

**SEPA PAYMENTS STANDARDISATION (SPS) "VOLUME"****STANDARDS' REQUIREMENTS****BOOK 2****FUNCTIONAL REQUIREMENTS***Payments and Cash Withdrawals in SEPA  
Applicable Standards and Conformance Processes*

© European Payments Stakeholders Group AISBL.

Any and all rights are the exclusive property of  
EUROPEAN PAYMENTS STAKEHOLDERS GROUP AISBL.

Abstract	This document contains the work on SEPA 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
10.01- 10.28	2023-2025	Working Versions towards v10.5
10.5	27.11.2025  (published in December 2025)	Public Consultation Release 10.5

## Table of Contents

0	<b>1</b>	<b>GENERAL</b>	<b>5</b>
1	1.1	Book 2 - Executive Summary	5
2	1.2	Description of Changes since the Last Version of Book 2	7
3	<b>2</b>	<b>SCOPE</b>	<b>8</b>
4	<b>3</b>	<b>FUNCTIONAL REQUIREMENTS FOR PAYMENT DEVICES</b>	<b>20</b>
5	3.1	Introduction	20
6	3.2	Electronic Product Identification	20
7	3.3	Local Customer Present Transactions	21
8	3.3.1	Chip with Contact	21
9	3.3.2	Chip and Mobile Contactless	22
10	3.3.3	Merchant-presented QR Code and Consumer-presented QR Code	24
11	3.4	Remote Customer Present Transactions	26
12	3.4.1	MOTO	26
13	3.4.2	e- and m-Commerce	26
14	<b>4</b>	<b>POI FUNCTIONAL REQUIREMENTS</b>	<b>28</b>
15	4.1	Introduction	28
16	4.2	Accessibility Requirements	30
17	4.3	General Requirements	31
18	4.3.1	POI Application	31
19	4.3.2	Configuration	37
20	4.3.3	Functions for Payment Service Processing	39
21	4.4	Basic Services	75
22	4.4.1	One-off Payment	75
23	4.4.2	Refund	81
24	4.4.3	Cancellation	84

25	4.4.4 Pre-Authorisation Services	88
26	4.4.5 Deferred Payment	97
27	4.4.6 No-Show	100
28	4.4.7 Instalment Payment	103
29	4.4.8 Recurring Payment	108
30	4.4.9 Quasi-Cash Payment	114
31	4.5 Cash Services	117
32	4.5.1 ATM Cash Withdrawal	117
33	4.5.2 Cash Advance (Attended)	120
34	4.6 Card Enquiry Services	123
35	4.6.1 Card Validity Check	123
36	4.6.2 Balance Enquiry	125
37	4.7 Card Electronic Transfer	129
38	4.7.1 Card Funds Transfer	129
39	4.7.2 Original Credit	133
40	4.7.3 Prepaid Card - Loading & Unloading	136
41	4.8 Additional Features	140
42	4.8.1 One-off Payment with Increased Amount	140
43	4.8.2 One-off Payment with Cashback	140
44	4.8.3 One-off Payment with Purchasing or Corporate Card Data	141
45	4.8.4 One-off Payment with Aggregated Amount	142
46	4.8.5 One-off Payment with Deferred Authorisation	142
47	4.8.6 Dynamic Currency Conversion (DCC)	144
48	4.8.7 Surcharging/Rebate	145
49	<b>5 PROTOCOL FUNCTIONAL REQUIREMENTS FOR CARD TRANSACTIONS</b>	<b>146</b>
50	<b>ANNEX 1 - FIGURES AND TABLES</b>	<b>150</b>
51		
52		

## 1 GENERAL

### 1.1 Book 2 - Executive Summary

This book defines functional requirements for Local and Remote Payment Transactions for the provision of the 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 Payment Services,

- ⇒ Involve, in general, a 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 Customer and the Acceptor interact using a particular *Payment Device* within a particular *Acceptance Environment* supporting *Authentication Methods*;

- ⇒ Are processed through a succession of *Functions* which may be executed in the Payment 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 for Local and Remote Transactions

**Table 4:** Book 2 Scope

**Table 5:** Mapping of Acceptance Technologies to Payment Devices

Section 3 defines core functional requirements for Payment Devices.

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.

- 84 References, definitions of terms and abbreviations are provided in Book 1.
- 85 Note: Payment Device and POI Application implementations may support additional functionality,
- 86 provided they do not conflict with the Volume requirements.

Public Consultation Draft

## 87    **1.2    Description of Changes since the Last Version of Book 2**

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

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

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

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

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

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

119

## 2 SCOPE

This Volume differentiates between Local and Remote Transactions.

- A **Local Transaction** is a Card or ICT Transaction initiated and completed<sup>1</sup> at the Acceptor's Physical POI which may be Attended (including Semi-Attended) or Unattended.

A Local Transaction is usually performed with the participation of the Customer using a Payment Device. In this case the Local Transaction is defined as a Local Customer Present Transaction.

When a transaction is performed by the Acceptor based on Stored 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 AIT<sup>2</sup>.

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.

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

<sup>1</sup> Completed refers to the Completion Function described in Section 4.3.3.8.

<sup>2</sup> Examples of Payment 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.



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 Transaction** is a Card or ICT Transaction initiated and completed<sup>1</sup> at the Acceptor's Virtual POI or, only for MOTO, at a Virtual Terminal or Physical POI configured to perform MOTO transactions.

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

- **e- and m-Commerce** Transactions are initiated by the Customer using a Consumer Device and are conducted via a Virtual POI over the internet.

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

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

- **MOTO** transactions are conducted in the Acceptor's environment using Manual Entry with the Customer interacting remotely for MOTO.

A Physical POI, configured to handle MOTO transactions or a Virtual Terminal may be used to process the Account Data for MOTO. When a transaction is performed by the Acceptor based on Stored 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 AIT<sup>2</sup>.

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 AIT<sup>2</sup> or as Customer 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, is shown in the following Table 1 for Local Transactions and Table 2 for Remote Transactions. Table 3 indicates for every Payment Service if it may be processed as a Customer Present transaction or as an Acceptor Initiated Transaction (AIT) and, if so, whether it is an MIT.

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

**TABLE 1:** USAGE OF ACCEPTANCE ENVIRONMENTS AND PAYMENT DEVICES FOR LOCAL TRANSACTIONS

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

<sup>4</sup> For attended POI, the Attendant operates the POI on behalf of the Customer.

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

<sup>6</sup> 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.

<sup>8</sup> Also referred to as Stored Card Data for Card Transactions.

Acceptance Environments:	Physical POI		Remote POI			
	Attended POI		Virtual Terminal		Virtual POI	
<b>Initiated by:</b>	Customer <sup>4 9</sup>	Acceptor <sup>5 6</sup>	Customer <sup>10 9</sup>	Acceptor <sup>5 6</sup>	Customer	Acceptor <sup>5 6</sup>
<b>Type of Transaction:</b>	MOTO in an Acceptor attended environment.	Remote AIT	MOTO	Remote AIT	e- & m-Commerce	Remote AIT
<b>Payment Device:</b>	Physical Card or Virtual Card	no Payment Device involved <sup>5</sup>	Physical Card or Virtual Card	no Payment Device involved <sup>5</sup>	Consumer Device <sup>11</sup>	no Payment Device involved <sup>5</sup>
<b>Acceptance Technologies:</b>	Manual Entry by Acceptor	Stored Account Data (Stored by Acceptor) <sup>5</sup>	Manual Entry by Acceptor or by Customer <sup>10</sup>	Stored Account Data (Stored by Acceptor) <sup>5</sup>	Consumer Device with Browser over Internet <sup>12</sup> , Consumer Device with Dedicated Application over Internet	Stored Account Data (Stored by Acceptor) <sup>5</sup>

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

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

<sup>10</sup> The Attendant operates the POI on behalf of the Customer, except the Customer uses DTMF.

<sup>11</sup> 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.

<sup>12</sup> 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.

Services	AIT (MIT)	AIT (Acceptor as Payer)	Customer Present Transaction <sup>4</sup>
One-off Payment	N	N	Y
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			
Refund (partial or total)	N	Y	Y
Cancellation			
Original Credit			
Pre-Authorisation Services	Y	N	Y
Card Validity Check			
No-Show	Y	N	N
Instalment Payment - Subsequent transactions			
Recurring Payment - Subsequent transactions			

**TABLE 3: CATEGORISATION OF SERVICES BY AIT AND CUSTOMER PRESENT TRANSACTION**

**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"):

- ⇒ Payment Services
- ⇒ Payment Devices and Acceptance Environments
- ⇒ Acceptance Technologies
- ⇒ Authentication Methods
- ⇒ Functions

Definitions of the different Payment Services, Payment Devices, Acceptance Environments, Acceptance Technologies, Authentication Methods, and Functions are provided in Book 1.

	SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
<b>PAYMENT SERVICES</b>				
<b>BASIC SERVICES</b>				
One-off Payment	Y	Y	Y	Y
Refund (partial or total)	Y	Y	N/A	N/A
Cancellation	Y	Y	N/A	N/A
Pre-Authorisation Services <ul style="list-style-type: none"> <li>Pre-Authorisation</li> <li>Update Pre-Authorisation</li> <li>Payment Completion</li> </ul>	Y	Y	N/A	N/A
Deferred Payment	Y	N	N/A	N/A
No-Show	Y	Y	N/A	N/A
Instalment Payment	Y	Y	N/A	N/A
Recurring Payment	Y	Y	N/A	N/A
Quasi-Cash Payment	Y	Y	N/A	N/A
<b>CASH SERVICES</b>				
ATM Cash Withdrawal	Y	N	N/A	N/A
Cash Advance (Attended)	Y	N	N/A	N/A
Cash Deposit	N/A	N/A	N/A	N/A
<b>CARD ENQUIRY SERVICES</b>				
Card Validity Check	Y	Y	N/A	N/A
Balance Enquiry	Y	N/A	N/A	N/A
<b>CARD ELECTRONIC TRANSFER OF FUNDS</b>				
Card Funds Transfer	Y	Y	N/A	N/A
Original Credit	Y	Y	N/A	N/A
Prepaid Card - Loading & Unloading	Y	Y	N/A	N/A
e-Purse - Loading/Unloading	N/A	N/A	N/A	N/A
<b>ADDITIONAL FEATURES</b>				
One-off Payment with Increased Amount	Y	N	N/A	N/A
One-off Payment with Cashback	Y	N	N/A	N/A
One-off Payment with Purchasing or Corporate Card Data	Y	Y	N/A	N/A
One-off Payment with Aggregated Amount	Y	Y	N/A	N/A
One-off Payment with Deferred Authorisation	Y	Y	N/A	N/A

	SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
Dynamic Currency Conversion (DCC)	Y	Y	N/A	N/A
Surcharging/Rebate	Y	Y	N/A	N/A
Payment with Deferred Clearing	N/A	N/A	N/A	N/A
Payment with Loyalty Information	N/A	N/A	N/A	N/A
Unsolicited Available Funds	N/A	N/A	N/A	N/A
<b>CARD MANAGEMENT SERVICES</b>				
PIN Change / Unlock	N/A	N/A	N/A	N/A
Card Activation	N/A	N/A	N/A	N/A
Return Card to Cardholder Request	N/A	N/A	N/A	N/A
Card Pick-up Advice	N/A	N/A	N/A	N/A
Return Card Advice	N/A	N/A	N/A	N/A
<b>ACCEPTANCE TECHNOLOGIES</b>				
Chip with Contact	Y	N	Y <sup>14</sup>	N
Magnetic Stripe	Y	N	N	N
Chip Contactless <sup>15</sup>	Y	N	Y <sup>14</sup>	N
Mobile Contactless <sup>15</sup>	Y	N	Y <sup>16</sup>	N
Manual Entry by Acceptor <sup>17</sup>	Y	Y <sup>18</sup>	N	N
Manual Entry by Customer	N	Y <sup>19</sup>	N	N
Stored Account Data (stored by the Acceptor)	Y <sup>20</sup>	Y <sup>20</sup>	N/A <sup>21</sup>	N/A <sup>21</sup>

<sup>14</sup> This Acceptance Technology may only be used for EMV based ICT Transactions.

<sup>15</sup> If it is not necessary to distinguish the Payment Device 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.

<sup>16</sup> 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.

<sup>17</sup> Acceptor may also stand for an Attendant in the Acceptor's environment.

<sup>18</sup> Only applicable to MOTO.

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

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

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

	SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
Consumer Device with Browser over Internet	N	Y	N	Y
Consumer Device with Dedicated Application over Internet	N	Y	N	Y
Merchant-presented QR Code	N/A	N <sup>22</sup>	Y	N <sup>22</sup>
Consumer-presented QR Code	N/A	N	Y	N
Imprint	N	N	N	N
<b>PAYMENT DEVICES</b>				
Physical Card	Y	Y	Y <sup>23</sup>	N
Consumer Device	Y <sup>24</sup>	Y	Y	Y
Virtual Card	N	Y	N	N
<b>ACCEPTANCE ENVIRONMENTS</b>				
Physical POI				
Attended <sup>3</sup>	Y	Y <sup>26</sup>	Y	N/A <sup>27</sup>
Unattended	Y	N	Y	N
Remote POI				
Virtual POI	N	Y <sup>28</sup>	Y	Y
Virtual Terminal	N	Y <sup>26</sup>	N	N

<sup>22</sup> 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.

<sup>23</sup> This Payment Device may only be used for EMV based ICT Transactions.

<sup>24</sup> Using a Mobile Device for Mobile Contactless.

<sup>26</sup> Only for MOTO and AIT, not applicable to e- and m-commerce.

<sup>27</sup> 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.

<sup>28</sup> Not applicable to MOTO.



		SPS Volume Book 2 Scope			
		Card Transactions		ICT Transactions	
		Local	Remote	Local	Remote
<b>AUTHENTICATION METHODS</b> (SCA factor-based classification: K = Knowledge, P = Possession, I = Inherence)					
Offline Plaintext PIN <sup>29, 30</sup>	K	Y	N	Y <sup>31</sup>	N
Offline Enciphered PIN <sup>29, 32</sup>	K	Y	N	Y <sup>31</sup>	N
Online PIN	K	Y	N	Y <sup>31</sup>	N
Signature	<sub>33</sub>	Y	N <sup>34</sup>	N	N
No CVM Required <sup>35</sup>	-	Y	Y <sup>35</sup>	Y <sup>31 35</sup>	Y <sup>35</sup>
Offline Biometric Verification <sup>29</sup>	I	Y	N	Y <sup>31</sup>	N
Biometrics via Sensor on Card	I	Y	Y <sup>36</sup>	Y <sup>31</sup>	Y <sup>31 36</sup>
Biometrics on Consumer Device (CDCVM) <sup>37 38</sup>	I	Y	Y	Y	Y
Offline Mobile Code (CDCVM) <sup>37 38</sup>	K	Y	Y	Y	Y
Online Mobile Code	K	N	Y	Y	Y
Offline Personal Code (CDCVM) <sup>37 38</sup>	K	N	Y	N	Y
Online Personal Code	K	N	Y	N	Y
SDA <sup>29</sup>	P <sup>33</sup>	Y	N	N	N
DDA	P	Y	N	N	N
CDA	P	Y	N	Y <sup>31</sup>	N
fDDA <sup>39</sup>	P	Y	N	N	N

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

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

<sup>31</sup> This Cardholder Verification Method may only be used for EMV based ICT Transactions.

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

<sup>33</sup> Still in use for Local Card Transactions, but not an SCA factor.

<sup>34</sup> However, a mail order form contains a cardholder signature.

<sup>35</sup> No CVM Required is a defined CVM for EMV technology, else it stands for "SCA Exemption allowed", e.g. based on Risk-Based Authentication or cases where SCA is not required (see Section 4.3.3.5).

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

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

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

<sup>39</sup> Only applicable to the Contactless Acceptance Technologies.

		SPS Volume Book 2 Scope			
		Card Transactions		ICT Transactions	
		Local	Remote	Local	Remote
XDA	P	Y <sup>40</sup>	N	Y <sup>31</sup>	N
BDHLA	P	Y <sup>39</sup>	N	Y <sup>31</sup>	N
EMV Online Authentication	P	Y	Y <sup>41</sup>	Y <sup>31</sup>	Y <sup>41</sup>
Static Authentication <sup>42</sup>	P <sup>43</sup>	Y	Y	N	N
Dynamic Authentication - One Time Password (OTP) <sup>44</sup>	P	N	Y	Y	Y
Dynamic Authentication - Challenge Response based on Additional Authentication Device <sup>45</sup>	P	N	Y	N	Y
Dynamic Authentication - Challenge Response based on Authentication/(Remote) Payment Application on a Consumer Device <sup>44</sup>	P	N	Y	Y (for Mobile Device)	Y
<b>FUNCTIONS</b>					
Configuration		Y	Y	Y	Y
Transaction Initialisation		Y	Y	Y	Y
Language Selection		Y	Y	Y	Y
Selection of the Payment Solution		Y	Y	Y	Y
Account Data Retrieval		Y	Y	Y	Y
Authentication		Y	Y	Y	Y
Authorisation		Y	Y	Y	Y
Referral		Y	N	N	N
Completion		Y	Y	Y	Y
Reversal		Y	Y	N/A	N/A
Data Capture		Y	Y	Y	Y
Financial Presentment		N/A	N/A	N/A	N/A
Settlement		N/A	N/A	N/A	N/A

<sup>40</sup> Only applicable to the Contact Acceptance Technology.

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

<sup>42</sup> Typically the Card Security Code (CSC) is used.

<sup>43</sup> Still in use for Remote Card Transactions, but not an SCA factor.

<sup>44</sup> This Authentication Method is used for e- and m-commerce and for conventional Local ICT Transactions.

<sup>45</sup> This Authentication Method may use EMV or FIDO authentication methods.

	SPS Volume Book 2 Scope			
	Card Transactions		ICT Transactions	
	Local	Remote	Local	Remote
Chargeback	N/A	N/A	N/A	N/A
<b>ADMINISTRATIVE SERVICE</b>				
Reconciliation	N/A	N/A	N/A	N/A

TABLE 4: BOOK 2 SCOPE

Table 5 shows which Acceptance Technologies can be used in combination with the Payment Devices.

ACCEPTANCE TECHNOLOGIES	PAYMENT DEVICES		
	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 <sup>49</sup>	N	N
Manual Entry by Customer	Y <sup>19</sup>	Y <sup>19</sup>	N
Stored Account Data (stored by the Acceptor) <sup>50</sup>	N/A	N/A	N/A
Consumer Device with Browser over Internet	N	N	Y
Consumer Device with Dedicated Application over Internet	N	N	Y
Merchant-presented QR Code	N	N	Y
Consumer-presented QR Code	N	N	Y

TABLE 5: MAPPING OF ACCEPTANCE TECHNOLOGIES TO PAYMENT DEVICES

<sup>49</sup> If used for Local Transactions or MOTO.

<sup>50</sup> For the Acceptance Technology Stored Account Data, Account Data, e.g. PAN and expiry date for Card Transactions, will have been provided earlier. Therefore no Payment Device is involved, which is denoted as "N/A".

