4.3.4.2.34.4.4.2.3](#) Data Capture

Req T184: If an [EMV Card Payment](#) 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 [EMV Card Payment](#) Application data retained from the Pre-Authorisation Service.

[4.3.54.4.5](#) Deferred Payment

For Deferred Payment, only Local [Customer Present](#) Transactions are allowed ~~and are always Local Card Present~~.

TABLE 16 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Deferred Payment Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗	✗
Consumer Device with Payment	*	*	*	*

	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Acceptance Technologies				
Credentials				
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗	✗	✗	✗

TABLE 16: DEFERRED PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 17** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Deferred Payment Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	-	-
Transaction Initialisation	M	-	-
Selection of the Payment Solution	M	-	-
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	-	-

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
<u>Account</u> Data Retrieval	M	-	-
<u>Authentication</u>	<u>M</u>	<u>-</u>	<u>-</u>
• Card Authentication ⁶⁹	C	-	-
• Cardholder Verification ⁶⁹	M	-	-
Authorisation	M	-	-
Referral ⁷⁰	O	-	-
Completion	M	-	-
(Partial) Reversal ⁷¹	C	-	-
Data Capture	M	-	-

TABLE 17: FUNCTIONS USED FOR DEFERRED PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Deferred Payment Service for Local Card Transactions (Physical POI).

4.3.5.14.4.5.1 POI Application

Req T185: 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 T186: 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 T187: The ~~Customer~~cardholder shall be informed of the transaction amount and 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 or if the Cardholder Verification is performed on the Physical Card or Mobile Device before the transaction amount is known, then the confirmation of the transaction amount shall either be implicit by informing

the [CustomerCardholder](#) of the transaction amount prior to presenting the Physical Card or Mobile Device, or explicit with a confirmation display showing the transaction amount, if confirmation of the transaction amount is configured for the Application Profile.

4.3.5.24.4.5.2 Configuration

- Req T188: It shall be configured that the Chip with Contact Acceptance Technology and/or the Contactless Acceptance Technology shall be supported (see Req T19) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T23).
- Req T189: It shall be possible to configure per Application Profile, if the transaction amount shall be checked against a maximum allowed amount.
- Req T190: For Deferred Payment, it shall be possible to configure per Application Profile, if the transaction amount shall be confirmed by the [Customercardholder](#).
- Req T191: 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 T192: 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.

4.3.5.34.4.5.3 Authorisation

- Req T193: Deferred Payment shall be authorised online.
- Req T194: 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.

4.3.5.44.4.5.4 Reversal

- Req T195: 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 T197.

4.3.5.54.4.5.5 Completion

- Req T196: The POI shall receive the delivery result from the sale system, including the final amount which may be a zero amount.

Req T197: 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 T198: The POI shall send a message to the sale system to indicate the transaction result.

4.3.5.64.4.5.6 Data Capture

Req T199: Data Capture shall be performed either as online capture through a completion message sent after each transaction (referred to as notification message in T197) or through batch capture.

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

4.3.64.4.6 No-Show

"No-Show" is processed as MITa "Card Not pPresent" Service, which can only be performed using recorded Card Data information including PAN and eExpiry dDate, because the reservation process (e.g., of a hotel room or a rental car) does not normally involve the Payment DeviceCardholder Environment being present or the EMV Card Payment 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 eExpiry dDate 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 Payment DeviceCard and CustomerCardholder are physically present at time of the reservation, only PAN and eExpiry dDate would be taken, for the purposes of the guaranteed reservation, in the event a No-Show needs to be processed.

For No-Show, Local Transactions are always Local AIT and attended. Remote Transactions are always Remote AIT.

TABLE 18 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the ~~Refund-No-Show~~ Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
	Attended (always Local AIT)	Unattended (not allowed)		
Chip with Contact	✗	✗	✗	✗
Magnetic Stripe ⁶⁴	✗	✗	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✗	✗	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗	✗
Consumer Device with Payment Credentials	✗	✗	✗	✗
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✓	✗	✓	✓

TABLE 18: NO-SHOW: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in Table 19 shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the No-Show Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	-	-	-
Transaction Initialisation	M	M	M
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Selection of the Payment Instrument</u>	-	-	-
• <u>Technology Selection</u>	-	-	-
• <u>Selection of the Payment Brand</u>	M	M	M
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	-	-	-
• Card Authentication ⁶⁹	-	-	-
• Cardholder Verification ⁶⁹	-	-	-
Authorisation	M	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 19: FUNCTIONS USED FOR NO-SHOW

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the No-Show Service for Local Card Transactions (attended Physical POI) and Remote Card Transactions MOTO (Virtual POI, attended Physical POI or Virtual Terminal).

4.3.6.14.4.6.1 Authorisation

Req T200: No-Show transactions shall be authorised online and shall be identified as No-Show.

4.3.6.24.4.6.2 Data Capture

Req T201: No-Show transactions shall be identified as No-Show when they are captured.

4.3.7.4.7 Instalment Payment

The Instalment Payment Service is initiated by a first transaction from the POI which is a [One-off 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 MIT 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 4.4.7.1.

The requirements for the subsequent transactions of an Instalment Payment are described in Section 4.4.7.2.

4.3.7.14.4.7.1 First Transaction

For the first transaction of an Instalment Payment, Local Transactions are always Local [CustomerCard](#) Present. Remote Transactions are always e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal.

TABLE 20 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the first transaction of an Instalment Payment.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by <u>CustomerCardholder</u>)	✗	✗	✗✓	✓ ⁷³
<u>Consumer Device with Payment Credentials</u>	✗	✗	✓	✗
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✓	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✓	✗
<u>Merchant-presented QR Code</u> ⁶⁷	✗	✗	✗	✗
<u>Consumer-presented QR Code</u> ⁶⁷	✗	✗	✗	✗
Stored <u>AccountCard</u> Data ⁶⁸	✗	✗	✗	✗

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

⁷³ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

The column "Requirement" in **TABLE 21** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the first transaction of an Instalment Payment and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
Language Selection	M	O	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	M	M	M
• Card Authentication ⁶⁹	C	M	M
• Cardholder Verification ⁶⁹	M	M	-
Authorisation	M	M	M
Referral ⁷⁰	O	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 21: FUNCTIONS USED FOR FIRST TRANSACTION OF AN INSTALMENT PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the first transaction of an Instalment Payment for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

~~4.3.7.1.14~~ 4.7.1.1 *POI Application*

Req T202: The first transaction of an Instalment Payment shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

~~4.3.7.1.24~~ 4.7.1.2 *Configuration*

Req T203: The allowed maximum total Instalment amount shall be configurable.

~~4.3.7.1.34~~ 4.7.1.3 *Authorisation*

Req T204: The first transaction of an Instalment Payment shall be authorised online and shall include the information which identifies it as the first transaction of an Instalment Payment and how many [Instalment](#) Payment [transactions](#) shall be made in the payment plan, e.g., 1:6 to indicate that this is the first of 6 [Instalment](#) Payment transactions.

~~4.3.7.1.44~~ 4.7.1.4 *Data Capture*

Req T205: 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 [Instalment Payment](#) transactions shall be made in the payment plan (e.g., 1:6 to indicate the first of 6 [Instalment Payment](#) transactions).

~~4.3.7.24~~ 4.7.2 *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 [CustomerCardholder](#) will not be involved. Therefore, for subsequent transactions, Local Transactions are always Local AIT and attended. Remote Transactions are always Remote AIT.