## 3 FUNCTIONAL REQUIREMENTS FOR PAYMENT DEVICES

### 3.1 Introduction

This section defines core functional requirements for Volume conformance for Payment Devices 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.

### 236 **3.3 Local Customer Present Transactions**

237 The Payment Device used for Local Customer Present Transactions, is a Physical Card or a  
 238 Consumer Device<sup>51</sup>. Functional requirements for Payment Applications are defined in Section  
 239 3.3.1 for the Acceptance Technology Chip with Contact, in Section 3.3.2 for the Acceptance  
 240 Technologies Chip Contactless and Mobile Contactless and in Section 3.3.3 for the Acceptance  
 241 Technologies Merchant-presented QR Code and Consumer-presented QR Code.

#### 242 **3.3.1 Chip with Contact**

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

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

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

255 Req C2: Physical Cards shall support Application Selection through PSE according to [EMV  
 256 B1]<sup>52</sup>.

257 Req C3: Contact EMV Card Payment Applications shall include the Language Preference  
 258 data element.

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

---

<sup>51</sup> Using the Mobile Device for Mobile Contactless

<sup>52</sup> 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.

261 Req C28: For Contact EMV Card Payment Applications used for Card Transactions, the PSE  
 262 and FCI shall include the Application Selection Registered Proprietary Data. The  
 263 Application Selection Registered Proprietary Data with ID = '0001' shall be present:

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

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

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

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

278 Req C5: Contact EMV Card Payment Applications shall support EMV Online Authentication.

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

- 281 • DDA is optional.
- 282 • CDA is mandatory.
- 283 • SDA is not permitted.

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

### 286 **3.3.2 Chip and Mobile Contactless**

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

291 The Payment Device used for Local Transactions with the Acceptance Technology Mobile  
 292 Contactless is a Mobile Device carrying a Mobile Contactless Payment (MCP) Application. Local

293 ICT Transactions for the Acceptance Technology Mobile Contactless are processed either as  
294 conventional ICT Transactions using a Mobile Contactless ICT Payment Application (see Figure 7  
295 in Section 1.8 of Book 1) or as EMV based ICT Transactions using a Mobile Contactless EMV Card  
296 Payment Application (see Figure 8 in Section 1.8 of Book 1).

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

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

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

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

306 Req C9: (Mobile) Contactless EMV Card Payment Applications used for Card Transactions  
307 shall allow identification of the Form Factor for use in authorisation and data  
308 capture.

309 Req C10: Physical Cards and Mobile Devices shall support Combination Selection through  
310 PPSE according to the card requirements in [EMV B] for all supported (Mobile)  
311 Contactless Payment Applications, including Mobile Contactless ICT Payment  
312 Applications.

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

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

318 Req C12: For (Mobile) Contactless EMV Card Payment Applications used for Card  
319 Transactions, the PPSE Entries and the FCI shall include the Application Selection  
320 Registered Proprietary Data.

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

- 323 • In every Directory Entry (tag '61') for (Mobile) Contactless EMV Card Payment  
324 Applications used for Card Transactions within the FCI of the PPSE,
- 325 • AND in the FCI Issuer Directory Discretionary data (tag 'BF0C') within the FCI of  
326 every ADF of such applications.

327 Req C13: Contactless EMV Card Payment Applications on Physical Cards that support  
328 Biometrics via Sensor on Card shall indicate this CVM to the POI as CDCVM.

329 Req C14: Mobile Contactless EMV Card Payment Applications that support Online Mobile  
330 Code shall indicate this CVM to the POI as CDCVM.

331 Req C21: For (Mobile) Contactless EMV Card Payment Applications that support ECC-based  
332 Offline Data Authentication, BDHLA is mandatory.

333 Req C29: Mobile Contactless ICT Payment Applications shall support processing as shown in  
334 Figure 7 (Open Banking-based ICT Transaction - Mobile Contactless with Mobile  
335 Contactless ICT Application) in Section 1.8 of Book 1.

### 336 **3.3.3 Merchant-presented QR Code and Consumer-presented QR Code**

#### 337 **3.3.3.1 Merchant-presented QR-Code**

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

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

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

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

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

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



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

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

### 370 3.3.3.2 Consumer-presented QR Code

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

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

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

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

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

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

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

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

400 Req C34: If a Mobile QR Code ICT Payment Application supporting multiple ICT Payment  
401 Brands is used to generate a standard Consumer-presented QR Code, the Payment  
402 Application shall allow the Customer to pre-select one or several of the Brands  
403 and to assign priorities to the Brands and shall generate a Consumer-presented QR  
404 Code indicating the pre-selected Brand(s) ordered according to the Customer's  
405 priorities. Req C35: If a Mobile QR Code ICT Payment Application displays the  
406 Consumer-presented QR Code, then it shall temporarily disable the contactless  
407 interface of the Mobile Device.

### 408 **3.4 Remote Customer Present Transactions**

#### 409 **3.4.1 MOTO**

410 In MOTO transactions, the Payment Device Physical Card or Virtual Card is used. MOTO  
411 transactions are always Card Transactions.

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

#### 414 **3.4.2 e- and m-Commerce**

415 The Payment Device used for e- and m-Commerce is a Consumer Device, where an Electronic  
416 Device is used for e-Commerce and a Mobile device is used for m-Commerce. The Acceptance  
417 Technologies used for e- and m-Commerce are Consumer Device with Dedicated Application  
418 over Internet and Consumer Device with Browser over Internet. ICT based e- and m-Commerce  
419 transactions are processed as shown in Figure 4 in Section 1.8 of Book 1. This implies, that from  
420 the Customer's perspective the functional steps of ICT based e- and m-Commerce transactions  
421 and Card based e- and m-Commerce transactions are very similar.

422 The Payment Device may be personalised with an (M)RP Application or with an Authentication  
423 Application. Entering Account Data on the Payment Device may also require the use of a Physical  
424 Card or a Virtual Card.

425 Req C23: If a (Mobile) Remote Payment Application, Payment Credentials or an  
426 Authentication Application is used, they shall be stored in a Secure Environment  
427 accessible via the Consumer Device.

428 Req C24: A (Mobile) Remote Payment Application or an Authentication Application shall  
429 support a Dynamic Authentication Method listed in **Table 4** and categorised as a  
430 possession factor.

- 431 Req C25: A (Mobile) Remote Payment Application or an Authentication Application shall  
432 support one of the following Authentication Methods listed in Table 4 and  
433 categorised as knowledge or inference factors: "Personal/Mobile Code" (online or  
434 offline) or "Biometrics on Consumer Device".
- 435 If an Additional Authentication Device is used with an EMV Card Authentication  
436 Application on a Physical Card, "Offline PIN" (knowledge factor) or "Offline  
437 Biometric Verification" (inherence factor) shall be supported as Authentication  
438 Methods by the EMV Card Authentication Application.
- 439 Req C26: Whether a Physical Card, a Virtual Card, Payment Credentials, or an  
440 Authentication / (M)RP Application is involved in a Remote Card Transaction shall  
441 be identifiable by the Issuer.
- 442 Req C27: Card Data entered for a Card based e- or m-Commerce transaction, shall include  
443 PAN, expiry date and Card Security Code (CSC).
- 444 Req C36: Account Data entered for an ICT based e- or m-Commerce transaction, shall  
445 include the identity of the Customer's ASPSP and, depending on how Customer  
446 authentication is performed (see Figure 4 in Section 1.8 of Book 1), also the  
447 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 Payment 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 contains general requirements that apply to Local Transactions (Physical POI) and/or 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 Payment 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 Payment 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).

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

- 477 • Allowed combinations of Acceptance Technologies and Acceptance Environments for  
478 each Payment Service.
- 479 • Applicability of the Functions for each Payment Service in the different Acceptance  
480 Environments.
- 481 • Payment Service dependent requirements for the POI Application and for Configuration, if  
482 any.
- 483 • Payment Service dependent requirements for the Functions that are applicable for  
484 processing the Payment Service as appropriate.

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

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

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

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

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

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

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

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

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

509 If it is not necessary to distinguish the Payment Device in use, the term "Contactless" is used to  
510 refer to both Acceptance Technologies, Chip Contactless and Mobile Contactless, because they  
511 are both implementations of [EMV L1 CL] and communication and behaviour are the same from  
512 the perspective of the POI.

513 The requirement T6 below provides for the usage of kernels according to [EMV C] as well as any  
514 other kernel that complies with [EMV A] and [EMV B].

#### 515 **4.2      Accessibility Requirements**

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

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

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

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

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

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

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

### 543 **4.3      General Requirements**

544 This section contains requirements that apply to Card Transactions for all or several Payment  
 545 Services and to ICT Transactions for One-off Payment. These requirements are grouped in  
 546 requirements for the POI Application (Section 4.3.1), for the Configuration Function (Section  
 547 4.3.2) and for the Functions used for Payment Service Processing (Section 4.3.3).

#### 548 **4.3.1      POI Application**

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

##### 552 **4.3.1.1      Local Transactions and Remote Transactions (all Acceptance Environments)**

553 Req T1:          The POI Application shall support processing with multiple Acquirers/PISPs.

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

##### 556 **4.3.1.2      Local Transactions (Physical POI)**

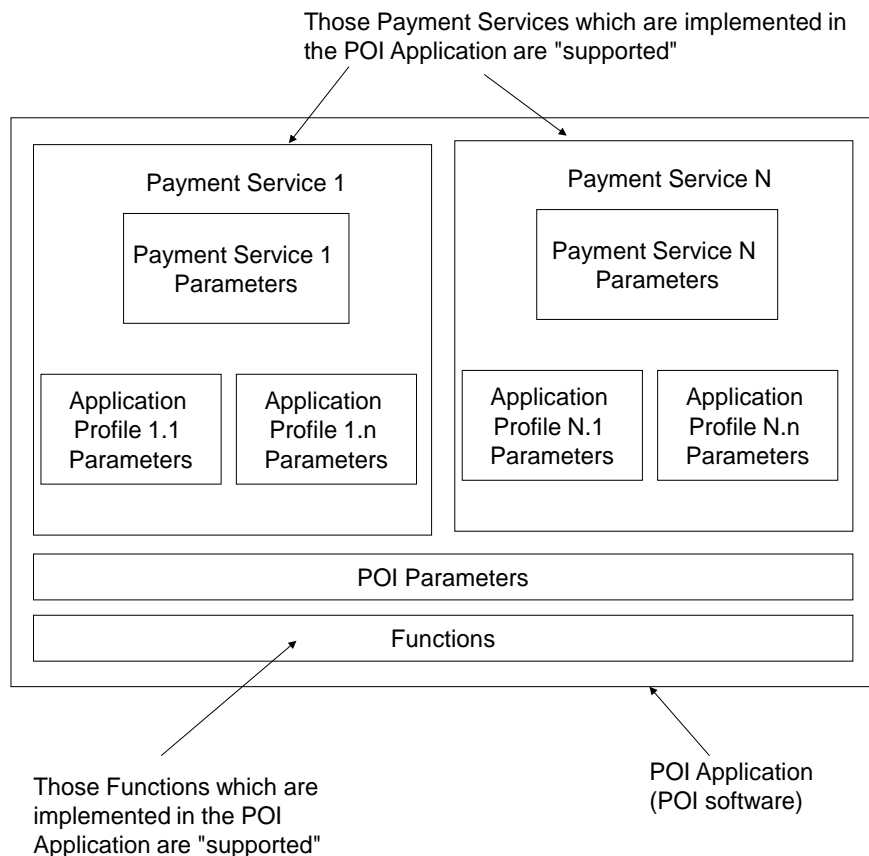
557 The following figure shows the logical relationship between the POI Application, the Payment  
 558 Services, the Functions and the configuration parameters:

- 559      • POI parameters configure the POI Application independently of the Payment Services,  
 560      e.g., define which of the supported Acceptance Technologies, Acceptance Environments,  
 561      Payment Services and Functions are available for transaction processing and which  
 562      Payment Brands and Payment Instruments are supported per Acceptance Technology.
- 563      • Payment Service parameters configure the Payment Service, e.g., define which of the  
 564      available Acceptance Technologies, Payment Brands and Payment Instruments are  
 565      allowed for a Payment Service.
- 566      • Application Profile parameters configure the Application Profile for a Payment Service, for  
 567      example:
  - 568          ○ define the limits to be used;



- restrict functionality for accepting EEA issued cards, 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 Req T54 and T56).



**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].



- 583 Req T329: The POI Application supporting the Chip with Contact Acceptance Technology for  
584 EMV based ICT Transactions shall support transaction processing according to  
585 Figure 8 in Section 1.8 of Book 1.
- 586 Req T5: The POI Application supporting the Contactless Acceptance Technology shall  
587 support and accept any contactless form factor according to [EMV L1 CL].
- 588 Req T6: The POI Application supporting the Contactless Acceptance Technology for EMV  
589 based Transactions (i.e. Card Transactions and/or EMV based ICT Transactions)  
590 shall support and comply with [EMV A] and [EMV B].
- 591 In particular, the POI Application supporting the Contactless Acceptance  
592 Technology for EMV based Transactions shall support Combination Selection  
593 through PPSE according to [EMV B] and at least one contactless kernel that  
594 complies with [EMV A] and [EMV B] to accept at least one (Mobile) Contactless  
595 EMV Card Payment Application.
- 596 Req T330: The POI Application supporting the Contactless Acceptance Technology for EMV  
597 based ICT Transactions shall support transaction processing according to Figure 8  
598 in Section 1.8 of Book 1.
- 599 Req T331: The POI Application supporting the Contactless Acceptance Technology for  
600 conventional ICT Transactions shall support Combination Selection through PPSE  
601 according to [EMV B] and at least one contactless kernel performing the  
602 communication with the Payment Application on the Payment Device according to  
603 steps 2. and 3. in Figure 7 in Section 1.8 of Book 1 to accept at least one Mobile  
604 Contactless ICT Payment Application.
- 605 Req T332: The POI Application supporting the Contactless Acceptance Technology for  
606 conventional ICT Transactions shall support transaction processing according to  
607 Figure 7 in Section 1.8 of Book 1.
- 608 Req T333: The POI Application supporting the Contactless Acceptance Technology for both,  
609 conventional ICT Transactions and EMV based Transactions shall support  
610 Combination Selection through PPSE in a uniform way for (Mobile) Contactless  
611 EMV Card Payment Applications and for Mobile Contactless ICT Payment  
612 Applications.
- 613 Req T334: The POI Application supporting the Merchant-presented QR Code Acceptance  
614 Technology (only for conventional ICT Transactions) shall support Selection of the  
615 Payment Brand as described in Section 4.3.3.3.2.3 and transaction processing  
616 according to Figure 5 in Section 1.8 of Book 1.
- 617 Req T335: The POI Application supporting the Consumer-presented QR Code Acceptance  
618 Technology (only for conventional ICT Transactions) shall support Selection of the  
619 Payment Brand as described in Section 4.3.3.3.2.3 and transaction processing  
620 according to Figure 6 in Section 1.8 of Book 1.

- 621 Req T7: The POI Application shall support at least a local language and English for the  
622 Customer display. English only is allowed if English is the local language.
- 623 Req T8: The POI Application shall support updating of displayable messages for Customer  
624 display languages.
- 625 Req T9: All POIs, attended and unattended, shall have mechanisms to ensure that only the  
626 authorised user can initiate the Payment Services Refund, Original Credit and  
627 Cancellation.
- 628 Req T10: For the unattended POI, independent of the level of integration with the sale  
629 system, the following communications shall be exchanged:
- 630 • Communication to request a transaction, including the transaction amount and  
631 Transaction Type if applicable, from the sale system to the POI Application.
  - 632 • Communication of the authorisation result, including authorised transaction  
633 amount if applicable, from POI Application to sale system.
  - 634 • In the event the final amount differs from the amount authorised, this event  
635 needs to be communicated from the sale system to the POI Application,  
636 including the final amount if needed to take the appropriate actions.
- 637 In addition the following communication should be supported by the unattended  
638 POI:
- 639 • Communication of presence of a Physical Card and, if the Contactless  
640 Acceptance Technology is supported, of a Mobile Device from POI Application  
641 to sale system.
- 642 Req T11: If the Chip with Contact Acceptance Technology has been tried and failed for a  
643 Card Transaction, and if subsequently, within the same transaction, Magnetic  
644 Stripe Acceptance Technology is tried, then the POI Application shall check the  
645 Application Profile configuration and, if applicable, whether the magnetic stripe  
646 data indicates that the Chip with Contact Acceptance Technology is supported, to  
647 determine, whether the magnetic stripe transaction is allowed and if it has to be  
648 considered as a fallback transaction (see Req T24).
- 649 Req T42: For attended POI, the messages for the Attendant shall be displayed in a local  
650 language.

651 4.3.1.3 Remote Transactions at the Virtual POI

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

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

658 It may also include

- 659     • A secure payment page where the Customer provides the relevant payment related data

660 Or

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

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

665 The Virtual POI may also facilitate redirection services to support "direct" remote authentication  
666 of the Customer by the Customer's ASPSP via a so-called Authentication server.

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

669 The payment page may be accessed by the Customer via a (mobile) browser or via a dedicated  
670 application on their Consumer Device.

671 A Virtual POI Application shall meet the requirements listed in this section.

672 Req T336: The Virtual POI Application supporting Remote ICT Transactions shall support  
673 transaction processing according to Figure 4 in Section 1.8 of Book 1.

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

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

679 Req T14: The Virtual POI Application shall use the Acceptor Name<sup>53</sup> on Customer displays.

680 Req T15: Refund, Original Credit and Cancellation Services shall be initiated by the Acceptor.  
681 These Payment Services shall never be initiated by the Customer.

682 Req T16: Refund, Original Credit and Cancellation Services shall have mechanisms to ensure  
683 that only the authorised user can initiate these Services.

684 **4.3.1.4 Remote Card Transactions at Physical POI and Virtual Terminal**

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

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

694 • For Mail Order transactions the Card Data and address data (as needed) are provided by  
695 the Cardholder in writing (e.g., by mail or fax or a chat facility) and the Acceptor enters  
696 the data manually

697 ○ Into a MOTO application on a Physical POI or

698 ○ Via a web-browser into a MOTO application on a Virtual Terminal.

699 • For Telephone Order transactions, the Card Data and address data (as needed) are  
700 provided by the Cardholder

701 ○ Verbally over a phone to the Acceptor who enters the data manually

702 • Into a MOTO application on a Physical POI or

703 • Via a web-browser into a MOTO application on a Virtual Terminal.

704 ○ By Manual Entry using the phone keypad e.g., via Touch Tone facility using Dual-Tone-  
705 Multi-Frequency-encoded technology (DTMF), to automatically populate a MOTO  
706 application on a Virtual Terminal.

---

<sup>53</sup> Detailed guidance on the usage of Acceptor Name can be found within Book 6.

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

709 Req T17: The Acceptor shall be able to confirm the transaction including the transaction  
710 amount to execute the transaction.

#### 711 **4.3.2 Configuration**

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

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

##### 715 **4.3.2.1 Local Transactions and Remote Transactions (all Acceptance Environments)**

716 Req T18: It shall be possible to configure the Payment Services, the Application Profiles and  
717 the Functions. In particular it shall be possible to configure the POI Application to  
718 activate or deactivate specific Payment Services and/or Functions.

719 Req T19: It shall be possible to configure which of the supported Acceptance Technologies  
720 are activated per Payment Service. Activation of the Contactless Acceptance  
721 Technology shall mean both, activation of Chip Contactless and Mobile  
722 Contactless.

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

725 Req T20: For Manual Entry, it shall be possible to configure the Physical POI or Virtual  
726 Terminal to prompt for the entry of the CSC. For No-Show transactions and  
727 transactions processed from Stored Card Data for Instalment or Recurring  
728 Payments it shall be possible to bypass entry of the CSC.

##### 729 **4.3.2.2 Local Transactions (Physical POI) and Remote Transactions at the Virtual POI**

730 Req T21: It shall be possible to configure the supported Authentication Methods per  
731 Application Profile.

##### 732 **4.3.2.3 Local Transactions (Physical POI)**

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

- 736 Req T338: For each Payment Brand supported for the Chip with Contact Acceptance  
737 Technology it shall be possible to configure an Application identifier (AID) as  
738 defined in [ISO/IEC 7816-4] corresponding to the Payment Brand.
- 739 Req T339: For each Payment Brand supported for the Contactless Acceptance Technology it  
740 shall be possible to configure a corresponding Application identifier (AID) as  
741 defined in [ISO/IEC 7816-4] and one or more Kernel ID(s) identifying the  
742 contactless kernel(s) that may be used for transaction processing with the  
743 respective AID.
- 744 Note that this requirement applies not only to Payment Brands which support  
745 Local EMV based Transaction processing but also to Payment Brands which  
746 support conventional Local ICT Transaction processing for the Contactless  
747 Acceptance Technology.
- 748 Req T23: As a default configuration, for Card Transactions, the Chip with Contact  
749 Acceptance Technology shall have priority over the Magnetic Stripe Acceptance  
750 Technology. However, it shall be possible to configure per Payment Service if the  
751 Chip with Contact Acceptance Technology is not required to have priority over the  
752 Magnetic Stripe Acceptance Technology.
- 753 Req T24: It shall be configurable per Application Profile whether a magnetic stripe  
754 transaction shall be allowed and considered as a fallback transaction in the event  
755 the Chip with Contact Acceptance Technology has been tried and failed for a Card  
756 Transaction and afterwards, within the same transaction, the Magnetic Stripe  
757 Acceptance Technology is tried.
- 758 In addition, it shall be configurable per Application Profile, if this configuration  
759 applies:
- 760 • Only if magnetic stripe data indicates that the Chip with Contact Acceptance  
761 Technology is supported by the Physical Card,
  - 762 • Or irrespective of whether magnetic stripe data indicates or does not indicate  
763 that the Chip with Contact Acceptance Technology is supported by the Physical  
764 Card.
- 765 Req T25: It shall be configurable per Application Profile whether PIN Bypass is allowed.
- 766 Req T26: For attended POIs that support referrals for Card Transactions it shall be  
767 configurable per Application Profile whether referrals are activated.

768 Req T27: It shall be configurable per transaction result (approved, declined or aborted) and  
 769 per Payment Service whether a Customer receipt shall be printed or delivered  
 770 electronically, either never, always or on request.<sup>54</sup>

771 Req T28: Data identifying an unattended POI used for the purposes of paying a transport  
 772 fare or parking fees shall be configurable per Application Profile.

#### 773 4.3.2.4 Remote Card Transactions at Physical POI and Virtual Terminal

774 Req T29: It shall be configurable per transaction result (approved, declined or aborted) and  
 775 per Payment Service, whether a Cardholder receipt shall be printed or delivered  
 776 electronically either never, always or on request.

### 777 4.3.3 Functions for Payment Service Processing

778 The following sections contain the Function specific requirements which are not only applicable  
 779 to an individual Payment Service but to all or to several Payment Services for Card Transactions  
 780 and to One-off-Payment for ICT Transactions.

#### 781 4.3.3.1 Transaction Initialisation

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

##### 785 4.3.3.1.1 Local Transactions (Physical POI)

786 Req T30: The attendant, Customer or sale system shall be able to select the required  
 787 Payment Service from the list of Payment Services that are activated. If Payment  
 788 Service selection is not performed, then the default Payment Service is the  
 789 selected Payment Service.

790 Req T31: For Transaction Initialisation the Customer display shall always display a message,  
 791 called Welcome Message, to the Customer, the contents of which will depend on  
 792 the selected Payment Service.

793 Req T32: The Welcome Message shall be shown only in the selected language if the default  
 794 language was overridden. Otherwise the Welcome Message shall be shown in the  
 795 default language and English (or in the default language only if it is English). If the

---

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



- 796 display is not capable of showing the Welcome Message in two different  
797 languages at the same time, it shall alternate between the two.
- 798 Req T33: For all Acceptance Technologies with the exception of the Contactless Acceptance  
799 Technology, the transaction shall be initiated either by attendant action or by  
800 insertion/swiping of a Physical Card or by external activation by the sale system.
- 801 Req T34: For contactless transactions, the transaction shall be initiated either by attendant  
802 action or by external activation by the sale system prior to the activation of the  
803 contactless reader of the POI.
- 804 Req T35: For unattended POIs capable of, and configured for, printing a transaction receipt,  
805 if the POI knows in advance that it cannot print a transaction receipt, it shall  
806 inform the Customer that a receipt cannot be printed and offer the choice to  
807 continue or abort the transaction.
- 808 *4.3.3.1.2 Remote Transactions at the (Virtual POI)*
- 809 Req T36: If more than one Payment Service is available for the transaction, the Customer  
810 shall be able to select the Payment Service from the list of Payment Services that  
811 are available. If only one Payment Service is available, this Payment Service shall  
812 be selected by default.
- 813 *4.3.3.1.3 Remote Card Transactions at Physical POI and Virtual Terminal*
- 814 Req T37: All transactions shall be initiated by the Acceptor only.
- 815 Requirements T30, T31, T32 and T33 defined above for Physical POIs also apply for MOTO, albeit  
816 it is the Acceptor that is interfacing with the POI.
- 817 Req T38: The default Service on a Virtual Terminal shall be the One-off Payment.
- 818 *4.3.3.2 Language Selection*
- 819 Language Selection is the Function which allows selecting one of the languages supported by the  
820 POI for the Customer display.
- 821 Language Selection is only performed for Customer Present Transactions.
- 822 *4.3.3.2.1 Local Transactions (Physical POI)*
- 823 Language Selection may be performed either as POI based or Card based Language Selection.



824 For the POI based Language Selection, either the sale system selects one of the languages  
825 supported by the POI or the POI Application offers the Attendant or the Customer the option to  
826 select one of the languages supported by the POI.

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

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

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

834 Req T39: If the POI receives the language from a sale system before the start of the financial  
835 transaction, it shall use it as the selected language for the duration of this  
836 transaction (POI based Language Selection by the sale system).

837 Req T40 If the POI does not receive a language from the sale system before the start of the  
838 financial transaction, or if the language that the POI receives is not supported by  
839 the POI, it may offer the attendant or the Customer the option to override the  
840 default language for the Customer display (see Req T22) and to select one of the  
841 languages supported by the POI for the Customer display (POI based Language  
842 Selection on the POI). If this option is supported, then it shall only be possible prior  
843 to the start of the transaction. If chosen in this manner, the language shall become  
844 the selected language for the duration of this transaction.

845 Req T41: If all of the following are true:

846 • the POI based Language Selection for the Customer display was not  
847 (successfully) performed prior to the start of the transaction,

848 • and the Chip with Contact Acceptance Technology or a Contactless Acceptance  
849 Technology is used,

850 • and the card data element Language Preference is retrieved,

851 then the selection of the language for the Customer display shall be performed  
852 according to [EMV] (Card based Language Selection) and the POI Application shall  
853 use from that moment on the first language in the Language Preference that it  
854 supports.

855 If any of the following is true:

856 • neither the Chip with Contact Acceptance Technology nor the Contactless  
857 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 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 Section 2.3 of Book 6 to retrieve the card data element Language Preference.

#### 4.3.3.2.2 *Remote Transactions at the Virtual POI*

Req T43: If the language selected on the Acceptor'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 Acceptor'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.

#### 4.3.3.2.3 *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.

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

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

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

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

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

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

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

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

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

918 POI requirements regarding Selection of the Payment Solution are contained in

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

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

923 POI requirements regarding Selection of the Application Profile are contained in Section  
924 4.3.3.3.5.

925 4.3.3.3.1 *IF Regulation Article 8.6 and Article 10.5 Requirements for Selection of the Payment*  
926 *Brand*

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

928 4.3.3.3.1.1 *Remits of IF Regulation Applicability*

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

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

933 • There shall be no impact on interregional (EEA/non EEA) transactions (both  
934 incoming and outgoing) to and from the EEA.

935 ○ An EEA issued card shall have no detriment to acceptance when used  
936 outside of the EEA region.

937 ○ A non-EEA issued card shall continue to be accepted when used inside the  
938 EEA region.

939 • The technical solution to implement [IFR] shall not impact non-EEA terminals  
940 or cards.

941 ○ The requirements shall not force international cards to be re-issued.

942 ○ The requirements shall not force terminals outside of the EEA to be  
943 upgraded.

## 944 4.3.3.3.1.2 IF Regulation Requirements

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

946 *"Payment card schemes, issuers, acquirers, processing entities and other technical service*  
947 *providers shall not insert automatic mechanisms, software or devices on the payment*  
948 *instrument or at equipment applied at the point of sale which limit the choice of payment*  
949 *brand or payment application, or both, by the payer or the payee when using a co-badged*  
950 *payment instrument.*

951 *Payees shall retain the option of installing automatic mechanisms in the equipment used*  
952 *at the point of sale which make a priority selection of a particular payment brand or*  
953 *payment application but payees shall not prevent the payer from overriding such an*  
954 *automatic priority selection made by the payee in its equipment for the categories of*  
955 *cards or related payment instruments accepted by the payee."*

956 The choice of the Payment Brand or Payment Application (including overriding) occurs when  
957 there are multiple mutually supported Payment Brands or Payment Applications in the  
958 Customer's Payment Device and in the POI of the Acceptor.

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

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

964 To address Article 8.6 the following requirements IFR Req T2 - IFR Req T5 shall be met. For the  
965 purposes of this Volume, requirements IFR Req T2 and IFR Req T3 are extended to also cover ICT  
966 Transactions. Requirements IFR Req T4 and IFR Req T5 only cover Card Transactions.

967 IFR Req T2: The option to have a priority selection of a particular Payment Brand or Payment  
968 Application by the Acceptor shall only be allowed if the priority Payment Brand or  
969 Payment Application is displayed to the Customer and the Customer is clearly  
970 given the possibility to override the Acceptor's priority selection.

971 **Note:**

- 972
- 973 • There are various contexts where it is not technically feasible to allow the  
974 Customer to override a priority selection (e.g., Environment with no screen  
and /or no Pin/touch/key Pad ...).
  - 975 • The priority Payment Brand or Payment Application shall be displayed on  
976 the POI or at the POS, e.g. together with the accepted Payment Brands.
  - 977 • Acceptor's priority selection can be achieved through various mechanisms.  
978 Examples and implementation guidance are provided in Book 6.

- Override of the Acceptor's priority selection by the Customer can be achieved through various mechanisms. It may include early Customer 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 Customer shall be informed of their ability to override the Acceptor's priority selection and how to override it so that the Customer 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 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 Transactions, the data element, [EMV] tag '9F0A' 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 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.

1007 4.3.3.3.2 *Selection of the Payment Solution for Local Transactions (Physical POI)*

1008 4.3.3.3.2.1 *Selection of the Payment Instrument*

1009 For Local Customer Present Transactions, Selection of the Payment Instrument is a Function,  
1010 which allows selection of one of the Payment Instruments, Card or ICT, in several ways:

- 1011 • If a Physical POI supports only one of the Payment Instruments (Card or ICT), then  
1012 Selection of the Payment Instrument is the first step of Selection of the Payment Solution,  
1013 implicitly performed by the Customer by using this POI.
- 1014 • If a Physical POI supports both Payment Instruments, then:
  - 1015 • Selection of the Payment Instrument may be the first step of Selection of the Payment  
1016 Solution. In this case, Selection of the Payment Solution has to be performed  
1017 explicitly.
  - 1018 • Selection of the Payment Instrument may be a subsequent step of the Selection of the  
1019 Payment Solution. In this case, Selection of the Payment Solution is always performed  
1020 implicitly:
    - 1021 • If Selection of the Payment Brand is the first step of the Selection of the Payment  
1022 Solution, then the Payment Instrument is selected implicitly since a specific  
1023 Payment Brand is either Card based or ICT based.
    - 1024 • If Technology Selection is the first step of the Selection of the Payment Solution,  
1025 then:
      - 1026 • Selecting Chip with Contact, Chip Contactless or Mobile Contactless will lead to  
1027 Application Selection or Combination Selection, selecting an AID and the  
1028 corresponding Payment Brand and therefore implicitly selecting the Payment  
1029 Instrument,
      - 1030 • Selecting a QR Code based Acceptance Technology implicitly selects ICT as  
1031 Payment Instrument since QR Code is only supported for ICT,
      - 1032 • Selecting Magnetic Stripe or Manual Entry by Acceptor implicitly selects Card  
1033 as Payment Instrument since these Acceptance Technologies are only  
1034 supported for Card.

1035 Req T340: Explicit Selection of the Payment Instrument shall only be performed at a POI that  
1036 supports both Payment Instruments, Card and ICT, and only if both Payment  
1037 Instruments are supported for the Service to be performed.

1038 Req T341: If explicit Selection of the Payment Instrument is performed, it shall be performed  
1039 as first step of the Selection of the Payment Solution.



1040 If Technology Selection or Selection of the Payment Brand is performed as first  
1041 step of the Selection of the Payment Solution, then explicit Selection of the  
1042 Payment Instrument shall not be performed, and the Payment Instrument shall be  
1043 selected implicitly as described in Sections 4.3.3.3.2.2 and 4.3.3.3.2.3.

1044 Req T342: If Selection of the Payment Instrument is the first step of Selection of the Payment  
1045 Solution, then both Payment Instruments shall be offered to the Customer to be  
1046 chosen from, either by a verbal communication with the Attendant at an attended  
1047 POI or by making a selection from a menu shown on the display of the attended or  
1048 unattended POI.

1049 In this version of Book 2, Local AITs are always Card Transactions. Therefore, Selection of Card as  
1050 Payment Instrument is implicitly performed for Local AITs.

#### 1051 4.3.3.3.2.2 *Technology Selection*

1052 For Local Customer Present Transactions, Technology Selection is a Function which allows for the  
1053 selection of one of the following Acceptance Technologies for transaction processing:

- 1054 • Chip with Contact (Card and ICT Transactions),
- 1055 • Contactless (Card and ICT Transactions),
- 1056 • Magnetic Stripe (Card Transactions),
- 1057 • Manual Entry by Acceptor (Card Transactions),
- 1058 • Merchant-presented QR Code (ICT Transactions),
- 1059 • Consumer-presented QR Code (ICT Transactions).

1060 For Local AITs, Technology Selection is implicitly performed since Local AITs are always processed  
1061 based on Stored Account Data.

1062 Req T45: For a Local AIT, Stored Account Data shall be used as Acceptance Technology  
1063 without performing Technology Selection.

1064 Req T46: Technology Selection shall be based on the configuration of the Payment Service  
1065 to be performed i.e., which Acceptance Technologies are activated for the Service,  
1066 which Payment Brand(s) and Payment Instrument(s) are supported per Payment  
1067 Service and Acceptance Technology, and, for Card as Payment Instrument,  
1068 whether Chip with Contact has priority over Magnetic Stripe for this Service (see  
1069 Reqs T19 and T23).

1070 Req T343: If Technology Selection is the first step of the Selection of the Payment Solution,  
1071 then all Acceptance Technologies activated for the Service to be performed shall



- 1072 be available in parallel for the Customer to choose for Technology Selection  
1073 ("open-to-all" scenario in Book 6).
- 1074 Req T344: If Selection of the Payment Instrument is performed before Technology Selection,  
1075 then only the Acceptance Technologies which are activated for the Payment  
1076 Service to be performed and for which the selected Payment Instrument is  
1077 supported shall be available for the Customer to choose for Technology Selection.
- 1078 Req T345: If Selection of the Payment Brand is performed before Technology Selection, then  
1079 only the Acceptance Technologies which are activated for the Payment Service to  
1080 be performed and for which the selected Payment Brand is supported shall be  
1081 available for the Customer to choose for Technology Selection.
- 1082 Req T346: A POI supporting Merchant-presented QR Code as Acceptance Technology shall, at  
1083 a minimum, be able to present QR Codes complying with [ISO/IEC 18004] and  
1084 providing the PISP information (URL) needed to connect to the PISP remotely.
- 1085 When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), the  
1086 QR Code presented by the POI shall comply with that standard.
- 1087 Req T347: If the POI supports one or more ICT Payment Brand(s) based on the standard  
1088 Merchant-presented QR Code, then, for Technology Selection, the POI shall  
1089 present a standard Merchant-presented QR Code indicating in the standardised  
1090 payload all available Payment Brand(s), which, if several Payment Brands are  
1091 available, may be ordered according to the Acceptor's priorities.
- 1092 Req T348: A POI supporting Consumer-presented QR Code as Acceptance Technology shall,  
1093 at a minimum, be able to read and decode QR Codes complying with [ISO/IEC  
1094 18004].
- 1095 When the EPSG has adopted a QR Code standard (see Section 1.8 of Book 1), the  
1096 POI shall support reading Consumer-presented QR Codes which comply with that  
1097 standard and shall be able to interpret the standardised payload and to act on its  
1098 contents. In particular, the POI shall be able to decode which Payment Brand(s)  
1099 are indicated as supported in the QR Code.
- 1100 Req T349: The POI shall be able to detect, which of the Acceptance Technologies made  
1101 available for the Customer is selected by the Customer.
- 1102 For the Merchant-presented QR Code Acceptance Technology, this may require  
1103 that Customer or Attendant enter on the POI an additional selection or  
1104 confirmation of this Acceptance Technology.
- 1105 Req T47: If an Acceptance Technology is selected, all other Acceptance Technologies shall  
1106 be deactivated until Technology Selection is re-started. However if the Contactless  
1107 Acceptance Technology is selected, insertion of a card in the contact reader must  
1108 be detected according to [EMV A].