The column "Requirement" in [Table 22](#) shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of an Instalment Payment for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	-	-	-
Transaction Initialisation	M	M	M
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Selection of the Payment Instrument</u>	-	-	-
• <u>Technology Selection</u>	-	-	-
• <u>Selection of the Payment Brand</u>	M	M	M
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	-	-	-
• Card Authentication ⁶⁹	-	-	-
• Cardholder Verification ⁶⁹	-	-	-
Authorisation	M	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 22: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF AN INSTALMENT PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the subsequent transactions of an Instalment Payment [for Local Card Transactions and Remote Card Transactions \(all Acceptance Environments\)](#).

[4.3.7.2.14.4.7.2.1](#) Authorisation

Req T206: Subsequent Instalment Payment transactions shall be authorised online using only PAN and [eExpiry dDate](#) 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 Payment [transactions](#)).

4.3.7.2.24.4.7.2.2 Data Capture

Req T207: 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 Payment [transactions](#)).

4.3.84.4.8 Recurring Payment

The Recurring Payment Service applies to [One-off](#) Payments and Deferred Payments performed on a recurring basis.

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

The subsequent transactions of a Recurring Payment are [MIT"Card Not pPresent" transactions initiated by the Acceptor](#) 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 4.4.8.1.

The requirements for the subsequent transactions of a Recurring Payment are described in Section 4.4.8.2.

4.3.8.14.4.8.1 First Transaction

For the first transaction of a Recurring Payment, Local Transactions are always Local [CustomerCard](#) Present. Remote Transactions are always e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal.

TABLE 23 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the first transaction of a Recurring Payment.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by <u>CustomerCardholder</u>)	✗	✗	<u>✗</u> ✓	✓ ⁷⁴
<u>Consumer Device with Payment Credentials</u>	* <u>✗</u>	* <u>✗</u>	<u>✗</u> ✓	* <u>✗</u>
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✓	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✓	✗
<u>Merchant-presented QR Code</u> ⁶⁷	<u>✗</u>	<u>✗</u>	<u>✗</u>	<u>✗</u>
<u>Consumer-presented QR Code</u> ⁶⁷	<u>✗</u>	<u>✗</u>	<u>✗</u>	<u>✗</u>
Stored <u>AccountCard</u> Data ⁶⁸	✗	✗	✗	✗

TABLE 23: RECURRING PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS FOR FIRST TRANSACTION

⁷⁴ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

The column "Requirement" in **TABLE 24** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the first transaction of a Recurring Payment and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
Language Selection	M	O	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	M	M	M
• Card Authentication ⁶⁹	C	M	M
• Cardholder Verification ⁶⁹	M	M	-
Authorisation	M	M	M
Referral ⁷⁰	O	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 24: FUNCTIONS USED FOR FIRST TRANSACTION OF A RECURRING PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the first transaction of a Recurring Payment for Local [Card](#) Transactions ~~and Remote Transactions (all Acceptance Environments)~~ (Physical POI), e- and m-~~C~~ommerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

~~4.3.8.1.14~~ [4.8.1.1](#) *POI Application*

Req T208: The first transaction of a Recurring Payment shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

Note:

Depending on the use case the [One-off](#) Payment may be performed with a zero amount.

~~4.3.8.1.24~~ [4.8.1.2](#) *Authorisation*

Req T209: The first transaction of a Recurring Payment shall be authorised online and it shall contain specific information which identifies it as a Recurring Payment transaction.

~~4.3.8.1.34~~ [4.8.1.3](#) *Data Capture*

Req T210: 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.

~~4.3.8.24~~ [4.8.2](#) *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 ~~Customer~~[Cardholder](#) will not be involved. Therefore, for subsequent transactions, Local Transactions are always Local AIT and attended. Remote Transactions are always Remote AIT.

The subsequent transactions may be [One-off](#) Payments or Deferred Payments.

The column "Requirement" in **TABLE 25** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of a Recurring Payment Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	-	-	-
Transaction Initialisation	M	M	M
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Selection of the Payment Instrument</u>	-	-	-
• <u>Technology Selection</u>	-	-	-
• <u>Selection of the Payment Brand</u>	M	M	M
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	-	-	-
• Card Authentication ⁶⁹	-	-	-
• Cardholder Verification ⁶⁹	-	-	-
Authorisation	M	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 25: FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF A RECURRING PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the subsequent transactions of a Recurring Payment [for Local Card Transactions and Remote Card Transactions \(all Acceptance Environments\)](#).

[4.3.8.2.14.4.8.2.1](#) Configuration

Req T211: If the subsequent transactions are Deferred Payments 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.

~~4.3.8.2.24~~ 4.4.8.2.2 *Authorisation*

Req T212: Subsequent Recurring Payment transactions shall be authorised online using only PAN and ~~e~~Expiry ~~d~~Date and shall contain specific information which identifies it as a Recurring Payment transaction and indicates whether it is a One-off Payment or a Deferred Payment.

~~4.3.8.2.34~~ 4.4.8.2.3 *Reversal*

Req T213: If the subsequent transactions are Deferred Payments 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 T215.

~~4.3.8.2.44~~ 4.4.8.2.4 *Completion*

Req T214: If the subsequent transactions are Deferred Payments the POI shall receive the delivery result from the sale system, including the final amount which may be a zero amount.

Req T215: If the subsequent transactions are Deferred Payments 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 T216: If the subsequent transactions are Deferred Payments the POI shall send a message to the sale system to indicate the transaction result.

~~4.3.8.2.54~~ 4.4.8.2.5 *Data Capture*

Req T217: The data captured for clearing of subsequent Recurring Payment transactions shall contain specific information which identifies it as a Recurring Payment transaction and indicates whether it is a Payment or a Deferred Payment.

Req T218: If the subsequent transactions are Deferred Payments Data Capture shall be performed either as online capture through a completion message sent after each transaction (referred to as notification message in T215) or through batch capture.

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

4.3.94.4.9 Quasi-Cash Payment

For Quasi Cash Payment, Local Transactions are always Local [CustomerCard](#) Present. Remote Transactions are always e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal.

TABLE 26 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Payment Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗ ✓	✓ ⁷⁵
Consumer Device with Payment Credentials	*	*	✗ ✓	*
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✓	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗	✗	✗	✗

TABLE 26: QUASI-CASH PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in TABLE 27 shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Quasi-Cash Payment Service and for

⁷⁵ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
Language Selection	M	O	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	M	M	M
• Card Authentication ⁶⁹	C	M	M
• Cardholder Verification ⁶⁹	M	M	-
Authorisation	M	M	M
Referral ⁷⁰	O	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	M	M	M

TABLE 27: FUNCTIONS USED FOR QUASI-CASH PAYMENT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Quasi-Cash Payment Service for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

[4.3.9.14.4.9.1 POI Application](#)

Req T219: The Quasi-Cash Payment shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

[4.3.9.24.4.9.2 Cardholder Verification](#)

Req T220: 'No CVM Required' shall not be supported for Quasi-Cash Payment transactions.

[4.3.9.34.4.9.3 Authorisation](#)

Req T221: The Quasi-Cash Payment shall be authorised online and it shall be identified as a Quasi-Cash Payment.

[4.3.9.44.4.9.4 Reversal](#)

Req T222: 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 T223: 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.

[4.3.9.54.4.9.5 Data Capture](#)

Req T224: The data captured for clearing of a Quasi-Cash Payment shall identify it as a Quasi-Cash Payment.

4.44.5 Cash Services

Only Local Card Transactions (Physical POI) are allowed for processing the Cash Services.