- 1109 Req T48: The POI shall display a message to use the Chip with Contact Acceptance  
1110 Technology, if all of the following are true:
- 1111 • The Magnetic Stripe Acceptance Technology is used, implicitly selecting Card  
1112 as Payment Instrument,
  - 1113 • and the service code within Track 2 indicates that the Chip with Contact  
1114 Acceptance Technology is supported by the Physical Card,
  - 1115 • and there has not been an attempt to use the Chip with Contact Acceptance  
1116 Technology during the current transaction,
  - 1117 • and the Chip with Contact Acceptance Technology is activated for the Service  
1118 and the Payment Instrument Card is supported for this Acceptance Technology  
1119 (see Req T19 and Req T337),
  - 1120 • and the Chip with Contact Acceptance Technology is configured to have  
1121 priority (see Req T23).
- 1122 Req T49: If before any other Acceptance Technology is selected a Chip Card is inserted in  
1123 the chip reader and the Acceptance Technology Chip with Contact is activated,  
1124 then the POI Application shall recognise this and shall initiate reset processing  
1125 according to [EMV B1].
- 1126 Req T50: If a Physical Card is inserted in the chip reader and if the reset processing is  
1127 unsuccessful and if the POI Application allows for additional re-reading of the chip,  
1128 then a message shall be displayed to retry the Chip with Contact Acceptance  
1129 Technology.
- 1130 Req T51: If a Physical Card is inserted in the chip reader, and if the Payment Instrument  
1131 Card is activated for the Chip with Contact Acceptance Technology, and if the  
1132 Payment Instrument ICT is not activated for the Chip with Contact Acceptance  
1133 Technology or has not (yet) been selected, and if the Chip with Contact  
1134 Acceptance Technology does not work and if the Magnetic Stripe Acceptance  
1135 Technology is activated, then the POI Application shall initiate magnetic stripe  
1136 processing identified as fallback according to Req T24.
- 1137 **4.3.3.3.2.3 Selection of the Payment Brand**
- 1138 For Local Customer Present Transactions, Selection of the Payment Brand is a Function which  
1139 allows the selection of a Payment Brand in several ways according to the following requirements:
- 1140 Req T350: The Acceptor shall display to the Customer the accepted Payment Brands in a  
1141 clear way.

- 1142 Req T351: If Selection of the Payment Brand is performed before Technology Selection,  
1143 Selection of the Payment Brand shall be performed explicitly, either by a verbal  
1144 communication with the Attendant at an attended POI or by making a selection  
1145 from a menu shown on the display of the attended or unattended POI. In addition,  
1146 only the Acceptance Technologies for which the selected Payment Brand is  
1147 supported shall available for Technology Selection (see Req T345).
- 1148 Req T352: If Technology Selection is performed before Selection of the Payment Brand, and if  
1149 the Acceptance Technology Chip with Contact is selected, then:
- 1150 • Application Selection according to [EMV B1] shall be performed, resulting in  
1151 selection of an AID supported by both the Payment Device and the POI,
  - 1152 • And the Payment Brand corresponding the selected AID (see Req T338) shall  
1153 implicitly be selected.
- 1154 Req T353: If Technology Selection is performed before Selection of the Payment Brand, and if  
1155 the Contactless Acceptance Technology is selected, then:
- 1156 • Combination Selection according to [EMV B] shall be performed, resulting in  
1157 selection of a Combination of AID and Kernel ID supported by both the  
1158 Payment Device and the POI,
  - 1159 • And the Payment Brand corresponding the selected AID (see Req T339) shall  
1160 implicitly be selected.
- 1161 Req T354: If Technology Selection is performed before Selection of the Payment Brand, and if  
1162 the Merchant-presented QR Code Acceptance Technology is selected, then:
- 1163 • The Selection of the Payment Brand shall be performed by the Customer,  
1164 selecting a Payment Brand from a list on the PISP website according to Req  
1165 T55,
  - 1166 • Or Selection of the Payment Brand shall be performed by the Customer on  
1167 their Payment Device, selecting one of the Payment Brand(s) mutually  
1168 supported by POI and Mobile QR Code ICT Application on the Payment Device,  
1169 if the QR Code is a standard QR Code indicating in the standardised payload  
1170 the ICT based Payment Brands supported by the POI for the Payment Service  
1171 to be performed and if the QR Code is read through a Mobile QR Code ICT  
1172 Application on the Payment Device supporting such a selection and  
1173 communicating its result to the PISP.
- 1174 Req T355: If Technology Selection is performed before Selection of the Payment Brand, and if  
1175 the Consumer-presented QR Code Acceptance Technology is selected, then:

- 1176                      • The Selection of the Payment Brand shall be performed by the Customer on  
1177                      the POI where the selection is made from all ICT based Payment Brands  
1178                      supported by the POI,
- 1179                      • Or Selection of the Payment Brand shall be performed by the Customer on the  
1180                      POI, selecting one of the ICT based Payment Brand(s) mutually supported by  
1181                      POI and the Payment Device, if the QR Code is a standard QR Code indicating  
1182                      in the standardised payload more than one ICT based Payment Brands  
1183                      supported by the Payment Device and if the standard QR Code is interpreted  
1184                      by the POI to identify the Payment Brand(s) supported by Payment Device and  
1185                      POI.
- 1186    Req T356:    If Technology Selection is performed after Selection of the Payment Brand, and if  
1187                      one of the Acceptance Technologies Chip with Contact or Contactless is selected,  
1188                      then Application Selection (Chip with Contact) or Combination Selection  
1189                      (Contactless) shall be performed after Technology Selection:
- 1190                      • To determine whether the AID corresponding to the selected Payment Brand is  
1191                      supported by the Payment Device,
- 1192                      • And to select the Payment Application on the Payment Device with the AID  
1193                      corresponding to the selected Payment Brand.
- 1194    Req T52:    For Selection of the Payment Brand for the Chip with Contact Acceptance  
1195                      Technology, in addition to Application Selection requirements of [EMV B1], the  
1196                      following rules shall apply only for EEA issued cards and Contact EMV Card  
1197                      Payment Applications used for ICT Transactions, in line with the IFR Requirements  
1198                      in Section 4.3.3.3.1.2:
- 1199                      1.        The POI shall always construct the list of mutually supported applications  
1200                      between the Chip Card and the POI.
- 1201                      If the POI successfully reads [EMV] tag '9F0A' with ID = '0001' for any  
1202                      application, then the POI may use the value assigned to ID '0001' (as  
1203                      described in Section 3.2) to determine whether to exclude the application  
1204                      from the list of mutually supported applications.
- 1205                      2.        If the list contains only one entry, then proceed according to [EMV B1] with  
1206                      the following modification: If the Customer has expressed the wish to make  
1207                      a choice, then this single application shall be shown for confirmation.
- 1208                      If the list contains more than one entry, the POI shall proceed according to  
1209                      Paragraph 3 or 4 or 5.

- 1210 Paragraph 5 shall only apply where it is not technically feasible to allow the  
 1211 Customer to override a choice of application (e.g., Environment with no  
 1212 screen and /or no Pin/touch/key Pad ...).
- 1213 3. The POI shall present without discrimination all mutually supported  
 1214 applications to enable Customer choice. The POI display ergonomics shall  
 1215 be designed such that the Customer is able to choose from the mutually  
 1216 supported applications in a convenient way.
- 1217 • The Acceptor may put their prioritised application on top.
  - 1218 • Once the Customer decides which application to be used for that  
 1219 specific transaction, the Acceptor shall not override that decision.
- 1220 4. The Customer will only be presented with the Acceptor's prioritised  
 1221 application (automatic mechanism according to [IFR], Article 8.6).
- 1222 If the Acceptor has chosen to implement priority selection, the Customer  
 1223 shall be offered an override mechanism. This mechanism shall be made  
 1224 available prior to EMVCo's Card Action Analysis being performed. In  
 1225 particular, this may be an early Customer preference mechanism.
- 1226 If the Customer overrides the Acceptor's priority selection, then Paragraph  
 1227 3 shall apply.
- 1228 5. The POI shall select the first mutually supported application. The Acceptor  
 1229 may put their prioritised application on top.
- 1230 Req T53: For Selection of the Payment Brand for the Contactless Acceptance Technology,  
 1231 Combination Selection shall follow [EMV B].
- 1232 For EEA issued cards, for Contactless EMV Card Payment Applications used for ICT  
 1233 Transactions and for Mobile Contactless ICT Payment Applications the following  
 1234 rules apply:
- 1235 • The following modifications are allowed for building the list of mutually  
 1236 supported combinations described in [EMV B]:
    - 1237 • If the POI successfully reads [EMV] tag '9F0A' with ID = '0001' for any  
 1238 combination, then the POI may use the value assigned to ID '0001' (as  
 1239 described in Section 3.2) to determine whether to exclude the combination  
 1240 from the list of mutually supported combinations.
    - 1241 • The Acceptor may put their prioritised application on top.
    - 1242 • The following modification applies for [EMV B] Final Combination Selection: If  
 1243 the list of mutually supported combinations contains only one application and

- 1244 the Customer has expressed the wish to make a choice, then this single  
1245 application shall be shown for confirmation.
- 1246 • If the list of mutually supported combinations contains more than one  
1247 application (different DF Names), then the following modifications apply for  
1248 Final Combination Selection described in [EMV B]:
- 1249 • The Customer shall have the means to select the application of their  
1250 choice. If the Customer makes a choice, then the chosen application shall  
1251 be used in Final Combination Selection.
- 1252 • If the Customer does not wish to make a choice, then Final Combination  
1253 Selection shall follow [EMV B] using the list of mutually supported  
1254 combinations built as described above with the allowed modifications.
- 1255 • If it is not technically feasible to allow the Customer to select the  
1256 application of their choice (e.g., Environment with no screen and /or no  
1257 Pin/touch/key Pad ...), then Final Combination Selection shall follow [EMV  
1258 B] using the list of mutually supported combinations built as described  
1259 above with the allowed modifications.
- 1260 Req T357: For Selection of the Payment Brand for the Consumer-Presented QR Code  
1261 Acceptance Technology the following rules apply:
- 1262 • When building the list of (mutually supported) Payment Brands, the Acceptor  
1263 may put their prioritised Payment Brand on top.
- 1264 • If the list of (mutually supported) Payment Brands contains only one entry and  
1265 the Customer has expressed the wish to make a choice, then this single  
1266 Payment Brand shall be shown to the Customer for confirmation.
- 1267 • If the list of (mutually supported) Payment Brands contains more than one  
1268 entries, then:
- 1269 • The Customer shall have the means to select the Payment Brand of their  
1270 choice. If the Customer makes a choice, then the chosen Payment Brand  
1271 shall be used for the transaction.
- 1272 • If the Customer does not wish to make a choice, or if it is not technically  
1273 feasible to allow the Customer to select the Payment Brand of their choice  
1274 (e.g., Environment with no screen and /or no Pin/touch/key Pad ...), then  
1275 the Payment Brand on top of the list of (mutually supported) Payment  
1276 Brands shall be selected and used for the transaction.



1277 For Local AITs, the Acceptor has to store the Payment Brand to be used together with the  
1278 Account Data to be used. Therefore, selection of the Payment Brand for a Local AIT is performed  
1279 according to the following requirement:

1280 Req T358: For processing a Local AIT, the Acceptor shall select and use the Payment Brand  
1281 stored together with the Account Data to be used for the Local AIT.

#### 1282 4.3.3.3.3 *Selection of the Payment Solution for Remote Transactions at the Virtual POI*

##### 1283 4.3.3.3.3.1 *Selection of the Payment Instrument*

1284 For Remote Customer Present Transactions, i.e. for e- and m-Commerce transactions, Selection  
1285 of the Payment Instrument is a Function, which allows selection of one of the Payment  
1286 Instruments, Card or ICT as follows:

- 1287 • If a Virtual POI supports only one of the Payment Instruments (Card or ICT), then  
1288 Selection of the Payment Instrument is the first step of Selection of the Payment Solution,  
1289 implicitly performed by the Customer by using this POI.
- 1290 • If a Virtual POI supports both Payment Instruments, then:
  - 1291 • Selection of the Payment Instrument may be the first step of Selection of the Payment  
1292 Solution. In this case, Selection of the Payment Solution has to be performed  
1293 explicitly.
  - 1294 • If Selection of the Payment Brand is the first step of the Selection of the Payment  
1295 Solution, then the Payment Instrument is selected implicitly since a specific Payment  
1296 Brand is either Card based or ICT based.

1297 Req T359: Explicit Selection of the Payment Instrument shall only be performed at a Virtual  
1298 POI that supports both Payment Instruments, Card and ICT, and only if both  
1299 Payment Instruments are supported for the Service to be performed.

1300 Req T360: If explicit Selection of the Payment Instrument is performed, it shall be performed  
1301 as first step of the Selection of the Payment Solution.

1302 If Selection of the Payment Brand is performed without performing explicit  
1303 Selection of the Payment Instrument before, then explicit Selection of the  
1304 Payment Instrument shall not be performed, and the Payment Instrument shall be  
1305 selected implicitly as described in Section 4.3.3.3.3.

1306 Req T361: If Selection of the Payment Instrument is the first step of Selection of the Payment  
1307 Solution, then both Payment Instruments shall be offered to the Customer to be  
1308 chosen from a menu displayed to the Customer.

1309 In this version of Book 2, Remote AITs are always Card Transactions. Therefore, Selection of Card  
1310 as Payment Instrument is implicitly performed for Remote AITs.

1311 *4.3.3.3.2 Technology Selection*

1312 For Remote Customer Present Transactions, i.e. for e- and m-Commerce transactions,  
1313 Technology Selection is implicitly performed by the Customer when choosing on their Consumer  
1314 Device a browser or a dedicated application for the access over the internet.

1315 For Remote AITs, Technology Selection is implicitly performed since Remote AITs are always  
1316 processed based on Stored Account Data.

1317 *4.3.3.3.3 Selection of the Payment Brand*

1318 For Remote Customer Present Transactions, Selection of the Payment Brand is a Function which  
1319 allows the selection of a Payment Brand according to the following requirement:

1320 Req T55: The Payment Brands<sup>55</sup> and, for Card based Payment Brands, Product Types  
1321 accepted by the Acceptor for the transaction shall be displayed so the Customer  
1322 can choose the Payment Brand to be used to perform the transaction. The  
1323 Acceptor may determine the method and the order in which the Payment Brands  
1324 and, for Card based Payment Brands, Product Types are displayed to the  
1325 Customer. If not all Payment Brands and Product Types are displayed at once for  
1326 selection, the Acceptor shall inform the Customer how to select the other  
1327 supported Payment Brands and Product Types.

1328 For Remote AITs, the Acceptor has to store the Payment Brand to be used together with the  
1329 Account Data to be used. Therefore, selection of the Payment Brand for a Remote AIT is  
1330 performed according to the following requirement:

1331 Req T362: For processing a Remote AIT, the Acceptor shall select and use the Payment Brand  
1332 stored together with the Account Data to be used for the Remote AIT.

1333 *4.3.3.3.4 Selection of the Payment Solution for Remote Card Transactions at Physical POI and*  
1334 *Virtual Terminal*

1335 In this version of Book 2, MOTO transactions are always Card Transactions. Therefore, Selection  
1336 of Card as Payment Instrument is implicitly performed for MOTO transactions.

---

<sup>55</sup> The Click to Pay Icon may be used in this context.



1337 For MOTO transactions, the Acceptance Technology is implicitly selected. It is determined by the  
1338 process used for MOTO, whether the Acceptance Technology is Manual Entry by the Acceptor or  
1339 Manual Entry by the Customer.

1340 For MOTO transactions, Selection of the Payment Brand is the Function which allows the POI to  
1341 select a Payment Brand, which is transparent for the Cardholder and the Acceptor:

1342 Req T363: The POI shall select the Payment Brand based on the PAN that is manually entered  
1343 for the MOTO transaction.

#### 1344 4.3.3.3.5 *Selection of the Application Profile*

1345 Req T54: For Local Customer Present Transactions, The Application Profile shall be selected  
1346 for a transaction based on the Payment Service to be performed and primarily on  
1347 the following:

- 1348 • The selected AID for a Card or ICT Transaction if the Chip with Contact  
1349 Acceptance Technology is used,
- 1350 • The selected Combination for a Card or ICT Transaction if a Contactless  
1351 Acceptance Technology is used,
- 1352 • The PAN for a Card Transaction if the Magnetic Stripe, Manual Entry or Stored  
1353 Card Data Acceptance Technology is used,
- 1354 • The selected Payment Brand for an ICT Transaction if the Merchant-presented  
1355 QR Code or Consumer-presented QR Code Acceptance Technology is used.

1356 In addition, for a Card Transaction using the Chip with Contact Acceptance  
1357 Technology or the Contactless Acceptance Technology, the Application Profile may  
1358 be selected based on the presence/absence of [EMV] tag '9F0A' with ID = '0001'  
1359 and on the value assigned to ID '0001'.

1360 Req T56: For Remote Transactions, the Application Profile shall be selected for a transaction  
1361 based on the Payment Service to be performed and on the selected Payment  
1362 Brand. In addition, for a Card based Payment Brand, the Application Profile may be  
1363 selected based on the Product Type.

1364    4.3.3.4    Account Data Retrieval

1365    Account Data Retrieval is the Function which allows retrieval of the data identifying the  
1366    Customer's account to be used for the transaction. The method to retrieve this data depends on  
1367    the Acceptance Technology.

1368    For Card Transactions, this Function is used to retrieve Card Data.

1369    4.3.3.4.1    *Local Transactions and Remote Transactions (all Acceptance Environments)*

1370    Req T58:        For Card Transactions, all authorisation and completion messages shall identify the  
1371                      method used to retrieve Card Data.

1372    4.3.3.4.2    *Local Transactions (Physical POI)*

1373    Req T59:        For Local Customer Present Card Transactions at a Physical POI, the Acceptance  
1374                      Technology shall be Chip with Contact, Chip Contactless, Mobile Contactless,  
1375                      Magnetic Stripe, or Manual Entry by Acceptor.

1376                      For Local Customer Present ICT Transactions at a Physical POI, the Acceptance  
1377                      Technology shall be Chip with Contact, Chip Contactless, Mobile Contactless,  
1378                      Merchant-presented QR Code or Consumer-presented QR Code.

1379                      For EMV based Local Card or ICT Transactions using Acceptance Technology Chip  
1380                      with Contact, Chip Contactless, or Mobile Contactless, and for Local Card  
1381                      Transactions using Acceptance Technology Magnetic Stripe or Manual Entry by  
1382                      Acceptor, Account Data to be retrieved is Card Data, i.e. PAN and expiry date.  
1383                      Depending on the Acceptance Technology, Card Data shall be read by the Physical  
1384                      POI Application from the EMV Card Payment Application selected for the  
1385                      transaction or from the magnetic stripe of the Card used for the transaction, or  
1386                      Card Data shall be entered to the POI by the Acceptor.

1387                      For conventional ICT Transactions using Acceptance Technology Mobile  
1388                      Contactless, Account Data consisting of Customer's ASPSP identification and  
1389                      Customer identification, shall be retrieved by the Physical POI Application from the  
1390                      Mobile Contactless ICT Payment Application selected for the transaction (see step  
1391                      3. in Figure 7 in Section 1.8 of Book 1).

1392                      For conventional ICT Transactions using Acceptance Technology Merchant-  
1393                      Presented QR Code, Account Data is not retrieved by the Physical POI Application,  
1394                      but by the PISP (see step 3. in Figure 5 in Section 1.8 of Book 1).

1395                      For conventional ICT Transactions using Acceptance Technology Consumer-  
1396                      presented QR Code, Account Data consisting of the Customer's ASPSP  
1397                      identification and, if not entered or retrieved later during the transaction, of the

1398		Customer identification, shall be retrieved by the Physical POI Application from the
1399		Consumer -presented QR Code (see step 2. in Figure 6 in Section 1.8 of Book 1).
1400		read by the Physical POI Application from the EMV Card Payment Application
1401		selected for the transaction or from the magnetic stripe of the Card used for the
1402		transaction, or Card Data shall be entered to the POI by the Acceptor.
1403		For Local AIT at a Physical POI, the Acceptance Technology shall be Stored Account
1404		Data.
1405	Req T60:	When Manual Entry by Acceptor is supported, the Physical POI Application shall
1406		facilitate entering the PAN, the expiry date and, when appropriate, the Card
1407		Security Code.
1408	4.3.3.4.3	<i>Remote Transactions at the Virtual POI</i>
1409	Req T61:	For e- and m-Commerce transactions, the Acceptance Technology shall be
1410		Consumer Device with Browser over Internet or Consumer Device with Dedicated
1411		Application over Internet.
1412		For these Acceptance Technologies, the Virtual POI shall display a payment page
1413		to the Customer.
1414		For Card based e- and m-Commerce transactions, this page shall facilitate for the
1415		Customer either the entry of the PAN, the expiry date, and the Card Security Code
1416		or the retrieval of stored PAN and expiry date <sup>56</sup> .
1417		For ICT based e- and m-commerce transactions, this page shall facilitate for the
1418		Customer the entry or retrieval of the Customer's ASPSP identification and, if not
1419		entered or retrieved later during the transaction, of the Customer identification
1420		(see step 3. in Figure 4 in Section 1.8 of Book 1).
1421		For Remote AIT at the Virtual POI, the Acceptance Technology shall be Stored
1422		Account Data.
1423	4.3.3.4.4	<i>Remote Card Transactions at Physical POI and Virtual Terminal</i>
1424	Req T62:	For MOTO transactions, the Acceptance Technology shall be Manual Entry by
1425		Acceptor or Manual Entry by Customer. For Remote AIT at Physical POI and Virtual
1426		Terminal, the Acceptance Technology shall be Stored Card Data.

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

1427 For MOTO transactions, the interface with the Cardholder is just to facilitate the  
 1428 entry of the Card Data via a Telephone keypad when Touch-Tone using DTMF  
 1429 technology is supported. Therefore the Physical POI and Virtual Terminal shall  
 1430 facilitate the entry of the PAN, the expiry date, and the Card Security Code by the  
 1431 Acceptor and where DTMF is enabled, the Virtual Terminal shall support the entry  
 1432 of the Card Data by the Cardholder via a telephone keypad.

1433 Req T63: The MOTO Application shall also support the entry and transmission of Address  
 1434 Data if address validation is supported.

#### 1435 4.3.3.5 Authentication

1436 Authentication is the Function to perform Strong Customer Authentication (SCA) according to  
 1437 [PSD2] and the [RTS SCA/CSC], including the decision whether any exemption applies.

##### 1438 4.3.3.5.1 *Authentication is only applicable for Customer Present Transactions. EMV Based* 1439 *Local Transactions (Physical POI)*

1440 For EMV based Local Transactions, Authentication consists of two sub-functions: Card  
 1441 Authentication, and Cardholder Verification as defined by EMV.

##### 1442 4.3.3.5.1.1 *Card Authentication*

1443 Card Authentication is a Function for EMV based Local Transactions defined by EMV by which an  
 1444 EMV Card Payment Application is authenticated to the POI (Offline Data Authentication) and/or  
 1445 the Issuer (EMV Online Authentication). Card Authentication applies only to the Chip with  
 1446 Contact Acceptance Technology and to the Contactless Acceptance Technologies.

1447 Card Authentication for EMV based Local Transactions using a Contactless Acceptance  
 1448 Technology may contain additional steps to detect relay attacks. These mechanisms are specific  
 1449 to each contactless EMV Kernel<sup>57</sup> and are out of scope of this document.

1450 Req T64: Online-only POI Applications are not required to support Offline Data  
 1451 Authentication.

1452 Req T65: The following applies for POI Applications supporting the Chip with Contact  
 1453 Acceptance Technology and RSA-based Offline Data Authentication:

- 1454 • DDA is mandatory.

---

<sup>57</sup> E.g. Relay Resistance Protocol in [EMV C8].

- 1455                      • CDA is mandatory.
- 1456                      • SDA is no longer supported.
- 1457                      For POI Applications supporting the Chip with Contact Acceptance Technology and  
1458                      ECC-based Offline Data Authentication, XDA is mandatory.
- 1459                      For POI Applications supporting Chip and Mobile Contactless, the Offline Data  
1460                      Authentication methods shall be supported as defined in the respective kernel  
1461                      specifications (in particular BDHLA, when supporting Kernel 8 [EMV C8]).
- 1462    4.3.3.5.1.2    *Cardholder Verification*
- 1463    Cardholder Verification is a Function for EMV based Local Transactions defined by EMV by which  
1464    a Cardholder Verification Method (CVM) is selected and performed.
- 1465    The CVMs to be used are listed in **Table 4**. The Acceptance Technologies with which they may be  
1466    used are shown below:
- 1467                      • Offline Enciphered PIN, if the Acceptance Technology is Chip with Contact,
- 1468                      • Offline Plaintext PIN, if the Acceptance Technology is Chip with Contact,
- 1469                      • Online PIN, if the Acceptance Technology is Chip with Contact, Chip Contactless, Mobile  
1470                      Contactless or Magnetic Stripe,
- 1471                      • Offline Biometric Verification, if the Acceptance Technology is Chip with Contact,
- 1472                      • Biometrics via Sensor on Card, if the Acceptance Technology is Chip Contactless,
- 1473                      Note that Biometrics via Sensor on Card may also be used with the Acceptance  
1474                      Technology Chip with Contact,
- 1475                      • CDCVM, i.e. Offline Mobile Code or Biometrics on Consumer Device<sup>58</sup>, if the Acceptance  
1476                      Technology is Mobile Contactless,
- 1477                      • Signature for all Acceptance Technologies with the exception of the Contactless  
1478                      Acceptance Technology with form factors that do not allow signature comparison, e.g.,  
1479                      Mobile phones,
- 1480                      • No CVM Required for all Acceptance Technologies.

58

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

1481    4.3.3.5.1.2.1    *General Requirements for Cardholder Verification*

1482    Req T69:    All Physical POI shall have a PIN Entry Device; with the exception of environments  
1483    where the interaction with the Customer must be minimized for Customer or  
1484    Acceptor convenience (e.g., low value payments, transaction speed, highway  
1485    tolls). The Physical POI may in addition have a Biometric Capture Device.

1486    Req T70:    For POIs that have a PIN Entry Device, the POI Application shall be able to support  
1487    PIN as CVM.

1488    Req T71:    The POI Application shall offer PIN Bypass to the Customer if PIN entry is  
1489    requested and PIN Bypass is allowed according to the Application Profile (see Req  
1490    T25).

1491    4.3.3.5.1.2.2    *Cardholder Verification for the Chip with Contact Acceptance Technology*

1492    Req T72:    POIs with a PIN Entry Device shall meet the following requirements:

- 1493    • For POIs which are not ATMs:
- 1494       ○ For offline-only POIs the POI Application shall support Offline PIN.
- 1495       ○ For offline with online capability POIs the POI Application shall support  
1496       Offline PIN and may support, in addition, Online PIN.
- 1497       ○ For online-only POIs the POI Application shall support Offline PIN, or Online  
1498       PIN or both.
- 1499       ○ Other CVMs as defined by [EMV], including Signature, No CVM Required  
1500       and Offline Biometric Verification, may be supported in addition to PIN.
- 1501       ○ Unattended POIs shall not support Signature CVM and Combined CVM  
1502       containing Signature.
- 1503    • For ATMs:
- 1504       ○ The POI Application shall support Online PIN.
- 1505       ○ The POI Application may in addition support Offline PIN and Offline  
1506       Biometric Verification.
- 1507       ○ ATMs shall not support No CVM Required, Signature CVM or Combined  
1508       CVM containing Signature.

1509    4.3.3.5.1.2.3    *Cardholder Verification for the Contactless Acceptance Technology*

1510    Req T73:    POIs supporting the Contactless Acceptance Technology shall support

- 1511                    • Online PIN
- 1512                    • Signature
- 1513                    • No CVM Required
- 1514                    • CDCVM

1515                    according to the requirements of the contactless kernels implemented in that POI.

1516    4.3.3.5.1.2.4    *Cardholder Verification for the Magnetic Stripe Acceptance Technology*

1517    Req T74:    POIs with a PIN Entry Device shall meet the following requirements:

- 1518                    • The only PIN CVM supported for magnetic stripe transactions shall be Online
- 1519                    PIN.

1520                    **Note:**

1521                    The CVMs No CVM Required and Signature may also be supported.

- 1522                    • Unattended POIs, including ATMs, shall not support Signature CVM.
- 1523                    • ATMs shall not support No CVM Required.

1524    4.3.3.5.1.2.5    *Cardholder Verification for the Manual Entry Acceptance Technology*

1525    Req T75:    POIs with a PIN Entry Device shall meet the following requirements:

- 1526                    • Neither Online PIN nor Offline PIN shall be supported.
- 1527                    • Either No CVM Required, or Signature, or both CVMs shall be supported.



1528 4.3.3.5.2 *Conventional Local ICT Transactions (Physical POI)*

1529 4.3.3.5.2.1 *Merchant-Presented QR Code*

1530 Authentication is performed by the Customer's ASPSP either directly (re-directed or decoupled  
1531 Authentication) or through the PISP (embedded Authentication).

1532 Req T364: Authentication shall be performed as shown in steps 5. and 6. in Figure 5 in  
1533 Section 1.8 of Book 1.

1534 The following Authentication Methods may be used:

- 1535 • Dynamic Authentication - One Time Password (OTP)
- 1536 • Dynamic Authentication - Challenge Response based on  
1537 Authentication/Remote Payment Application on a Consumer Device
- 1538 • Biometrics on Consumer Device (CDCVM)
- 1539 • Offline Mobile Code (CDCVM)
- 1540 • Online Mobile Code
- 1541 • No CVM Required, if an SCA Exemption is allowed, e.g. based on Risk-Based  
1542 Authentication or cases where SCA is not required

1543 4.3.3.5.2.2 *Consumer-Presented QR Code*

1544 Authentication is performed by the Customer's ASPSP either directly (re-directed or decoupled  
1545 Authentication) or through the PISP (embedded Authentication) or via the Acceptor's POI.

1546 If Authentication is performed via the Acceptor's POI, an interface would have been established  
1547 between PISP and Acceptor's POI to collect the Customer data needed for authentication (e.g. an  
1548 Online Personal Code and an OTP).

1549 Req T365: Authentication shall be performed as shown in steps 5. and 6. in Figure 6 in  
1550 Section 1.8 of Book 1.

1551 The following Authentication Methods may be used:

- 1552 • Dynamic Authentication - One Time Password (OTP)
- 1553 • Dynamic Authentication - Challenge Response based on  
1554 Authentication/Remote Payment Application on a Consumer Device
- 1555 • Biometrics on Consumer Device (CDCVM)



- 1556                      • Offline Mobile Code (CDCVM)
- 1557                      • Online Mobile Code
- 1558                      • No CVM Required, if an SCA Exemption is allowed, e.g. based on Risk-Based
- 1559                      Authentication or cases where SCA is not required

#### 1560    4.3.3.5.2.3    *Mobile Contactless*

1561    Authentication is performed via an e-signed/authorised payment request with support of the  
1562    Customer's bank app.

1563    Req 366:    Authentication shall be performed as shown in steps 2. and 3. in Figure 7 in  
1564                      Section 1.8 of Book 1 with support of the Customer's bank app, acting as a Mobile  
1565                      Contactless ICT Payment Application.

1566                      The following Authentication Methods may be used:

- 1567                      • Biometrics on Consumer Device (CDCVM)
- 1568                      • Offline Mobile Code (CDCVM)
- 1569                      • Dynamic Authentication - Challenge Response based on
- 1570                      Authentication/(Remote) Payment Application on a Consumer Device
- 1571                      • No CVM Required, if an SCA Exemption is allowed, e.g. where SCA is not
- 1572                      required

#### 1573    4.3.3.5.3    *Remote Transactions at the Virtual POI*

1574    Authentication is the Function by which Strong Customer Authentication (SCA) is performed to  
1575    the Customer's ASPSP/Issuer. Risk Based Authentication may be used by the Customer's  
1576    ASPSP/Issuer to decide, whether an exemption for SCA applies (see Section 2.3.2.4 of Book 4).

1577    For Remote Customer Present Transactions, i.e. e- and m-Commerce transactions,  
1578    Authentication may involve a redirection from the Virtual POI to an authentication server in the  
1579    Customer's ASPSP/Issuer domain.

1580    Req T76:    The Virtual POI shall support at least two of the following Authentication Methods  
1581                      of different SCA factors:.

- 1582                      • Dynamic Authentication - One Time Password (OTP)
- 1583                      • Dynamic Authentication - Challenge Response based on
- 1584                      Authentication/Remote Payment Application on a Consumer Device

- 1585                   • Dynamic Authentication - Challenge Response based on Additional  
1586                   Authentication Device
- 1587                   • CDCVM, i.e. Biometrics on Consumer Device, Offline Personal Code or Offline  
1588                   Mobile Code,
- 1589                   • Online Personal Code or Online Mobile Code,
- 1590                   • No CVM Required, if an exemption for SCA applies.
- 1591                   • No CVM Required if an SCA Exemption is allowed, e.g. based on Risk-Based  
1592                   Authentication or cases where SCA is not required
- 1593                   Note that other CVMs (Offline PIN, Offline Biometric Verification, Biometrics via  
1594                   Sensor on Card) may be used which do not involve the Virtual POI (e.g., a PIN entry  
1595                   via an additional authentication device may be used, see Book 4).
- 1596    To perform Authentication during a Card based e- or m-Commerce transaction, the Cardholder  
1597    may be redirected to the Issuer, as the first step of the Authorisation process. The Issuer can  
1598    then verify the Cardholder using the previously registered Personal or Mobile code. The result of  
1599    this verification is then passed by the Issuer to the Acceptor. This process is known as 3 Domain  
1600    Security. It is highly recommended to support [EMV 3DS] for 3 Domain Security.
- 1601    For ICT based e- and m-Commerce transactions, Authentication is performed by the Customer's  
1602    ASPSP either directly (re-directed or decoupled Authentication) or through the PISP (embedded  
1603    Authentication) as shown in steps 5. and 6. in Figure 4 in Section 1.8 of Book 1.
- 1604    4.3.3.5.4    *Remote Card Transactions at Physical POI and Virtual Terminal*
- 1605    Req T67:       All MOTO Applications shall support Static Authentication.
- 1606    Req T68:       For MOTO transactions, Static Authentication is performed whereby the Card  
1607                   Issuer verifies the Card Security Code.
- 1608                   • For recurring and instalment type transactions, Static Authentication can only  
1609                   be performed on the initial transaction because storage of the Card Security  
1610                   Code (CSC) is prohibited. Stored Card Data derived initially from manual entry  
1611                   as a result of a MOTO transaction, shall be processed as per the requirements  
1612                   described for Recurring or Instalment Payments (see Sections 4.4.7 and 4.4.8).
- 1613                   • For No-Show transactions, Static Authentication is not performed because the  
1614                   CSC cannot be stored, consequently is not available, when the No-Show is  
1615                   processed.

1616 For MOTO, no other Authentication Method is applicable. However, the address and Card Data  
1617 provided by the Cardholder may be used for validation. "Signature on File", when available, may  
1618 also be used for validation.

#### 1619 4.3.3.6 Authorisation

1620 Authorisation is the Function performed by the POI to get information whether a Payment  
1621 Service has a positive or negative result.

1622 For Card Transactions, this Function can be processed online to the Acquirer according to Book 3  
1623 or processed offline by the EMV Card Payment Application.

1624 For ICT Transactions, this Function is currently only described for One-off Payment. It is  
1625 processed as shown in Figures 4 to 8 in Section 1.8 of Book 1. According to these Figures,  
1626 Authorisation is initiated at the POI either by providing the payment details (step 0 in Figures 4  
1627 and 5 in Section 1.8 of Book 1) or by sending a payment request (step 3 in Figure 6, step 1 in  
1628 Figure 7, step 2 in Figure 8 in Section 1.8 of Book 1).

1629 At the latest, the POI receives the Authorisation result when the PISP informs about success or  
1630 failure of the payment execution (step 11 in Figures 4 to 6, step 9 in Figures 7 and 8 in Section 1.8  
1631 of Book 1). However, if delays are allowed for payment execution and/or confirmation of success  
1632 or failure, delivery of this information may take several seconds.

1633 A faster delivery of the Authorisation result may be achieved if the PISP communicates success or  
1634 failure of payment initiation by the Customer's ASPSP to the POI (see optional communication in  
1635 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  
1636 initiation always means a negative result for the One-off Payment. Successful payment initiation  
1637 implies that the Customer's ASPSP has made a positive decision regarding the payment.  
1638 Therefore, this information may be considered as the positive result of the Authorisation,  
1639 provided error solutions are in place in case a payment execution is initiated but is finally not  
1640 successful.

#### 1641 4.3.3.6.1 *Local Card Transactions (Physical POI) and Remote Card Transactions at the Virtual* 1642 *POI*

1643 Req T77: If the authorisation response message includes a response code indicating that  
1644 SCA is required, then the POI shall take appropriate action to obtain Cardholder  
1645 Verification or, if this is not possible, decline the transaction.