4.4.14.5.1 ATM Cash Withdrawal

An ATM is a specific Unattended POI supporting the ATM Cash Withdrawal [PaymentCard](#) Service. In this section, "Application" refers to a POI Application that supports the ATM Cash Withdrawal Service.

For ATM Cash Withdrawal, only [unattended](#) Local [Customer Present](#) Transactions are allowed ~~and are always unattended and Local Card Present~~.

TABLE 28 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the ATM Cash Withdrawal Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (not allowed)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✗	✓	✗	✗
Magnetic Stripe ⁶⁴	✗	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✗	✗	✗	✗
Contactless (Chip and Mobile)	✗	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗	✗
Consumer Device with Payment Credentials	✗	✗	✗	✗
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗	✗	✗	✗

TABLE 28: ATM CASH WITHDRAWAL: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 29** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the ATM Cash Withdrawal Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	-	-
Transaction Initialisation	M	-	-
Selection of the Payment Solution	M	-	-
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	-	-
Account Data Retrieval	M	-	-
Authentication	M	-	-
• Card Authentication ⁶⁹	C	-	-
• Cardholder Verification ⁶⁹	M	-	-
Authorisation	M	-	-
Referral ⁷⁰	-	-	-
Completion	M	-	-
(Partial) Reversal ⁷¹	C	-	-
Data Capture	M	-	-

TABLE 29: FUNCTIONS USED FOR ATM CASH WITHDRAWAL

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the ATM Cash Withdrawal Service for Local [Card](#) Transactions (Physical POI).

~~4.4.1.14~~5.1.1 Configuration

Req T225: It shall be configured that the Chip with Contact Acceptance Technology shall be supported (see Req T19) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T23).

~~4.4.1.24~~5.1.2 Transaction Initialisation

Req T226: The Welcome Screen shall be shown initially in the default language and English (or in the default language only if it is English).

Req T227: Transactions on the ATM shall be initiated by insertion or presentment of a Physical Card, presentment of a Mobile Device or by [CustomerCardholder](#) interaction.

~~4.4.1.34~~5.1.3 Authorisation

Req T228: ATM Cash Withdrawal transactions shall be authorised online. Otherwise ATM transactions shall be declined.

~~4.4.1.44~~5.1.4 Completion

Req T229: To minimise the risk of the [CustomerCardholder](#) leaving the Physical Card in the ATM; if the [CustomerCardholder](#) 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 T230: If the Physical Card is inserted in the reader of an ATM with card capture capability and if the [CustomerCardholder](#) does not retrieve the Card, the Card shall be retained.

Req T231: If the Physical Card is retained in response to the authorisation response message, an appropriate message shall be displayed to inform the [CustomerCardholder](#).

Req T232: An ATM shall not allow a declined transaction to be accepted.

Req T233: 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.

4.4.1.5.1.5 Reversal

- Req T234: If the actual amount was authorised but cash could not be delivered, a reversal shall be performed to nullify the original authorisation.
- Req T235: 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.

4.4.2.5.2 Cash Advance (Attended)

For Cash Advance, only attended Local Customer Present Transactions are allowed ~~and are always attended and Local Card Present.~~

TABLE 30 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗) for the Cash Advance Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local <u>Customer Card</u> Present)	Unattended (not allowed)		
Chip with Contact	✓	✗	✗	✗
Magnetic Stripe ⁶⁴	✓	✗	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✗	✗	✗
Manual Entry (by <u>Customer Cardholder</u>)	✗	✗	✗	✗
Consumer Device with Payment Credentials	✗	✗	✗	✗
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✗	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✗	✗

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local <u>CustomerCard</u> Present)	Unattended (not allowed)		
<u>Merchant-presented QR Code</u> ⁶⁷	x	x	x	x
<u>Consumer-presented QR Code</u> ⁶⁷	x	x	x	x
Stored <u>AccountCard</u> Data ⁶⁸	x	x	x	x

TABLE 30: CASH ADVANCE: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 31** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Cash Advance Service and for Local and Remote Card Transactions 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	Remote Transactions	
	Physical POI (always Local <u>CustomerCard</u> Present)	Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	-	-
Transaction Initialisation	M	-	-
<u>Selection of the Payment Solution</u>	<u>M</u>	-	-
• <u>Selection of the Payment Instrument</u>	-	-	-
• <u>Technology Selection</u>	M	-	-
• <u>Selection of the Payment Brand</u>	M	-	-
<u>Account</u> Data Retrieval	M	-	-
<u>Authentication</u>	<u>M</u>	-	-
• <u>Card Authentication</u> ⁶⁹	C	-	-
• <u>Cardholder Verification</u> ⁶⁹	M	-	-

Authorisation	M	-	-
Referral ⁷⁰	O	-	-
Completion	M	-	-
(Partial) Reversal ⁷¹	C	-	-
Data Capture	M	-	-

TABLE 31: FUNCTIONS USED FOR CASH ADVANCE

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Cash Advance Service for Local [Card](#) Transactions (Physical POI).

4.4.2-14.5.2.1 POI Application

Req T236 The Cash Advance Service shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

4.4.2-24.5.2.2 Configuration

Req T237: 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 T19) and that the Magnetic Stripe Acceptance Technology is subordinate to the Chip with Contact Acceptance Technology (see Req T23).

Req T238: 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.

4.4.2-34.5.2.3 Transaction Initialisation

Req T239: For Cash Advance, the transaction amount (i.e. the authorised amount) shall be available to the POI Application at Transaction Initialisation.

4.4.2-44.5.2.4 Cardholder Verification

Req T240: No CVM Required shall not be supported for the Cash Advance Service.

4.4.2-54.5.2.5 Authorisation

Req T241: 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~~4.5.2.6 Reversal

Req T242: If the actual amount was authorised but cash could not be delivered, a reversal shall be performed to nullify the original authorisation.

4.5.4.6 Card Enquiry Services

4.5.14.6.1 Card Validity Check

For Card Validity Check, Local Transactions are Local [CustomerCard](#) Present, which are attended or unattended, or Local AIT, which are attended. Remote Transactions are e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal, or Remote AIT.

TABLE 32 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Card Validity Check Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
	Attended (Local CustomerCard Present / Local AIT)	Unattended (Local CustomerCard Present)		
Chip with Contact	✓/✗	✓	✗	✗
Magnetic Stripe ⁶⁴	✓/✗	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓/✗	✗	✗	✓/✗
Contactless (Chip and Mobile)	✓/✗	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✓/✗	✓ ⁷⁶ /✗
Consumer Device with Payment Credentials	*	*	✓/✗	*
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✓/✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✓/✗	✗

⁷⁶ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
	Attended (Local CustomerCard Present / Local AIT)	Unattended (Local CustomerCard Present)		
Acceptance Technologies				
Merchant-presented QR Code ⁶⁷	x	x	x	x
Consumer-presented QR Code ⁶⁷	x	x	x	x
Stored AccountCard Data ⁶⁸	x/✓	x	x/✓	x/✓

TABLE 32: CARD VALIDITY CHECK: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 33** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Card Validity Check Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
Language Selection	M/-	O/-	-
Transaction Initialisation	M	M	M
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M/-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	C/-	C/-	O/-
• Card Authentication ⁶⁹	C/-	C/-	O/-
• Cardholder Verification ⁶⁹	O/-	O/-	-

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (Local CustomerCard Present / Local AIT)	Virtual POI (e- and m- Commerce / Remote AIT)	Physical POI or Virtual Terminal (MOTO / Remote AIT)
Authorisation	M	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	-	-	-
Data Capture	-	-	-

TABLE 33: FUNCTIONS USED FOR CARD VALIDITY CHECK

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Card Validity Check Service for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

4.5.1.14.6.1.1 POI Application

Req T243: A Card Validity Check transaction shall be performed like a [One-off](#) Payment transaction, but using its own configuration and without displaying and printing the transaction amount.

4.5.1.24.6.1.2 Transaction Initialisation

Req T244: For Card Validity Check, the authorised amount sent to the [EMV](#) Card [Payment](#) Application shall be set to zero.

4.5.1.34.6.1.3 Authorisation

Req T245: Card Validity Check transactions shall be authorised online. Otherwise Card Validity Check transactions shall be declined.

Req T246: Card Validity Check transactions shall be identified as such in the online authorisation request.

4.5.1.44.6.1.4 Data Capture

Req T247: Card Validity Check transactions shall not be captured for "Financial Presentment".

4.5.24.6.2 Balance Enquiry

For Balance Enquiry, only Local [Customer Present](#) Transactions are allowed ~~and are always Local Card Present.~~

TABLE 34 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Balance Enquiry Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗	✗
Consumer Device with Payment Credentials	✗	✗	✗	✗
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✗	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code ⁶⁷	✗	✗	✗	✗
Consumer-presented QR Code ⁶⁷	✗	✗	✗	✗
Stored AccountCard Data ⁶⁸	✗	✗	✗	✗

TABLE 34: BALANCE ENQUIRY: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 35** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Balance Enquiry Service and for Local and Remote [Card](#) Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (not allowed)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	-	-
Transaction Initialisation	M	-	-
Selection of the Payment Solution	M	-	-
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	-	-
Account Data Retrieval	M	-	-
Authentication	M	-	-
• Card Authentication ⁶⁹	C	-	-
• Cardholder Verification ⁶⁹	M	-	-
Authorisation	M	-	-
Referral ⁷⁰	-	-	-
Completion	M	-	-
(Partial) Reversal ⁷¹	-	-	-
Data Capture	-	-	-

TABLE 35: FUNCTIONS USED FOR BALANCE ENQUIRY

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Balance Enquiry Service for Local [Card](#) Transactions (Physical POI).

[4.5.2.14.6.2.1 POI Application](#)

Req T248: A Balance Enquiry transaction shall be performed like a [One-off](#) Payment transaction, but using its own configuration and without displaying and printing the transaction amount.

4.5.2.24.6.2.2 Transaction Initialisation

Req T249: For Balance Enquiry, the authorised amount sent to the [EMV](#) Card [Payment](#) Application shall be set to zero.

4.5.2.34.6.2.3 Authorisation

Req T250: Balance Enquiry transactions shall be authorised online. Otherwise Balance Enquiry transactions shall be declined.

Req T251: Balance Enquiry transactions shall be identified as such in the online authorisation request.

Req T252: The balance of the Card Account shall only be retrieved from a positive authorisation response.

4.5.2.44.6.2.4 Completion

Req T253: If the balance of the Card Account is retrieved from a positive authorisation response, it shall be displayed to the [Customer](#)~~cardholder~~ and printed on the [Customer](#)~~cardholder~~ receipt, if any.

Req T254: If Balance Enquiry is performed in an attended Acceptance Environment, the balance shall not be displayed to the attendant or printed on a merchant receipt.

4.6.4.7 Card Electronic Transfer

4.6.14.7.1 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-owner 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.

For Card Funds Transfer, Local Transactions are always Local CustomerCard Present. Remote Transactions are always e- or m-Ceommerce.

TABLE 36 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗) for the Card Funds Transfer Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by <u>CustomerCardholder</u>)	✗	✗	✗/✓	✗
<u>Consumer Device with Payment Credentials</u>	✗	✗	✓	✗
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✓	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✓	✗
<u>Merchant-presented QR Code</u> ⁶⁷	✗	✗	✗	✗
<u>Consumer-presented QR Code</u> ⁶⁷	✗	✗	✗	✗
Stored <u>AccountCard</u> Data ⁶⁸	✗	✗	✗	✗

TABLE 36: CARD FUNDS TRANSFER: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 37** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Card Funds Transfer Service and for Local and Remote Card Transactions 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	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	O	-
Transaction Initialisation	M	M	-
Selection of the Payment Solution	M	M	-
• Selection of the Payment Instrument	-	-	-
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	M	-
Account Data Retrieval	M	M	-
Authentication	M	M	-
• Card Authentication ⁶⁹	C	M	-
• Cardholder Verification ⁶⁹	M	M	-
Authorisation	M	M	-
Referral ⁷⁰	-	-	-
Completion	M	M	-
(Partial) Reversal ⁷¹	C	C	-
Data Capture	C	C	-

TABLE 37: FUNCTIONS USED FOR CARD FUNDS TRANSFER

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Card Funds Transfer Service for Local [Card](#) Transactions (Physical POI) and [Card based](#) e- and m-[Commerce transactions](#) (Virtual POI).

[4.6.1.14.7.1.1 POI Application](#)

Req T255: The Card Funds Transfer shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

4.6.1.24.7.1.2 Transaction Initialisation

- Req T256: The ~~Customer~~~~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 T257: The ~~Customer~~~~cardholder~~ shall be able to select the transaction amount to be credited to or debited from the Card Account.
- Req T258: ~~If in the case of an (Mobile)-EMV Card Payment Application based or a (Mobile) Remote Card Payment Application is used to process the based-Card Funds Transfer transaction, the application shall only be used it is only~~ for the purpose of retrieving the Card Data, not to perform a complete EMV based Card Payment transaction~~Transaction~~.

4.6.1.34.7.1.3 AccountCard Data Retrieval

- Req T259: If funds shall be transferred to the Card Account from a Funding Account the ~~Customer~~~~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 an ~~a (Mobile)-EMV Card Payment Application or a (Mobile) Remote Card Payment Application~~ is used to process the Card Funds Transfer transaction, this information may be retrieved from the ~~PaymentCard~~ Application.
- Req T260: If funds shall be transferred from the Card Account to another account the ~~Customer~~~~cardholder~~ shall have the opportunity to provide information to identify the account to be credited.
- Req T261: After the ~~AccountCard~~ Data Retrieval Function has obtained either the relevant Card Data (e.g., the Track 2 equivalent data), or the PAN together with the ~~eExpiry dDate~~, the ~~Card~~-Acceptor may decide to raise a fee for the Card Funds Transfer Service.
- The ~~Customer cardholder~~ shall be informed of any fee to be paid to the ~~card~~ ~~A~~acceptor for the Card Funds Transfer and the ~~Customer cardholder~~ shall have the opportunity to accept or decline the conditions of the Card Funds Transfer.

4.6.1.44.7.1.4 Authorisation

- Req T262: Card Funds Transfer transactions shall be authorised online and shall be identified as Card Funds Transfer.
- Req T263: 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 A~~acceptor as an additional amount.

4.6.1.54.7.1.5 Data Capture

Req T264: Data Capture for "Financial Presentment" is required only if the ~~card~~-Aacceptor raises a fee for the Card Funds Transfer.

4.6.24.7.2 Original Credit

For Original Credit, Local Transactions are always Local CustomerCard Present and attended. Remote Transactions are always e- or m-Commerce.