#### 1646 **Note:**

1647 There are several methods to obtain Cardholder Verification:

- 1648 • SWITCH INTERFACE
- 1649 • RE-PRESENT CARD AND ENTER PIN

- 1650                      • ENTER PIN WITHOUT A SECOND TAP
- 1651    4.3.3.6.2    *Local Card Transactions (Physical POI)*
- 1652    Req T78:      Magnetic Stripe and Manual Entry transactions shall be sent online for  
1653                      authorisation. If the magnetic stripe transaction is a fallback transaction, it shall be  
1654                      identified as a fallback transaction.
- 1655    Req T79:      If the Authorisation Response Code indicates that the Online PIN entered did not  
1656                      verify correctly ("Wrong PIN"), for the Chip with Contact Acceptance Technology  
1657                      and for the Contactless Acceptance Technology, the transaction shall be declined  
1658                      and Online PIN re-entry shall not be allowed within this same transaction.
- 1659                      If the Acceptance Technology is Chip with Contact, the POI may start a new  
1660                      transaction transparently for the Customer to facilitate the re-entry of the PIN (i.e.  
1661                      without ejecting the Chip Card, without repeating Language Selection and  
1662                      Selection of the Application, but with repeating the complete EMV card process  
1663                      including Online PIN entry).
- 1664    Req T80:      For attended POIs, for all Payment Services with exception of the One-off Payment  
1665                      Service (see Req T120) and the Deferred Payment Service (see Req T191), the  
1666                      attendant shall not be allowed to force a declined transaction to be accepted.
- 1667    Req T81:      The DF Name [EMV] tag '84' and, if successfully read by the POI, the value for ID =  
1668                      '0001' of Application Selection Registered Proprietary Data [EMV] tag '9F0A' of the  
1669                      selected application shall be included in the authorisation messages.
- 1670    4.3.3.6.3    *Remote Card Transactions at the Virtual POI*
- 1671    Req T82:      For e- or m-Commerce transaction, the POI shall perform an online authorisation  
1672                      exchange to the Issuer.
- 1673    Req T83:      The Payment Brand and Product Type of the selected application shall be included  
1674                      in the authorisation messages.
- 1675    4.3.3.6.4    *Remote Card Transactions at Physical POI or Virtual Terminal*
- 1676    Req T84:      MOTO transactions shall be sent online for authorisation.
- 1677    Req T85:      If it is not possible to perform an online authorisation, either Voice Authorisation  
1678                      shall be performed or the transaction shall be declined.
- 1679    Req T86:      The authorisation message shall identify that the transaction is MOTO.

1680 Req T87: If available, the Payment Brand and Product Type shall be included in the  
1681 authorisation messages.

1682 4.3.3.7 Referral

1683 Referral is the Function where a Payment Service is completed with a verbal dialogue between  
1684 the Acceptor and the Acquirer to obtain an approval code when the Authorisation response  
1685 contains a referral response code. This Function is only performed for Local Card Transactions. It  
1686 does not necessarily involve the Cardholder or the Payment Device.

1687 Req T88: Only attended POIs shall support referrals. If an unattended POI receives a request  
1688 for referral it shall decline the transaction.

1689 Req T89: If the attended POI supports referrals, then it shall support it for all Acceptance  
1690 Technologies supported.

1691 If the POI does not support referrals or if referrals are not activated for the  
1692 Application Profile and the POI receives a request for referral it shall decline the  
1693 transaction.

1694 Req T90: If a Chip with Contact transaction is being processed and a request for referral is  
1695 received then chip processing shall be terminated by requesting a decline from the  
1696 Card Application and a message shall be displayed requesting the removal of the  
1697 Chip Card.

1698 Req T91: If a request for referral is received and the attended POI supports referrals, the  
1699 following process shall be followed:

- 1700
- The contact number for voice authorisation shall be made available.
  - If an approval code is received orally during voice authorisation it shall be  
1701 manually entered in the POI.  
1702
    - 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  
1705 capture.  
1706

1707 Req T92: The POI shall have mechanisms to ensure that only the authorised user can initiate  
1708 the Referral Function.

1709    4.3.3.8    Completion

1710    Completion is the Function which provides information on how a Card or ICT Transaction was  
1711    completed. It depends on the Payment Service, on the Acceptance Technology and on the  
1712    Acceptance Environment whether all or some of the following steps are performed:

- 1713        • Complete the transaction for the Payment Application
- 1714        • Inform Customer, Attendant and/or Acquirer/PISP about the result of the transaction
- 1715        • Deliver a receipt to Customer and/or Attendant

1716    4.3.3.8.1    *Local Card Transactions and Remote Card Transactions (all Acceptance*  
1717                    *Environments)*

1718    Req T93:    If the transaction (approved, declined or aborted) is not immediately online-  
1719                    captured, the transaction data shall be securely stored for data capture.

1720    4.3.3.8.2    *Local Transactions (Physical POI)*

1721    Req T94:    If the POI is capable of printing receipts and/or of providing electronic receipts, a  
1722                    transaction receipt shall be provided for the Customer if configured for the  
1723                    Application Profile. The receipt for the Customer shall be printed/provided in a  
1724                    local language of the POI and, if offered by the Acceptor, in the Customer selected  
1725                    language. The transaction receipt may be combined with the sales receipt, if any.

1726                    The following are the minimum data that shall be present on receipts.<sup>59</sup> The  
1727                    sequence of the data elements shown is not mandatory for the receipt. Additional  
1728                    data may be present but is out of scope of this document.

- 1729                    • Transaction Date and Transaction Time (local date/time)
- 1730                    • Transaction Reference, e.g., a sequence number or a sale reference number
- 1731                    • Transaction Amount<sup>60</sup> and Transaction Currency<sup>61</sup>
- 1732                    • Truncated PAN or truncated or tokenised Account Reference

---

<sup>59</sup>        Provided these requirements are in line with the local laws and regulations.

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

<sup>61</sup>        For transactions with Dynamic Currency Conversion see Req T324.

1733		<ul style="list-style-type: none"> <li>DF Name (as returned by the Payment Application) for the Chip with Contact Acceptance Technology and for the Contactless Acceptance Technology</li> </ul>
1734		
1735		<ul style="list-style-type: none"> <li>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.</li> </ul>
1736		
1737		
1738		
1739		<ul style="list-style-type: none"> <li>Acceptor Name<sup>62</sup></li> </ul>
1740		<ul style="list-style-type: none"> <li>The Payment Service, e.g., "One-off Payment"</li> </ul>
1741		<ul style="list-style-type: none"> <li>Transaction Result, e.g., "Approved"</li> </ul>
1742	4.3.3.8.3	<i>Remote Transactions at the Virtual POI</i>
1743	Req T95:	The POI shall provide a transaction receipt to the Customer after a successful authorisation process. The transaction receipt may be combined with the sales receipt.
1744		
1745		
1746		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.
1747		
1748		
1749		<ul style="list-style-type: none"> <li>Transaction Date and Transaction Time</li> </ul>
1750		<ul style="list-style-type: none"> <li>Transaction Amount and Transaction Currency</li> </ul>
1751		<ul style="list-style-type: none"> <li>Truncated PAN or truncated or tokenised Account Reference</li> </ul>
1752		<ul style="list-style-type: none"> <li>Payment Brand name</li> </ul>
1753		<ul style="list-style-type: none"> <li>Acceptor Name<sup>62</sup></li> </ul>
1754		<ul style="list-style-type: none"> <li>Transaction Reference number</li> </ul>
1755		<ul style="list-style-type: none"> <li>The Payment Service, e.g., "One-off Payment"</li> </ul>
1756		<ul style="list-style-type: none"> <li>Transaction Result, e.g., "Approved"</li> </ul>
1757	Req T96:	The transaction receipt shall be made available as confirmation to the Customer according to Customer's preference and communication channels available.
1758		

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



- 1759 Req T97: In case of partial delivery the final amount shall be reduced and a new receipt shall  
1760 be sent to the Customer.
- 1761 Req T98: The POI shall receive from the Acceptor the final amount which may be lower than  
1762 the authorised amount (in case of non-availability of goods or services). The  
1763 clearing data shall always include the final amount.
- 1764 **4.3.3.8.4 Remote Card Transactions at Physical POI or Virtual Terminal**
- 1765 Req T99: For Telephone Order transactions, at least a transaction reference shall be  
1766 provided to the Cardholder during the call.
- 1767 Req T100: For MOTO transactions a transaction receipt shall be provided to the Cardholder  
1768 with the delivery. The minimum data on the receipt is the same as listed in Req  
1769 T95.
- 1770 Req T101: In case of partial delivery, the final amount shall be reduced accordingly and a  
1771 receipt reflecting the reduced amount shall be provided to the Cardholder.
- 1772 **4.3.3.9 Reversal**
- 1773 Reversal is the Function where the sender informs the receiver that a transaction cannot be  
1774 processed as instructed with the intention to partially or completely nullify the effects of this  
1775 transaction. This Function is only performed for Local Card Transactions. It involves neither the  
1776 Cardholder nor the Payment Device. Reversal can be performed offline by removing the  
1777 transaction data or by storing cancellation data for capture or online.
- 1778 The following requirement applies to Local Transactions and Remote Transactions (all  
1779 Acceptance Environments):
- 1780 Req T102: Reversal shall be performed online if Authorisation is performed online and if any  
1781 of the following is true:
- 1782 • A correct response is not received or no response (timeout) is received
  - 1783 • Or the transaction is declined/aborted after an online (full or partial) approval.



1784    4.3.3.10    Data Capture

1785    Data Capture is the Function to transfer data captured at a POI to the Acquirer/PISP for  
1786    "Financial Presentment". Data Capture can be performed either as part of the Authorisation  
1787    message or after transaction completion through either a Completion Message or Batch File  
1788    transfer.

1789    A requirement requesting specific data in Data Capture requires the POI to provide the  
1790    respective data in the Data Capture Function. However, this does not mean that all data provided  
1791    by the POI in the Data Capture Function shall be used for Financial Presentment.

1792    If not specified elsewhere in the Volume, it is a Scheme/Acquirer/PISP decision, which of the data  
1793    provided by the POI has to be provided by the Acquirer/PISP for Financial Presentment.

1794    4.3.3.10.1    *Local Transactions and Remote Transactions (all Acceptance Environments)*

1795    Req T103:    One or more of the following methods of transferring the transactions to an  
1796    Acquirer shall be supported:

- 1797                    •    Online capture through the authorisation message.
- 1798                    •    Online capture through a Completion Message sent after each transaction.
- 1799                    •    Batch capture through file transfer or transaction by transaction.

1800    Req T367:    For Open Banking based ICT Transactions, Online capture through the  
1801    authorisation message, i.e., according to Section 4.3.3.6, when providing the  
1802    payment details (step 0 in Figures 4 and 5 in Section 1.8 of Book 1) or by sending a  
1803    payment request (step 3 in Figure 6, step 1 in Figure 7, step 2 in Figure 8 in Section  
1804    1.8 of Book 1), shall be performed.

1805    4.3.3.10.2    *Local Transactions (Physical POI)*

1806    Req T104:    For Card Transactions, the DF Name [EMV] tag '84' and, if successfully read by the  
1807    POI, the value for ID = '0001' of Application Selection Registered Proprietary Data  
1808    [EMV] tag '9F0A' of the selected application shall be included in Data Capture.

1809    4.3.3.10.3    *Remote Transactions at the Virtual POI*

1810    Req T105:    The Payment Brand and, for Card Transactions, Product Type shall be included in  
1811    Data Capture.

1812    4.3.3.10.4    *Remote Card Transactions at Physical POI and Virtual Terminal*

1813    Req T106:    The completion message shall identify that the transaction is MOTO.

1814    Req T107:    If available, the Payment Brand and Product Type shall be included in Data  
1815                    Capture.

Public Consultation Draft

## 1816 4.4 Basic Services

### 1817 4.4.1 One-off Payment

1818 For One-off Payment, Local Transactions are always Local Customer Present. Remote  
1819 Transactions are always e- or m-Commerce if performed at the Virtual POI, or MOTO if  
1820 performed at the Physical POI or Virtual Terminal.

1821 **Table 7** shows which combinations of Acceptance Technologies and Acceptance Environments  
1822 used in Local and Remote Transactions are allowed (✓) or not allowed/not applicable (✗) for the  
1823 One-off 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓ <sup>63</sup>	✓ <sup>63</sup>	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓ <sup>65</sup>	✓ <sup>65</sup>	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>66</sup>
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✓	✓	✗	✗
Consumer-presented QR Code <sup>67</sup>	✓	✓	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

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

<sup>64</sup> This Acceptance Technology is only allowed for Card Transactions.

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

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

<sup>67</sup> This Acceptance Technology is not allowed for Card Transactions.

<sup>68</sup> This Acceptance Technology may be called Stored Card Data for Card Transactions.

**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 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	C	C	C
• Technology Selection	M	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	M	M	M
• Card Authentication <sup>69</sup>	C	M	M
• Cardholder Verification <sup>69</sup>	M	M	-
Authorisation	M	M	M
Referral <sup>70</sup>	O	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

**TABLE 8: FUNCTIONS USED FOR ONE-OFF PAYMENT**

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

<sup>70</sup> This Function is only performed for Local Card Transactions.

<sup>71</sup> This Function is only performed for Card Transactions.

1831 In addition to the general requirements listed in Section 4.3, the following specific requirements  
 1832 apply to the One-off Payment Service for Local Transactions and Remote Transactions (all  
 1833 Acceptance Environments).

#### 1834 4.4.1.1 POI Application

##### 1835 4.4.1.1.1 *Local and Remote Card and ICT Transactions (all Acceptance Environments)*

1836 Req T108: The transaction amount shall be checked against a minimum allowed amount  
 1837 and/or a maximum allowed amount, if configured for the Application Profile. If the  
 1838 check fails, the transaction shall not proceed.

##### 1839 4.4.1.1.2 *Local Card Transactions (Physical POI)*

1840 Req T109: The Customer shall be able to confirm the transaction amount and the selected  
 1841 Payment Brand when performing the CVM.

1842 The only exceptions are where the CVM is No CVM Required or where the  
 1843 Cardholder Verification is performed on the Physical Card or Mobile Device before  
 1844 the transaction amount is known. In those cases, the Customer shall be informed  
 1845 of the transaction amount so that the confirmation of the transaction amount  
 1846 shall be implicit by presenting the Physical Card or Mobile Device.

1847 Req T110: For unattended POIs, if the transaction amount is defined before the delivery of  
 1848 the goods or services, the amount used to process the transaction shall be the  
 1849 actual amount.

1850 Req T111: If the POI supports partial approvals of online authorisations, then it shall support  
 1851 it for all Acceptance Technologies supported.

##### 1852 4.4.1.1.3 *Local ICT Transactions (Physical POI)*

1853 Req T368: The Customer shall be able to confirm the transaction amount prior to Account  
 1854 Data Retrieval (see Figures 5 to 8 in Section 1.8 of Book 1).

##### 1855 4.4.1.1.4 *Remote Transactions at the Virtual POI*

1856 Req T112: For e- and m-Commerce transactions the Virtual POI shall inform the Customer  
 1857 about the transaction including the transaction amount prior to Account Data  
 1858 Retrieval.

1859    4.4.1.1.5    *Remote Transactions at Physical POI and Virtual Terminal*

1860    Req T113:    For MOTO transactions it is the Acceptor that shall confirm the transaction,  
1861                   including the transaction amount.

1862    4.4.1.2    Configuration

1863    4.4.1.2.1    *Local Transactions and Remote Transactions (all Acceptance Environments)*

1864    Req T114:    It shall be possible to configure per Application Profile, if the transaction amount  
1865                   shall be checked against a minimum allowed amount and/or a maximum allowed  
1866                   amount.

1867    4.4.1.2.2    *Local Card Transactions (Physical POI)*

1868    Req T115:    It shall be configured that the Chip with Contact Acceptance Technology and/or  
1869                   the Contactless Acceptance Technology shall be supported (see Req T19) and that  
1870                   the Magnetic Stripe Acceptance Technology is subordinate to the Chip with  
1871                   Contact Acceptance Technology (see Req T23).

1872    Req T116:    For attended POIs that support One-off Payment with increased amount, it shall  
1873                   be possible to configure the POI to support the addition of a gratuity to be entered  
1874                   and confirmed by the Customer.

1875    Req T117:    For the specific Unable-to-go-online processing described in Req T127, the POI  
1876                   Application shall be configurable per Application Profile to either approve the  
1877                   transaction or, for attended POIs, perform a voice authorisation according to  
1878                   scheme rules, or decline.

1879    Req T118:    For attended POIs that support partial approvals of online authorisations it shall  
1880                   be configurable per Application Profile whether partial approvals are activated.

1881    Req T119:    For attended POIs, if the POI is offline with online capability, it shall be possible to  
1882                   configure the POI Application to allow/not allow the attendant to force a  
1883                   transaction online.

1884    Req T120:    For attended POIs, if the POI is offline with online capability or online-only, it shall  
1885                   be possible to configure the POI Application to allow/not allow the attendant to  
1886                   force a declined transaction to be accepted.

1887    Req T121:    For unattended POIs, forcing a declined transaction to be accepted shall not be  
1888                   supported.

1889                   However, for unattended environments where the interaction with the Customer  
1890                   must be minimized because of a need of speed, if the POI is offline with online

1891 capability, it shall be possible to configure the POI Application to allow/not allow  
1892 the transaction approval to be automatically forced.

#### 1893 4.4.1.2.3 *Remote Card Transactions at Physical POI and Virtual Terminal*

1894 Req T122: For attended POIs (Physical POI or Virtual Terminal) that support partial approvals  
1895 of online authorisations, it shall be configurable per Application Profile whether  
1896 partial approvals are activated.

#### 1897 4.4.1.3 Transaction Initialisation

1898 The following requirement applies to Local Transactions and Remote Transactions (all  
1899 Acceptance Environments):

1900 Req T123: For One-off Payment, the transaction amount (i.e. the amount to be authorised,  
1901 which includes any additional amount) shall be available to the POI Application at  
1902 Transaction Initialisation.

#### 1903 4.4.1.4 Authorisation

##### 1904 4.4.1.4.1 *Local and Remote Card Transactions (all Acceptance Environments)*

1905 Req T124: If an online authorisation is required and it is not possible to perform the  
1906 authorisation, the transaction shall be declined.

1907 Req T125: For Authorisation, the transaction amount as defined in Req T123 shall be used.

1908 Req T126: For online authorisation, the authorisation response may return a lower  
1909 authorised amount (partial approval).

1910 If the POI does not support partial approvals for online authorisation or if partial  
1911 approvals are not activated for the Application Profile and the POI receives a  
1912 partial approval it shall decline the transaction.

1913 If partial approvals are supported and activated, the POI shall always return the  
1914 actual authorised amount to the sale system and/or to the attendant.

##### 1915 4.4.1.4.2 *Local Card Transactions (Physical POI)*

1916 Req T127: For Chip with Contact transactions, if it is not possible to perform an online  
1917 authorisation, the EMV Unable-to-go-online processing shall be performed with  
1918 the following extension. If the POI requests an approval, and the Card Application  
1919 approves the transaction, and the amount exceeds the POI floor limit, the POI  
1920 Application shall be configurable per Application Profile whether to approve the



1921		transaction (or for attended POIs perform a voice authorisation according to
1922		scheme rules) or decline.
1923	4.4.1.4.3	<i>Remote Card Transactions at Physical POI and Virtual Terminal</i>
1924	Req T128:	For MOTO, as online authorisation is required if it is not possible to perform an
1925		online or voice authorisation, the transaction shall be declined.
1926	4.4.1.5	<u>Completion</u>
1927	4.4.1.5.1	<i>Local Transactions (Physical POI) and Remote Transactions at the Virtual POI</i>
1928	Req T129:	Any POI which is integrated with the sale system shall send a message to the sale
1929		system to indicate the transaction result.
1930		In addition, for Card Transactions, the POI shall receive the final transaction
1931		amount if different from the authorised amount, from the sale system.
1932	4.4.1.5.2	<i>Local Transactions (Physical POI)</i>
1933	Req T130:	For Card Transactions, the POI shall have mechanisms to ensure that only the
1934		authorised user can force a declined transaction to be accepted.
1935	Req T131:	For Card and ICT Transactions using a Physical Card, to prevent the Customer from
1936		leaving the Physical Card in the unattended POI, card removal shall always be
1937		prompted prior to goods or service delivery.
1938	4.4.1.6	<u>Reversal</u>
1939	These Requirements apply to Local and Remote Card Transactions (all Acceptance	
1940	Environments):	
1941	Req T132:	If the actual amount was authorised but goods or service could not be delivered,
1942		the POI shall receive an indication of this from the sale system. If the transaction
1943		was authorised online, the POI shall then perform a reversal to nullify the original
1944		authorisation.
1945	Req T133:	If the actual amount was authorised but not all the goods or service could be
1946		delivered; the POI shall receive an indication of this from the sale system,
1947		including the reduced amount. If the transaction was authorised online and
1948		capture is not performed immediately, the POI shall then perform a partial
1949		reversal. The captured data shall always include the final, reduced amount.