TABLE 38 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗) for the Original Credit Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- <u>C</u> ommerce)	Physical POI or Virtual Terminal (not allowed)
	Attended (always Local <u>CustomerCard</u> Present)	Unattended (not allowed)		
Chip with Contact	✓	✗	✗	✗
Magnetic Stripe ⁶⁴	✓	✗	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✗	✗	✗
Manual Entry (by <u>CustomerCardholder</u>)	✗	✗	<u>✗</u> ✓	✗
<u>Consumer Device with Payment Credentials</u>	<u>*</u>	<u>*</u>	<u>✓</u>	<u>*</u>
Consumer Device with <u>Browser over Internet Payment Credentials and Authentication Application</u>	✗	✗	✓	✗
Consumer Device with <u>Dedicated (M)RP Application over Internet</u>	✗	✗	✓	✗
<u>Merchant-presented QR Code</u> ⁶⁷	<u>✗</u>	<u>✗</u>	<u>✗</u>	<u>✗</u>
<u>Consumer-presented QR Code</u> ⁶⁷	<u>✗</u>	<u>✗</u>	<u>✗</u>	<u>✗</u>
Stored <u>AccountCard</u> Data ⁶⁸	✗	✗	✗	✗

TABLE 38: ORIGINAL CREDIT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 39** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Original Credit Service and for Local and Remote Card Transactions 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	Remote Transactions	
	Physical POI (always Local <u>CustomerCard</u> Present)	Virtual POI (always e- or m- <u>Ceommerce</u>)	Physical POI or Virtual Terminal (not allowed)
Language Selection	M	O	-
Transaction Initialisation	M	M	-
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>-</u>
• <u>Selection of the Payment Instrument</u>	<u>-</u>	<u>-</u>	<u>-</u>
• <u>Technology Selection</u>	M	-	-
• <u>Selection of the Payment Brand</u>	M	M	-
<u>Account</u> Data Retrieval	M	M	-
<u>Authentication</u>	<u>-</u>	<u>-</u>	<u>-</u>
• <u>Card Authentication</u> ⁶⁹	-	-	-
• <u>Cardholder Verification</u> ⁶⁹	-	-	-
Authorisation	O	O	-
Referral ⁷⁰	-	-	-
Completion	M	M	-
(Partial) Reversal ⁷¹	C	C	-
Data Capture	M	M	-

TABLE 39: FUNCTIONS USED FOR ORIGINAL CREDIT

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Original Credit Service for Local Card Transactions (Physical POI) and Card based e- and m-Ceommerce (Virtual POI).

4.6.2.14.7.2.1 POI Application

Req T265: For Local CustomerCard Present transactions the Original Credit Service shall not be initiated by the CustomerCardholder without the Acceptor being involved.

Req T266: 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 [complete EMV based Card Transaction](#). Therefore, EMV processing shall be followed until the [AccountCard Data Retrieval Function](#) has obtained either the Track 2 equivalent data, or the PAN together with the [eExpiry dDate](#). If Chip with Contact Acceptance Technology is used, the EMV process shall be terminated by requesting a decline from the [EMV Card Payment Application](#).

~~If in the case of an (Mobile) Remote Card Payment Application is used to process the based-Original Credit transaction, the (M)RP-Payment Application processing shall be terminated after the AccountCard Data Retrieval Function has obtained either the relevant card data (e.g., the Track 2 equivalent data), or the PAN together with the eExpiry dDate.~~

If the [Payment Card](#) Application requires entry of an amount, the amount given to the [Payment Card](#) Application during the Original Credit should be zero to avoid unnecessary Card Risk Management.

Req T267: 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.

4.6.2.24.7.2.2 Configuration

Req T268: 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 T269: It shall be configurable per Application Profile, whether the Original Credit is performed online or not.

4.6.2.34.7.2.3 Transaction Initialisation

Req T270: The Original Credit amount shall be available to the POI Application at Transaction Initialisation.

4.6.2.44.7.2.4 Authorisation

Req T271: If authorisation is required by the Application Profile, then the Original Credit shall be authorised online.

4.6.34.7.3 Prepaid Card - Loading & Unloading

The Prepaid Card Loading Service requires that the [CustomerCardholder](#) 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 [of the Customer](#) 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.

For Prepaid Card Loading, Local Transactions are always Local [CustomerCard](#) Present. Remote Transactions are always e- or m-[Commerce](#) if performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal.

TABLE 40 shows which combinations of Acceptance Technologies and Acceptance Environments used in Local and Remote [Card](#) Transactions are allowed (✓) or not allowed/not applicable (✗) for the Prepaid Card - Loading & Unloading Service.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local CustomerCard Present)	Unattended (always Local CustomerCard Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe ⁶⁴	✓	✓	✗	✗
Manual Entry (by Acceptor) ⁶⁴	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by CustomerCardholder)	✗	✗	✗ ✓	✓ ⁷⁷
Consumer Device with Payment Credentials	*	*	✓	*
Consumer Device with Browser over Internet Payment Credentials and Authentication Application	✗	✗	✓	✗
Consumer Device with Dedicated (M)RP Application over Internet	✗	✗	✓	✗

⁷⁷ On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m- <u>C</u> ommerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local <u>C</u> ustomer <u>C</u> ard Present)	Unattended (always Local <u>C</u> ustomer <u>C</u> ard Present)		
<u>Merchant-presented QR Code</u> ⁶⁷	x	x	x	x
<u>Consumer-presented QR Code</u> ⁶⁷	x	x	x	x
Stored <u>Account</u> <u>C</u> ard Data ⁶⁸	x	x	✓	x

TABLE 40: PREPAID CARD LOADING: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

The column "Requirement" in **TABLE 41** shows which Functions are not applicable (-) or which are either mandatory (M), optional (O) or conditional (C) for the Prepaid Card - Loading & Unloading Service and for Local and Remote Card Transactions 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	Remote Transactions	
	Physical POI (always Local <u>C</u> ustomer <u>C</u> ard Present)	Virtual POI (always e- or m- <u>C</u> ommerce)	Physical POI or Virtual Terminal (always MOTO)
Language Selection	M	O	-
Transaction Initialisation	M	M	M
<u>Selection of the Payment Solution</u>	<u>M</u>	<u>M</u>	<u>M</u>
• <u>Selection of the Payment Instrument</u>	-	-	-
• Technology Selection	M	-	-
• Selection of the <u>Payment Brand</u>	M	M	M
<u>Account</u> Data Retrieval	M	M	M
<u>Authentication</u>	<u>M</u>	<u>M</u>	<u>M</u>
• Card Authentication ⁶⁹	C	M	M
• Cardholder Verification ⁶⁹	M	M	M

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local CustomerCard Present)	Virtual POI (always e- or m- Commerce)	Physical POI or Virtual Terminal (always MOTO)
Authorisation	M	M	M
Referral ⁷⁰	-	-	-
Completion	M	M	M
(Partial) Reversal ⁷¹	C	C	C
Data Capture	C	C	C

TABLE 41: FUNCTIONS USED FOR PREPAID CARD - LOADING & UNLOADING

In addition to the general requirements listed in Section 4.3, the following specific requirements apply to the Prepaid Card - Loading & Unloading Service for Local [Card](#) Transactions and Remote [Card](#) Transactions (all Acceptance Environments).

4.6.3.14.7.3.1 POI Application

Req T272: The Prepaid Card - Loading & Unloading shall follow the same process as the [One-off](#) Payment Service for all available Acceptance Technologies, but using its own configuration.

4.6.3.24.7.3.2 Transaction Initialisation

Req T273: The [Customercardholder](#) shall be able to select whether the Prepaid Card shall be loaded or unloaded.

Req T274: The [Customercardholder](#) shall be able to select the transaction amount to be loaded to or unloaded from the Prepaid Card account.

Req T275: ~~If a~~ [an EMV Card Payment Application or a \(Mobile\) Remote Card Payment Application is used to process](#) 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 [Payment Card](#) Application during the Prepaid Card - Loading & Unloading shall be set to zero to avoid unnecessary Card Risk Management.

4.6.3.4.7.3.3 AccountCard Data Retrieval

Req T276: After the AccountCard Data Retrieval Function has obtained either the relevant Card Data (e.g., the Track 2 equivalent data), or the PAN together with the eExpiry dDate, the Card-Acceptor may decide to raise a fee for the Prepaid Card - Loading & Unloading Service.

The Customercardholder shall be informed of any fee to be paid to the card Aacceptor for the Prepaid Card - Loading & Unloading and the Customercardholder shall have the opportunity to accept or decline the conditions of the Prepaid Card - Loading & Unloading.

4.6.3.4.7.3.4 Authorisation

Req T277: Prepaid Card - Loading & Unloading transactions shall be authorised online and shall be identified as Prepaid Card - Loading & Unloading.

Req T278: The authorisation message shall identify the amount to be loaded or unloaded and any fee raised by the card acceptor as an additional amount.

4.6.3.4.7.3.5 Data Capture

Req T279: Data Capture for "Financial Presentment" is required only if the card Aacceptor raises a fee for the Prepaid Card - Loading & Unloading.

4.74.8 Additional Features

4.7.14.8.1 One-off Payment with Increased Amount

- Req T280: [One-off](#) Payment with Increased Amount shall be restricted to the [One-off](#) Payment Service at the attended Physical POI.
- Req T281: Any extra amount shall be included in the transaction amount before or during Transaction Initialisation.
- Req T282: The extra amount shall be displayed separately for transaction confirmation and printed on the receipt, if any.

4.7.24.8.2 One-off Payment with Cashback

- Req T283: All requirements applicable to the [One-off](#) Payment Service shall also apply to [One-off](#) Payment with Cashback. Requirements that are specific for [One-off](#) Payment with Cashback are listed below.
- Req T284: [One-off](#) Payment with Cashback shall be restricted to the [One-off](#) Payment Service at the attended Physical POI.
- Req T285: For a [One-off](#) Payment with Cashback, the transaction amount shall be the sum of the payment amount and the Cashback amount.
- Req T286: The Cashback amount shall be identified separately in the authorisation and settlement messages.
- Req T287: For a [One-off](#) Payment with Cashback transaction, the Cashback amount to be confirmed shall be displayed to the [CustomerCardholder](#) 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 T288: [CustomerCardholder](#) confirmation of the Cashback amount shall be implicit with the confirmation of the transaction amount.
- Req T289: For attended POIs that support [One-off](#) Payment with Cashback, it shall be possible to configure per Application Profile to support the addition of a Cashback amount or not.

- Req T290: For attended POIs that support [One-off](#) Payment with Cashback, it shall be possible to configure per Application Profile a maximum Cashback amount.
- Req T291: For attended POIs that support [One-off](#) Payment with Cashback, it shall be possible to configure whether the POI Application supports magnetic stripe processing for [One-off](#) Payment with Cashback.
- Req T292: [One-off](#) Payment with Cashback transactions shall be authorised online.
- Req T293: The POI Application shall support handling of an authorisation response indicating the payment part is authorised but the Cashback is not.
- Req T294: If a receipt is printed for a [One-off](#) Payment with Cashback transaction, then in addition to the data listed in Req T94 the following data shall also be printed:
- Payment amount
 - Cashback amount

4.7.34.8.3 One-off Payment with Purchasing or Corporate Card Data

- Req T295: For a POI Application that supports [One-off](#) Payment with Purchasing or Corporate Card Data it shall be configurable per Application Profile whether this additional feature is activated for [One-off](#) Payment.
- Req T296: If a POI Application supports [One-off](#) 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 T297: If a [One-off](#) Payment transaction is performed with Card Data for which the [One-off](#) Payment with Purchasing or Corporate Card Data is activated in the POI Application, the additional data required for clearing of [One-off](#) Payments with Purchasing or Corporate Card Data shall be stored and captured at the POI.

4.7.44.8.4 One-off Payment with Aggregated Amount

- Req T298: When batch capture is used, if allowed by scheme rules, the [One-off](#) Payment transactions may be aggregated by the acceptor before sending the transactions to the acquirer for capture.
- Req T299: When online capture methods are used, if allowed by scheme rules, only the Acquirer may aggregate the [One-off](#) Payment transactions.
- Req T300: The maximum amount of the aggregated [One-off](#) Payment transactions shall be defined by Scheme rules.
- Req T301: ~~(Mobile)~~ EMV [Card](#) Payment Application and (M~~obile~~) [Remote Card Payment](#) Application based [One-off](#) Payment transactions shall be aggregated separately from [One-off](#) Payment transactions based on other Acceptance Technologies.
- Req T302: For aggregated ~~(Mobile)~~ EMV [Card](#) Payment Application or (M~~obile~~) [Remote Card Payment](#) Application based [One-off](#) Payment transactions, the cryptogram of the last aggregated transaction shall be sent together with the data elements used to calculate it.
- Req T303: The aggregation can only be made for the [One-off](#) 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.

4.7.54.8.5 One-off Payment with Deferred Authorisation

- Req T304: With the exception of Completion and Data Capture, all requirements applicable to the [One-off](#) Payment Service shall also apply to [One-off](#) Payment with Deferred Authorisation. Requirements that are specific for [One-off](#) Payment with Deferred Authorisation are listed below.
- Req T305: [One-off](#) Payment with Deferred Authorisation shall be restricted to the [One-off](#) Payment Service at the Physical ~~or Virtual~~ POI.
- ~~Req T306: It shall be possible for the attendant or the sale system to request the subsequent [One-off](#) Payment or [One-off](#) Payments to be performed with Deferred Authorisation.~~
- ~~Req T307: It shall be configurable whether all [One-off](#) Payments are performed with Deferred Authorisation.~~
- ~~Req T308: It shall be configurable whether Deferred Authorisation, in case unable to go online is detected during a [One-off](#) Payment transaction, is not initiated, or is initiated automatically, or is only initiated ~~on after request of a~~ confirmation by an Attendant.~~

- Req T309: It shall be configurable which of the Acceptance Technologies supported for [One-off](#) Payment are allowed for Deferred Authorisation.
- ~~Req T307: It shall be configurable whether Deferred Authorisation is initiated automatically or only on request of an attendant.~~
- Req T310: It shall be possible to activate/deactivate Deferred Authorisation for [One-off](#) Payment per Application Profile.
- Req T311: A minimum and a maximum amount for [One-off](#) Payment with Deferred Authorisation shall be configurable per Application Profile.
- Req T312: It shall be configurable per Application Profile which of the CVMs supported for [One-off](#) Payment are allowed for Deferred Authorisation. Online PIN shall never be allowed for [One-off](#) Payment with Deferred Authorisation.
- Req T313: It shall be configurable per Application Profile whether Deferred Authorisation shall only be allowed for [Payment Card](#) Application based transactions if Offline Data Authentication was successfully performed.
- Req T314: For POIs that support [One-off](#) 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 [One-off](#) Payment transaction shall be authorised online but the POI is (temporarily) unable to go online and the transaction is not authorised offline by an [EMV Card Payment](#) Application.
- If necessary according to the Application Profile configuration, confirmation of an attendant shall be requested for Deferred Authorisation.
- Req T315: 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 [One-off](#) Payment transaction shall be performed. Note that if configured for the Completion function this process may include forcing acceptance by an attendant.
- Req T316: If Deferred Authorisation can be performed according to the Application Profile configuration, Completion of an approved transaction shall be performed for the [Customer cardholder](#) (display and receipt, if any).
- Req T317: 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 an [\(Mobile\) EMV Card Payment](#) Application or [\(Mobile\) Remote Card Payment](#) 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 T318: If Deferred Authorisation has been performed for an ~~an (Mobile)~~ EMV Card Payment Application or (M~~obile~~) Remote Card Payment 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.