#### 4.4.2 Refund

For Refund, Local Transactions are Local Customer 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 Present / Local AIT)	Unattended (not allowed)		
Chip with Contact	✓/✗	✗	✗	✗
Magnetic Stripe <sup>64</sup>	✓/✗	✗	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓/✗	✗	✗	✗
Contactless (Chip and Mobile)	✓/✗	✗	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗/✓	✗	✓	✓

TABLE 9: REFUND: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS

1957 The column "Requirement" in Table 10 shows which Functions are not applicable (-) or which are  
1958 either mandatory (M), optional (O) or conditional (C) for the Refund Service and for Local and  
1959 Remote Card Transactions using the respective Acceptance Environments Physical POI (attended  
1960 and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is  
1961 described either in the general or in the Service specific description of the Function.

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (Local Customer 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 <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	O	O	O
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

1962 **TABLE 10: FUNCTIONS USED FOR REFUND**

1963 In addition to the general requirements listed in Section 4.3, the following specific requirements  
 1964 apply to the Refund Service for Local Card Transactions (Physical POI) and for Remote Card  
 1965 Transactions (Virtual POI, Physical POI or Virtual Terminal).

1966 4.4.2.1 POI Application

1967 4.4.2.1.1 *Local Transactions and Remote Transactions (all Acceptance Environments)*

1968 Req T134: The transaction amount shall be checked against a maximum allowed amount if  
 1969 configured for the Application Profile. If the check fails, the transaction shall not  
 1970 proceed.

1971 4.4.2.1.2 *Local Transactions (Physical POI)*

1972 Req T135: For Local Customer Present transactions the Refund Service shall not be initiated  
 1973 by the Customer without the Acceptor being involved.

1974 Req T136: If the Chip with Contact Acceptance Technology or the Contactless Acceptance  
 1975 Technology is used, it is only for the purpose of retrieving the Card Data for the  
 1976 Refund transaction, not to perform a complete EMV based Card Transaction.  
 1977 Therefore, EMV processing shall be followed until the Account Data Retrieval  
 1978 Function has obtained either the Track 2 equivalent data, or the PAN together  
 1979 with the expiry date. If Chip with Contact Acceptance Technology is used, the EMV  
 1980 process shall be terminated by requesting a decline from the EMV Card Payment  
 1981 Application.

1982 4.4.2.2 Configuration

1983 The following requirements apply to Local Transactions and Remote Transactions (all Acceptance  
 1984 Environments):

1985 Req T137: In addition to Req T9, it shall be configurable for the Refund Service to further  
 1986 protect high value amounts using additional security e.g., a supervisor's password.  
 1987 The amount above which this additional security is required shall be configurable.

1988 Req T138: It shall be configurable per Application Profile, whether the Refund is performed  
 1989 online or not.

1990 **4.4.2.3** Transaction Initialisation

1991 The following requirement applies to Local Transactions and Remote Transactions (all  
1992 Acceptance Environments):

1993 Req T139: The Refund amount shall be available to the POI Application at Transaction  
1994 Initialisation. The way to link the Refund transaction to a previous One-off  
1995 Payment is out of scope.

1996 **4.4.2.4** Authorisation

1997 The following requirement applies to Local Transactions and Remote Transactions (all  
1998 Acceptance Environments):

1999 Req T140: If authorisation is required by the Application Profile, then the Refund shall be  
2000 processed online.

2001 **4.4.3** Cancellation

2002 For Cancellation, Local Transactions are Local Customer Present or Local AIT and are always  
2003 attended. Remote Transactions are always Remote AIT.

2004 **Table** 11 shows which combinations of Acceptance Technologies and Acceptance Environments  
2005 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2006 for the Cancellation 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 Present / Local AIT)	Unattended (not allowed)		
Chip with Contact	✓/✗	✗	✗	✗
Magnetic Stripe <sup>64</sup>	✓/✗	✗	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓/✗	✗	✗	✗
Contactless (Chip and Mobile)	✓/✗	✗	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗

Acceptance Technologies	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
	Attended (Local Customer Present / Local AIT)	Unattended (not allowed)		
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗/✓	✗	✓	✓

**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 Customer 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 <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-

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

**TABLE 12: FUNCTIONS USED FOR CANCELLATION**

2013

2014 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2015 apply to the Cancellation Service for Local Card Transactions and Remote Card Transactions (all  
2016 Acceptance Environments).

#### 2017 4.4.3.1 POI Application

##### 2018 4.4.3.1.1 *Local Transactions and Remote Transactions (all Acceptance Environments)*

2019 Req T141: A Cancellation shall always be performed for the full amount of the original  
2020 transaction.

2021 Req T142: When performed for the Pre-Authorisation Services, the Cancellation Service shall  
2022 cancel a Pre-Authorisation and all linked Update Pre-Authorisation(s).

2023 Req T143: The Cancellation Service shall be supported to cancel a Payment Completion.

##### 2024 4.4.3.1.2 *Local Transactions (Physical POI)*

2025 Req T144: For Local Customer Present transactions the Cancellation Service shall not be  
2026 initiated by the Customer without the Acceptor being involved.

2027 Req T145: If the Chip with Contact Acceptance Technology or the Contactless Acceptance  
2028 Technology is used, it is only for the purpose of retrieving the Card Data for the  
2029 Cancellation transaction, not to perform a complete EMV based Card Transaction.  
2030 Therefore, EMV processing shall be followed until the Account Data Retrieval  
2031 Function has obtained either the Track 2 equivalent data, or the PAN together  
2032 with the expiry date. If Chip with Contact Acceptance Technology is used, the EMV



2033 process shall be terminated by requesting a decline from the EMV Card Payment  
2034 Application.

#### 2035 4.4.3.2 Configuration

2036 The following requirements apply to Local Transactions and Remote Transactions (all Acceptance  
2037 Environments):

2038 Req T146: It shall be configurable per Application Profile which of the Payment Services can  
2039 be cancelled.

2040 Req T147: It shall be possible to configure for the POI whether Cancellations shall be  
2041 restricted to the last transaction processed at the POI or may be extended to  
2042 previous transactions.

2043 Req T148: It shall be possible to configure per Application Profile, whether Cancellations shall  
2044 be declined or processed online if the original transaction has already been  
2045 captured to the Acquirer.

2046 Req T149: It shall be possible to configure per Application Profile, whether Cancellations shall  
2047 be declined or sent online, if the original transaction cannot be retrieved in the  
2048 POI.

2049 Req T150: It shall be possible to configure per Application Profile, whether Cancellations shall  
2050 be performed offline or processed online if the original transaction was authorised  
2051 offline and has not been captured to the Acquirer.

#### 2052 4.4.3.3 Authorisation

2053 The following requirements apply to Local Transactions and Remote Transactions (all Acceptance  
2054 Environments):

2055 Req T151: If the original transaction cannot be recognised by the POI or has been already  
2056 captured to the Acquirer, the Cancellation shall either be aborted or be processed  
2057 online according to the configuration of the Cancellation Service.

2058 Req T152: If the original transaction can be recognised by the POI and has not been captured  
2059 to the Acquirer, Cancellation shall be performed as follows:

2060 • If the original transaction was authorised online, Cancellation shall also be  
2061 processed online.

2062 • If the original transaction was authorised offline (only applicable to Local  
2063 Customer Present Transactions), Cancellation shall be either performed offline  
2064 or processed online according to the configuration of the Cancellation Service.

2065 For offline Cancellation either the original transaction data is removed from  
2066 the POI or the cancellation data is stored for capture.

- 2067 • Upon successful online processing of the Cancellation, either the original  
2068 transaction data is removed from the POI or the cancellation data is stored for  
2069 capture.

#### 2070 4.4.3.4 Data Capture

2071 The following requirements apply to Local Transactions and Remote Transactions (all Acceptance  
2072 Environments):

2073 Req T153: Data Capture shall be performed according to the conditions described in T152.

2074 Req T154: Every captured Cancellation transaction shall include a (set of) data element(s)  
2075 uniquely referencing the original transaction.

#### 2076 4.4.4 Pre-Authorisation Services

2077 Pre-Authorisation Services are:

- 2078 • Pre-Authorisation Service (see Section 4.4.4.1.1),  
2079 • Update Pre-Authorisation Service (see Section 4.4.4.1.2) and  
2080 • Payment Completion Service (see Section 4.4.4.2).

2081 Update Pre-Authorisation may either:

- 2082 • Increase the previously authorised amount(s) to reserve funds or,  
2083 • Decrease the previously authorised amount(s) to release funds.

2084 Decreasing the previously authorised amount(s) may be achieved by a reversal or an  
2085 authorisation adjustment.

2086 As soon as the final amount is known, then Payment Completion is used to finalise the  
2087 transaction using the final amount.

2088 In the event that the amount(s) pre-authorised is not used, the previously authorised amount(s)  
2089 are released by the Cancellation Service. In this case Payment Completion does not follow. Note  
2090 that in an unattended environment the Cancellation Service would be initiated automatically by  
2091 the POI application.

2092 For Pre-Authorisation Services, Local Transactions are Local Customer Present, which are  
2093 attended or unattended, or Local AIT, which are attended. At least one of the Pre-Authorisation

2094 Service(s) prior to Payment Completion shall be Local Customer Present. Remote (Update) Pre-  
2095 Authorisation transactions are e- or m-Commerce if performed at the Virtual POI, or MOTO if  
2096 performed at the Physical POI or Virtual Terminal, or Remote AIT. At least one of the Pre-  
2097 Authorisation Service(s) prior to Payment Completion performed at the Virtual POI shall be e- or  
2098 m-Commerce. Remote Payment Completion transactions are always Remote AIT.

2099 It is recommended that at least one of the Pre-Authorisation Service(s) prior to Payment  
2100 Completion is performed based on one of the following Acceptance Technologies:

- 2101 • Chip with Contact,
- 2102 • Contactless,
- 2103 • Consumer Device with Browser over Internet,
- 2104 • Consumer Device with Dedicated Application over Internet.

2105 **Table 13** shows which combinations of Acceptance Technologies and Acceptance Environments  
2106 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2107 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 Customer Present / Local AIT)	Unattended (Local Customer Present)		
Chip with Contact	✓/✗	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓/✗	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓/✗	✗	✗	✓/✗
Contactless (Chip and Mobile)	✓/✗	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>72</sup> /✗
Consumer Device with Browser over Internet	✗	✗	✓/✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓/✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗

<sup>72</sup> On the Virtual Terminal, key entry by cardholder can be performed when a Touch Tone facility, using DTMF, is supported.

Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗/✓	✗	✗/✓	✗/✓

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

2108

2109

#### 4.4.4.1 Pre-Authourisation Service and Update Pre-Authourisation Service

2110

2111

2112

2113

2114

2115

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-Authourisation 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 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 Customer 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 <sup>69</sup>	C/-	C/-	C/-
• Cardholder Verification <sup>69</sup>	C/-	C/-	-

Authorisation	M	M	M
Referral <sup>70</sup>	O/-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	-	-	-

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

2116

#### 2117 4.4.4.1.1 Pre-Authorisation Service

2118 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2119 apply to the Pre-Authorisation Service for Local Card Transactions and Remote Card Transactions  
2120 (all Acceptance Environments).

##### 2121 4.4.4.1.1.1 POI Application

2122 Req T155: The POI shall either receive the amount from the attendant or the sale system or  
2123 use a default amount, which - in both cases - should be an estimated amount (no  
2124 single unit currency), or be based on known or estimated expenditure.

2125 Req T156: If the Customer is participating, the Customer shall be informed of the transaction  
2126 amount and shall be able to confirm the transaction amount and the Customer  
2127 display shall clearly indicate that the amount to be confirmed is an estimated  
2128 amount and is a Pre-Authorisation.

2129 Req T157: For Local Customer Present Transactions, the Customer shall be informed of the  
2130 transaction amount and shall be able to confirm the transaction amount and the  
2131 Payment Brand when performing the CVM.

2132 The only exceptions are when the CVM is No CVM Required or when the  
2133 Cardholder Verification is performed on the Physical Card or Mobile Device before  
2134 the transaction amount is known. In those cases, the Customer shall be informed  
2135 of the transaction amount so that the confirmation of the transaction amount  
2136 shall be implicit by presenting the Physical Card or Mobile Device.

2137 Req T158: A Pre-Authorisation shall be identified as such in authorisation messages and  
2138 transaction data.

2139 Req T159: Data from approved Pre-Authorisations (e.g., PAN and expiry date, amount,  
2140 authorisation code and unique reference) shall be stored for performing  
2141 subsequent steps (i.e. Update Pre-Authorisation, Payment Completion).

2142 Req T160: If an EMV Card Payment Application is used, the appropriate EMV Card Payment  
2143 Application data elements from both the Pre-Authorisation request and response  
2144 must be retained for the Payment Completion Service, including the EMV  
2145 Application Cryptogram(s) (ARQC and, if generated, TC), because all fields needed  
2146 to validate the cryptogram must be included in the Payment Completion record.

2147 *4.4.4.1.1.2 Configuration*

2148 Req T161: The POI Application shall be configurable to allow the Pre-Authorisation amount  
2149 to be received or to be a configurable default amount.

2150 *4.4.4.1.1.3 Card Authentication and Cardholder Verification*

2151 Req T162: The Pre-Authorisation or at least one of the subsequent Update Pre-  
2152 Authorisations shall be performed with Cardholder Verification and, if necessary  
2153 for SCA, with Card Authentication.

2154 *4.4.4.1.1.4 Authorisation*

2155 Req T163: A Pre-Authorisation shall be authorised online in order to reserve the funds.

2156 Req T164: For Pre-Authorisation, the authorisation response message shall contain the  
2157 Transaction Lifecycle Identifier (as defined in Book 3) or corresponding element,  
2158 which is the unique reference to be used to link any subsequent Update Pre-  
2159 Authorisation(s) and the Payment Completion to the Pre-Authorisation.

2160 *4.4.4.1.1.5 Data Capture*

2161 Req T165: Approved Pre-Authorisations shall not be captured.

2162 *4.4.4.1.2 Update Pre-Authorisation Service*

2163 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2164 apply to the Update Pre-Authorisation Service for Local Transactions and Remote Transactions  
2165 (all Acceptance Environments).

2166 *4.4.4.1.2.1 POI Application*

2167 Acceptance Technology for Update Pre-Authorisation may be different from the Pre-  
2168 Authorisation (or previous Update Pre-Authorisation) Acceptance Technology mainly because  
2169 the Payment Device or Customer are normally not present when Up-date Pre-Authorisations are  
2170 being performed.

**2171 Note:**

2172 If the Update Pre-Authorisation is performed based on Stored Card Data obtained in the Pre-  
2173 Authorisation, then the Card Data for an Update Pre-Authorisation will not contain the CSC,  
2174 because it is not allowed to store the CSC after authorisation.

2175 Req T166: An Update Pre-Authorisation shall be identified as such in authorisation messages  
2176 and transaction data and shall contain the unique reference from the original  
2177 linked Pre-Authorisation.

2178 Req T167: An approved Update Pre-Authorisation shall increment or decrement the amount  
2179 of the previously linked Pre-Authorisation and Update Pre-Authorisation(s).

2180 Req T168: Data from approved Update Pre-Authorisations (e.g., amount and authorisation  
2181 code) shall be stored for future use as needed.

2182 If the Update Pre-Authorisation is performed using an EMV Card Payment  
2183 Application then the relevant EMV Card Payment Application data shall be stored  
2184 for subsequent steps.

2185 Req T169: An Update Pre-Authorisation shall include the increment or decrement amount to  
2186 be authorised.

2187 Req T170: If the Customer is participating, the Customer shall be informed of the transaction  
2188 amount and shall be able to confirm the transaction amount and the Customer  
2189 display shall clearly indicate that the amount to be confirmed is the increment or  
2190 decrement amount.

2191 Req T171: For Local Customer Present Transactions, the display shall clearly indicate that the  
2192 amount to be confirmed is an increment or decrement amount. In addition, the  
2193 Customer shall be able to confirm the transaction amount and the Payment Brand  
2194 when performing the CVM.

2195 The only exception is when the CVM is No CVM Required or when the Cardholder  
2196 Verification is performed on the Physical Card or Mobile Device before the  
2197 transaction amount is known. In those cases, the Customer shall be informed of  
2198 the transaction amount so that the confirmation of the transaction amount shall  
2199 be implicit by presenting the Physical Card or Mobile Device.

2200 Req T172: If the Update Pre-Authorisation is declined, the previously linked Pre-  
2201 Authorisation (or Update Pre-Authorisation(s)) shall remain unchanged and valid.

2202 Req T173: As soon as it is known that a Pre-Authorisation and any Update Pre-Authorisation  
2203 linked to it will not be used, the previously authorised amount(s) must be released  
2204 by a Cancellation. In this case Payment Completion shall not follow.



2205    4.4.4.1.2.2    *Card Authentication and Cardholder Verification*

2206    Req T174:    If the Pre-Authorisation was not performed with Cardholder Verification and with  
2207    Card Authentication, then at least one of the subsequent Update Pre-  
2208    Authorisations shall be performed with Cardholder Verification and, if necessary  
2209    for SCA, with Card Authentication.

2210    4.4.4.1.2.3    *Authorisation*

2211    Req T175:    An Update Pre-Authorisation shall be processed online.

2212    4.4.4.1.2.4    *Completion*

2213    Req T176:    The transaction receipt, if any, shall clearly show that this is an Update Pre-  
2214    Authorisation and shall indicate the increment or decrement amount.

2215    4.4.4.1.2.5    *Data Capture*

2216    Req T177:    Approved Update Pre-Authorisations shall not be captured.

2217    4.4.4.2    *Payment Completion Service*

2218    The column "Requirement" in **TABLE 15** shows which Functions are not applicable (-) or which are  
2219    either mandatory (M), optional (O) or conditional (C) for the Payment Completion Service for  
2220    Local and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2221    (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2222    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 Customer Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
Language Selection	M/-	-	-
Transaction Initialisation	M	M	M

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (Local Customer Present / Local AIT)	Virtual POI (always Remote AIT)	Physical POI or Virtual Terminal (always Remote AIT)
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 <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	-	-	-
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	-	-	-
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).