4.7.64.8.6 Dynamic Currency Conversion (DCC)

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

Req T319: It shall be configurable per Application Profile, whether DCC is supported.

Req T320: To perform DCC, the POI or attendant shall give the ~~Customer~~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 One-off Payment, the ~~Customer~~cardholder shall be informed of

- The original transaction amount in the card acceptor's currency,
- The transaction amount in the cardholder billing currency,
- The conversion rate (ratio) used to calculate the amount in the cardholder billing currency and
- The total currency conversion charges as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB).

Req T321: If the POI is used to offer the choice to the ~~Customer~~cardholder the following items shall be displayed to the ~~Customer~~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,
- The conversion rate (ratio) between these two amounts and
- The total currency conversion charges as a percentage mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB),

And the ~~Customer~~cardholder shall have the opportunity to select the currency the transaction will be performed in.

- Req T322: If the [Customercardholder](#) 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 T323: If the [Customercardholder](#) has selected the transaction amount in the cardholder billing currency, the amounts shall be conveyed to the [Customercardholder](#) in both the cardholder billing currency and the card acceptor's currency. The conversion rate used and the mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB) shall also be included.
- Req T324: If the [Customercardholder](#) 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 and the mark-up over the latest available euro foreign exchange reference rates issued by the European Central Bank (ECB) shall also be included.
- Req T325: If for a Contact EMV [Card](#) Payment Application or (M**obile**) [Remote Card Payment](#) Application based transaction, data from the Contact EMV [Card](#) Payment Application or (M**obile**) [Remote Card Payment](#) 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 [Customercardholder](#) has selected the transaction amount in the cardholder billing currency, then the Contact EMV [Card](#) Payment Application or (M**obile**) [Remote Card Payment](#) Application based transaction shall be re-started without further [Customercardholder](#) interaction with the previously selected [Payment Application](#).

4.7.74.8.7 Surcharging/Rebate

- Surcharging/Rebate is an additional feature which may be used for [One-off](#) Payment and Cash Services.
- Req T326: For [the One-off](#) Payment Services, any kind of surcharge/rebate shall be part of the agreed total sales amount.⁷⁸
- Req T327: If a surcharge/rebate is applied at the ATM for a Cash Withdrawal, the surcharge/rebate shall be displayed to the [Customercardholder](#) prior to authorisation, and the [Customercardholder](#) shall have the opportunity to abort

⁷⁸ Note that surcharging/rebate is subject to scheme or legal regulations.

the transaction or to continue with the understanding of a surcharge/rebate being applied.

Req T328: For a Cash Withdrawal with surcharge/rebate, the transaction amount shall be the total of the withdrawal amount and the surcharge/rebate amount.

5 **PROTOCOL FUNCTIONAL REQUIREMENTS FOR CARD TRANSACTIONS**

This section defines core functional requirements for Volume conformance for [Card Transaction](#) 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" ...) [for Card Transactions](#).

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 42: POI CONNECTED DIRECTLY TO AN ACQUIRER HOST

POI directly connected to several acquirers:

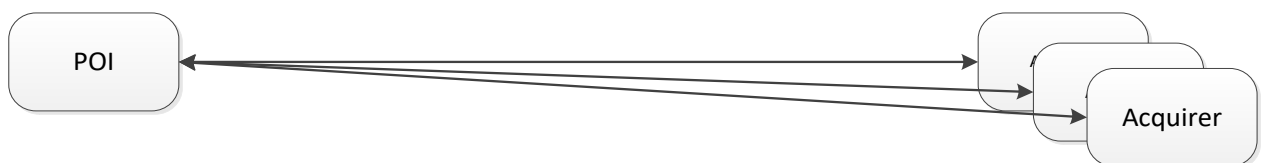


FIGURE 43: POI DIRECTLY CONNECTED TO SEVERAL ACQUIRERS

Environment of large retailer:

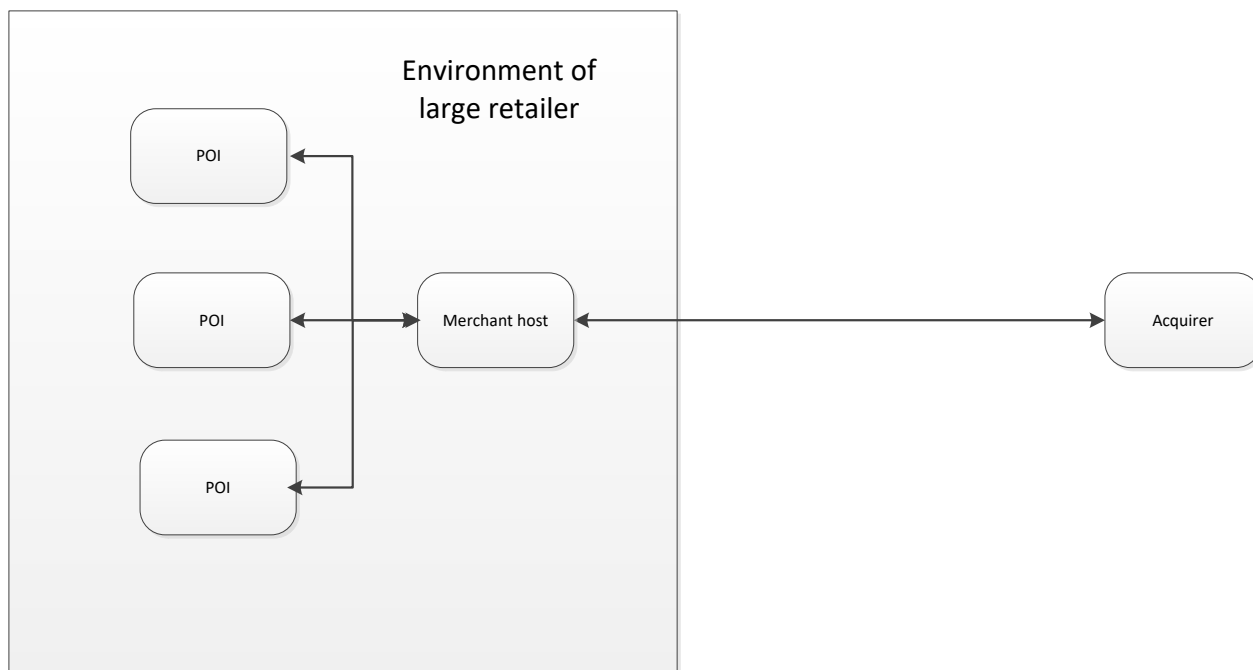


FIGURE 44: ENVIRONMENT OF LARGE RETAILER

Environment of a terminal provider:

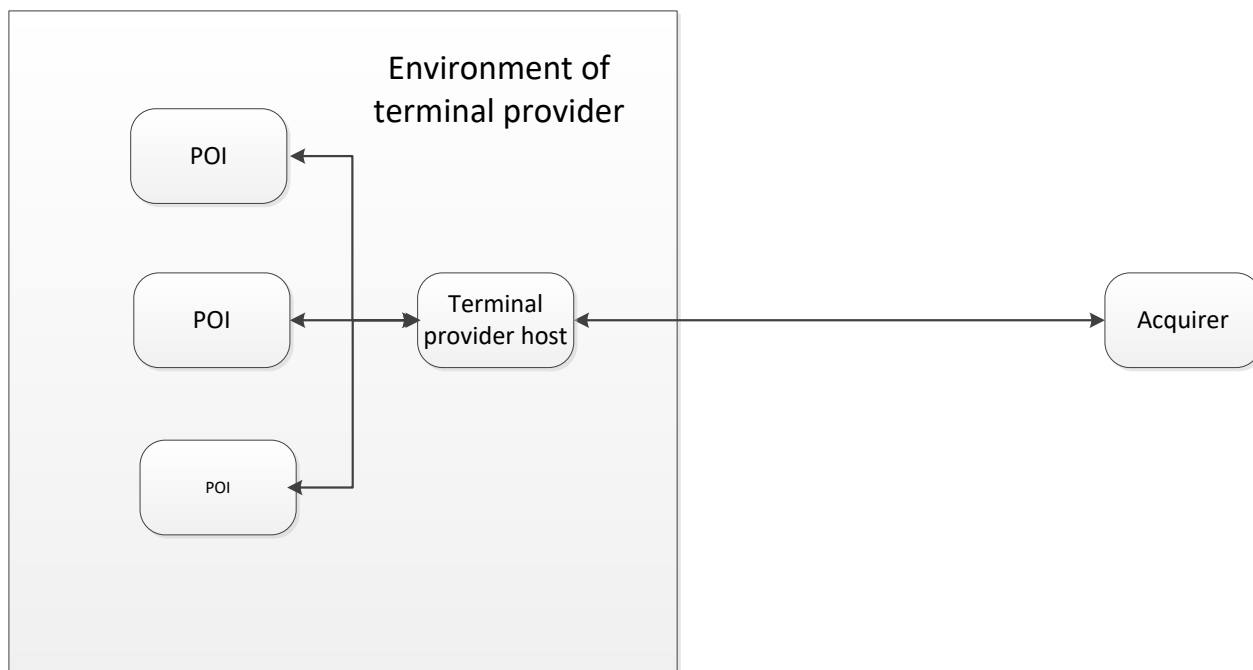


FIGURE 45: ENVIRONMENT OF A TERMINAL PROVIDER

Environment with an intermediate agent:

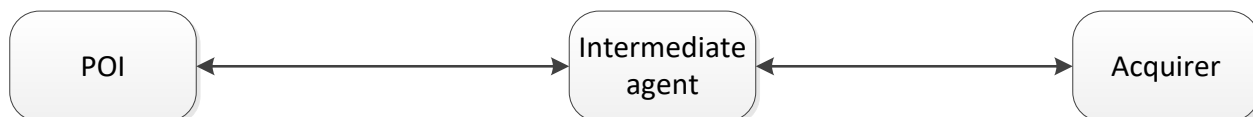


FIGURE 46: ENVIRONMENT WITH AN INTERMEDIATE AGENT

Intermediate host connected to several acquirers:

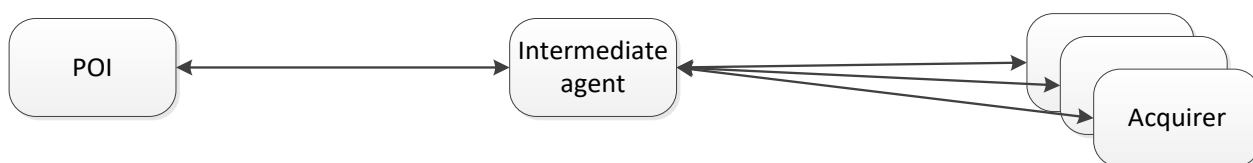


FIGURE 47: INTERMEDIATE HOST CONNECTED TO SEVERAL ACQUIRERS

- Req P1: The T2A protocols shall support the [PaymentCard](#) 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

Table 1: Usage of Acceptance Environments and Payment Devices for Local Transactions	12
Table 2: Usage of Acceptance Environments and Payment Devices for Remote Transactions	14
Table 3: Categorisation of Services by AIT and Customer Present Transaction	15
Table 4: Book 2 Scope	21
Table 5: Mapping of Acceptance Technologies to Payment Devices	22
Figure 6: POI Application - Logical Structure and Configuration Parameters	35
Table 7: One-off Payment: Acceptance Technologies and Acceptance Environments	81
Table 8: Functions used for One-off Payment	82
Table 9: Refund: Acceptance Technologies and Acceptance Environments	87
Table 10: Functions used for Refund	88
Table 11: Cancellation: Acceptance Technologies and Acceptance Environments	91
Table 12: Functions used for Cancellation	92
Table 13: Pre-Authorisation Services: Acceptance Technologies and Acceptance Environments	96
Table 14: Functions used for Pre-Authorisation and Update Preauthorisation	97
Table 15: Functions used for Payment Completion	102
Table 16: Deferred Payment: Acceptance Technologies and Acceptance Environments	104
Table 17: Functions used for Deferred Payment	105
Table 18: No-Show: Acceptance Technology and Acceptance Environments	108
Table 19: Functions used for No-Show	109
Table 20: Instalment Payment: Acceptance Technologies and Acceptance Environments for First Transaction	111
Table 21: Functions used for first Transaction of an Instalment Payment	112

Table 22: Functions used for Subsequent Transactions of an Instalment Payment	114
Table 23: Recurring Payment: Acceptance Technologies and Acceptance Environments for First Transaction	116
Table 24: Functions used for First Transaction of a Recurring Payment	117
Table 25: Functions used for Subsequent Transactions of a Recurring Payment	119
Table 26: Quasi-Cash Payment: Acceptance Technologies and Acceptance Environments	121
Table 27: Functions used for Quasi-Cash Payment	122
Table 28: ATM Cash Withdrawal: Acceptance Technologies and Acceptance Environments	124
Table 29: Functions used for ATM Cash Withdrawal	125
Table 30: Cash Advance: Acceptance Technologies and Acceptance Environments	128
Table 31: Functions used for Cash Advance	129
Table 32: Card Validity Check: Acceptance Technologies and Acceptance Environments	132
Table 33: Functions used for Card Validity Check	133
Table 34: Balance Enquiry: Acceptance Technologies and Acceptance Environments	134
Table 35: Functions used for Balance Enquiry	135
Table 36: Card Funds Transfer: Acceptance Technologies and Acceptance Environments	138
Table 37: Functions used for Card Funds Transfer	139
Table 38: Original Credit: Acceptance Technologies and Acceptance Environments	141
Table 39: Functions used for Original Credit	142
Table 40: Prepaid Card Loading: Acceptance Technologies and Acceptance Environments	145
Table 41: Functions used for Prepaid Card - Loading & Unloading	146
Figure 42: POI connected directly to an acquirer host	155
Figure 43: POI directly connected to several acquirers	155

Figure 44: Environment of large retailer	156
Figure 45: Environment of a terminal provider	157
Figure 46: Environment with an intermediate agent	157
Figure 47: Intermediate host connected to several acquirers	157