#### 4.4.4.2.1 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.

- 2235 If the accumulated authorised amount is exceeded by the configurable overspent  
2236 percentage allowed by scheme rules, an Update Pre-Authorisation shall be  
2237 performed for the difference, before the Payment Completion Service is  
2238 performed.
- 2239 Req T179: If the Chip with Contact Acceptance Technology or the Contactless Acceptance  
2240 Technology is used, it is only for the purpose of retrieving the Card Data for the  
2241 Payment Completion transaction, not to perform a complete EMV based Card  
2242 Transaction. Therefore, EMV processing shall be followed until the Account Data  
2243 Retrieval Function has obtained either the Track 2 equivalent data, or the PAN  
2244 together with the expiry date. If Chip with Contact Acceptance Technology is used,  
2245 the EMV process shall be terminated by requesting a decline from the EMV Card  
2246 Payment Application.
- 2247 Req T180: A Payment Completion shall be identified as such in transaction data and shall  
2248 contain the unique reference from the original linked Pre-Authorisation.
- 2249 Req T181: A Payment Completion shall include the final amount.
- 2250 Req T182: If the Customer is participating, the POI display shall clearly indicate that the  
2251 amount is the final amount.
- 2252 4.4.4.2.2 *Configuration*
- 2253 Req T183: The POI Application shall be configurable to either perform online capture by  
2254 sending a completion message immediately after the Payment Completion, or  
2255 perform batch capture.
- 2256 4.4.4.2.3 *Data Capture*
- 2257 Req T184: If an EMV Card Payment Application was used in one of the Pre-Authorisation  
2258 Service(s), the Card Data to be used for the Payment Completion Service shall be  
2259 the EMV Card Payment Application data retained from the Pre-Authorisation  
2260 Service.

#### 2261 4.4.5 Deferred Payment

2262 For Deferred Payment, only Local Customer Present Transactions are allowed.

2263 **TABLE 16** shows which combinations of Acceptance Technologies and Acceptance Environments  
 2264 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
 2265 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2266 **TABLE 16: DEFERRED PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

2267 The column "Requirement" in **TABLE 17** shows which Functions are not applicable (-) or which are  
2268 either mandatory (M), optional (O) or conditional (C) for the Deferred Payment Service and for  
2269 Local and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2270 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2271 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 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 <sup>69</sup>	C	-	-
• Cardholder Verification <sup>69</sup>	M	-	-
Authorisation	M	-	-
Referral <sup>70</sup>	O	-	-
Completion	M	-	-
(Partial) Reversal <sup>71</sup>	C	-	-
Data Capture	M	-	-

2272 **TABLE 17: FUNCTIONS USED FOR DEFERRED PAYMENT**

2273 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2274 apply to the Deferred Payment Service for Local Card Transactions (Physical POI).

#### 2275 4.4.5.1 POI Application

2276 Req T185: For Deferred Payment, the unattended POI shall use as transaction amount for  
2277 authorisation either a predefined amount available in the POI Application, or an

- 2278 amount available and provided by the sale system (e.g., a selected amount). The  
2279 predefined amount may be configurable per Application Profile.
- 2280 Req T186: The transaction amount for authorisation shall be checked against a maximum  
2281 allowed amount if configured for the Application Profile. If the check fails, the  
2282 transaction shall not proceed.
- 2283 Req T187: The Customer shall be informed of the transaction amount and shall be able to  
2284 confirm the transaction amount for authorisation and the Payment Brand when  
2285 performing the CVM if confirmation of the transaction amount is configured for  
2286 the Application Profile.
- 2287 If the CVM is No CVM Required or if the Cardholder Verification is performed on  
2288 the Physical Card or Mobile Device before the transaction amount is known, then  
2289 the confirmation of the transaction amount shall either be implicit by informing  
2290 the Customer of the transaction amount prior to presenting the Physical Card or  
2291 Mobile Device, or explicit with a confirmation display showing the transaction  
2292 amount, if confirmation of the transaction amount is configured for the  
2293 Application Profile.
- 2294 4.4.5.2 Configuration
- 2295 Req T188: It shall be configured that the Chip with Contact Acceptance Technology and/or  
2296 the Contactless Acceptance Technology shall be supported (see Req T19) and that  
2297 the Magnetic Stripe Acceptance Technology is subordinate to the Chip with  
2298 Contact Acceptance Technology (see Req T23).
- 2299 Req T189: It shall be possible to configure per Application Profile, if the transaction amount  
2300 shall be checked against a maximum allowed amount.
- 2301 Req T190: For Deferred Payment, it shall be possible to configure per Application Profile, if  
2302 the transaction amount shall be confirmed by the Customer.
- 2303 Req T191: For attended POIs, it shall be possible to configure the POI Application to  
2304 allow/not allow the attendant to force a declined transaction to be accepted.
- 2305 Req T192: It shall be possible to configure for the POI Application the timeframe in which  
2306 reception of the delivery result is expected from the sale system.
- 2307 4.4.5.3 Authorisation
- 2308 Req T193: Deferred Payment shall be authorised online.

2309 Req T194: For Deferred Payment, the authorisation response may return a lower authorised  
2310 amount. In any case the POI shall always return the actual authorised amount to  
2311 the sale system.

#### 2312 4.4.5.4 Reversal

2313 Req T195: Online Reversal shall not be performed if the transaction is declined/aborted after  
2314 an online approval. Instead a notification message with final amount zero shall be  
2315 used as described in T197.

#### 2316 4.4.5.5 Completion

2317 Req T196: The POI shall receive the delivery result from the sale system, including the final  
2318 amount which may be a zero amount.

2319 Req T197: A notification of the final amount that shall not exceed the authorised amount  
2320 (e.g., an Advice message) shall be sent online immediately after the delivery result  
2321 is received. This notification shall also be sent to nullify the effects of the  
2322 authorisation if the final amount is zero (no delivery or a delivery result is not  
2323 received in the configured timeframe).

2324 Req T198: The POI shall send a message to the sale system to indicate the transaction result.

#### 2325 4.4.5.6 Data Capture

2326 Req T199: Data Capture shall be performed either as online capture through a completion  
2327 message sent after each transaction (referred to as notification message in T197)  
2328 or through batch capture.

2329 Data Capture shall always include the final amount. If the final amount is zero Data  
2330 Capture is not required.

#### 2331 4.4.6 No-Show

2332 "No-Show" is processed as MIT, which can only be performed using recorded Card Data  
2333 information including PAN and expiry date, because the reservation process (e.g., of a hotel  
2334 room or a rental car) does not normally involve the Payment Device being present or the EMV  
2335 Card Payment Application being read. This data would have been previously received:

- 2336 • By phone, via a secure fax or from a letter in which case the PAN and expiry date could be  
2337 recorded on a manual folio or on a paper booking schedule.
- 2338 • Electronically from a booking agent or via a web service, in which case it would be  
2339 regarded as "Stored Card Data", which is commonly thought of as electronically stored.



2340 In the event the Payment Device and Customer are physically present at time of the reservation,  
2341 only PAN and expiry date would be taken, for the purposes of the guaranteed reservation, in the  
2342 event a No-Show needs to be processed.

2343 For No-Show, Local Transactions are always Local AIT and attended. Remote Transactions are  
2344 always Remote AIT.

2345 **TABLE 18** shows which combinations of Acceptance Technologies and Acceptance Environments  
2346 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2347 for the 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 <sup>64</sup>	✗	✗	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✗	✗	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✓	✗	✓	✓

2348 **TABLE 18: NO-SHOW: ACCEPTANCE TECHNOLOGY AND ACCEPTANCE ENVIRONMENTS**

2349 The column "Requirement" in **Table 19** shows which Functions are not applicable (-) or which are  
2350 either mandatory (M), optional (O) or conditional (C) for the No-Show Service and for Local and  
2351 Remote Card Transactions using the respective Acceptance Environments Physical POI (attended  
2352 and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional Functions is  
2353 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
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	-	-	-
• Card Authentication <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	M	M	M
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	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 (Virtual POI, attended Physical POI or Virtual Terminal).

#### 4.4.6.1 Authorisation

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

#### 4.4.6.2 Data Capture

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

2363     **4.4.7     Instalment Payment**

2364     The Instalment Payment Service is initiated by a first transaction from the POI which is a One-off  
2365     Payment transaction and contains specific information which identifies it as an Instalment  
2366     Payment transaction and which shall describe the payment schedule and conditions.

2367     The subsequent transactions of an Instalment Payment are MIT where the Card Data used is  
2368     extracted from Stored Card Data. In addition, subsequent transactions of an Instalment Payment  
2369     are not necessarily initiated by the POI that performed the first Instalment Payment transaction.

2370     In particular, for the first transaction Card Authentication and Cardholder Verification may be  
2371     performed whereas in subsequent transactions these Functions will not be performed.

2372     The requirements for the first transaction of an Instalment Payment are described in Section  
2373     4.4.7.1.

2374     The requirements for the subsequent transactions of an Instalment Payment are described in  
2375     Section 4.4.7.2.

2376     **4.4.7.1     First Transaction**

2377     For the first transaction of an Instalment Payment, Local Transactions are always Local Customer  
2378     Present. Remote Transactions are always e- or m-Commerce if performed at the Virtual POI, or  
2379     MOTO if performed at the Physical POI or Virtual Terminal.

2380     **TABLE** 20 shows which combinations of Acceptance Technologies and Acceptance Environments  
2381     used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2382     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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>73</sup>
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

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

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

2384 The column "Requirement" in TABLE 21 shows which Functions are not applicable (-) or which are  
2385 either mandatory (M), optional (O) or conditional (C) for the first transaction of an Instalment  
2386 Payment and for Local and Remote Card Transactions using the respective Acceptance  
2387 Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The  
2388 condition (C) for conditional Functions is described either in the general or in the Service specific  
2389 description of the Function.

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local Customer 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 <sup>69</sup>	C	M	M
• Cardholder Verification <sup>69</sup>	M	M	-
Authorisation	M	M	M
Referral <sup>70</sup>	O	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

2390 **TABLE 21: FUNCTIONS USED FOR FIRST TRANSACTION OF AN INSTALMENT PAYMENT**

2391 In addition to the general requirements listed in Section 4.3, the following specific requirements  
 2392 apply to the first transaction of an Instalment Payment for Local Card Transactions and Remote  
 2393 Card Transactions (all Acceptance Environments).

#### 2394 4.4.7.1.1 *POI Application*

2395 Req T202: The first transaction of an Instalment Payment shall follow the same process as  
 2396 the One-off Payment Service for all available Acceptance Technologies, but using  
 2397 its own configuration.

#### 2398 4.4.7.1.2 *Configuration*

2399 Req T203: The allowed maximum total Instalment amount shall be configurable.

#### 2400 4.4.7.1.3 *Authorisation*

2401 Req T204: The first transaction of an Instalment Payment shall be authorised online and shall  
 2402 include the information which identifies it as the first transaction of an Instalment  
 2403 Payment and how many Instalment Payment transactions shall be made in the  
 2404 payment plan, e.g., 1:6 to indicate that this is the first of 6 Instalment Payment  
 2405 transactions.

#### 2406 4.4.7.1.4 *Data Capture*

2407 Req T205: The data captured for clearing of the first transaction of an Instalment Payment  
 2408 shall include the information which identifies it as the first transaction of an  
 2409 Instalment Payment and how many Instalment Payment transactions shall be  
 2410 made in the payment plan (e.g., 1:6 to indicate the first of 6 Instalment Payment  
 2411 transactions).

#### 2412 4.4.7.2 *Subsequent Transactions*

2413 Regardless what Acceptance Technology or Acceptance Environment was used for the first  
 2414 transaction, subsequent transactions will use Stored Card Data and may be processed by the  
 2415 Acceptor or entirely in the environment of the PSP. The Customer will not be involved.  
 2416 Therefore, for subsequent transactions, Local Transactions are always Local AIT and attended.  
 2417 Remote Transactions are always Remote AIT.

2418 The column "Requirement" in **Table 22** shows which Functions are not applicable (-) or which are  
 2419 either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of an  
 2420 Instalment Payment for Local and Remote Card Transactions using the respective Acceptance  
 2421 Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The

2422 condition (C) for conditional Functions is described either in the general or in the Service specific  
2423 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
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	-	-	-
• Card Authentication <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	M	M	M
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

2424 **TABLE 22:** FUNCTIONS USED FOR SUBSEQUENT TRANSACTIONS OF AN INSTALMENT PAYMENT

2425 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2426 apply to the subsequent transactions of an Instalment Payment for Local Card Transactions and  
2427 Remote Card Transactions (all Acceptance Environments).

#### 2428 4.4.7.2.1 Authorisation

2429 Req T206: Subsequent Instalment Payment transactions shall be authorised online using only  
2430 PAN and expiry date and shall include the information which identifies the  
2431 instalment number being processed from the payment plan (e.g., 3:6 to indicate  
2432 the third of 6 Instalment Payment transactions).

2433    4.4.7.2.2    *Data Capture*

2434    Req T207:    The data captured for clearing of subsequent Instalment Payment transactions  
2435                    shall include the information which identifies the instalment number being  
2436                    processed from the payment plan (e.g., 3:6 to indicate the third of 6 Instalment  
2437                    Payment transactions).

2438    **4.4.8    Recurring Payment**

2439    The Recurring Payment Service applies to One-off Payments and Deferred Payments performed  
2440    on a recurring basis.

2441    The Recurring Payment Service is initiated by a first transaction from the POI with specific  
2442    information which identifies it as the initial transaction for a Recurring Payment.

2443    The subsequent transactions of a Recurring Payment are MIT where the Card Data used is  
2444    extracted from Stored Card Data. In addition, subsequent transactions of a Recurring Payment  
2445    are not necessarily initiated by the POI that performed the first Recurring Payment transaction.

2446    In particular, for the first transaction Card Authentication and Cardholder Verification may be  
2447    performed whereas in subsequent transactions these Functions will not be performed.

2448    The requirements for the first transaction of a Recurring Payment are described in Section  
2449    4.4.8.1.

2450    The requirements for the subsequent transactions of a Recurring Payment are described in  
2451    Section 4.4.8.2.

2452    4.4.8.1    First Transaction

2453    For the first transaction of a Recurring Payment, Local Transactions are always Local Customer  
2454    Present. Remote Transactions are always e- or m-Commerce if performed at the Virtual POI, or  
2455    MOTO if performed at the Physical POI or Virtual Terminal.

2456    **TABLE** 23 shows which combinations of Acceptance Technologies and Acceptance Environments  
2457    used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2458    for the first transaction of a Recurring Payment.



	Local Transactions		Remote Transactions	
	Physical POI		Virtual POI (always e- or m-Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local Customer Present)	Unattended (always Local Customer Present)		
<b>Acceptance Technologies</b>				
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>74</sup>
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

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

<sup>74</sup>

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

2460 The column "Requirement" in **TABLE 24** shows which Functions are not applicable (-) or which are  
2461 either mandatory (M), optional (O) or conditional (C) for the first transaction of a Recurring  
2462 Payment and for Local and Remote Card Transactions using the respective Acceptance  
2463 Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The  
2464 condition (C) for conditional Functions is described either in the general or in the Service specific  
2465 description of the Function.

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local Customer 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 <sup>69</sup>	C	M	M
• Cardholder Verification <sup>69</sup>	M	M	-
Authorisation	M	M	M
Referral <sup>70</sup>	O	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

2466 **TABLE 24: FUNCTIONS USED FOR FIRST TRANSACTION OF A RECURRING PAYMENT**

2467 In addition to the general requirements listed in Section 4.3, the following specific requirements  
 2468 apply to the first transaction of a Recurring Payment for Local Card Transactions (Physical POI), e-  
 2469 and m-Commerce (Virtual POI) and MOTO (Physical POI or Virtual Terminal).

#### 2470 4.4.8.1.1 *POI Application*

2471 Req T208: The first transaction of a Recurring Payment shall follow the same process as the  
 2472 One-off Payment Service for all available Acceptance Technologies, but using its  
 2473 own configuration.

#### 2474 **Note:**

2475 Depending on the use case the One-off Payment may be performed with a  
 2476 zero amount.

#### 2477 4.4.8.1.2 *Authorisation*

2478 Req T209: The first transaction of a Recurring Payment shall be authorised online and it shall  
 2479 contain specific information which identifies it as a Recurring Payment transaction.

#### 2480 4.4.8.1.3 *Data Capture*

2481 Req T210: The data captured for clearing of the first transaction of a Recurring Payment shall  
 2482 additionally contain specific information which identifies it as a Recurring Payment  
 2483 transaction.

#### 2484 4.4.8.2 *Subsequent Transactions*

2485 Regardless what Acceptance Technology or Acceptance Environment was used for the first  
 2486 transaction, subsequent transactions will use Stored Card Data and may be processed by the  
 2487 Acceptor or entirely in the environment of the PSP. The Customer will not be involved.  
 2488 Therefore, for subsequent transactions, Local Transactions are always Local AIT and attended.  
 2489 Remote Transactions are always Remote AIT.

2490 The subsequent transactions may be One-off Payments or Deferred Payments.

2491 The column "Requirement" in **TABLE 25** shows which Functions are not applicable (-) or which are  
 2492 either mandatory (M), optional (O) or conditional (C) for the subsequent transactions of a  
 2493 Recurring Payment Local and Remote Card Transactions using the respective Acceptance  
 2494 Environments Physical POI (attended and unattended), Virtual POI and Virtual Terminal. The  
 2495 condition (C) for conditional Functions is described either in the general or in the Service specific  
 2496 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
Selection of the Payment Solution	M	M	M
• Selection of the Payment Instrument	-	-	-
• Technology Selection	-	-	-
• Selection of the Payment Brand	M	M	M
Account Data Retrieval	M	M	M
Authentication	-	-	-
• Card Authentication <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	M	M	M
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

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

2497

2498 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2499 apply to the subsequent transactions of a Recurring Payment for Local Card Transactions and  
2500 Remote Card Transactions (all Acceptance Environments).

#### 2501 4.4.8.2.1 Configuration

2502 Req T211: If the subsequent transactions are Deferred Payments it shall be possible to  
2503 configure for the POI Application the timeframe in which reception of the delivery  
2504 result is expected from the sale system.

2505    4.4.8.2.2    *Authorisation*

2506    Req T212:    Subsequent Recurring Payment transactions shall be authorised online using only  
2507    PAN and expiry date and shall contain specific information which identifies it as a  
2508    Recurring Payment transaction and indicates whether it is a One-off Payment or a  
2509    Deferred Payment.

2510    4.4.8.2.3    *Reversal*

2511    Req T213:    If the subsequent transactions are Deferred Payments online Reversal shall not be  
2512    performed if the transaction is declined/aborted after an online approval. Instead  
2513    a notification message with final amount zero shall be used as described in T215.

2514    4.4.8.2.4    *Completion*

2515    Req T214:    If the subsequent transactions are Deferred Payments the POI shall receive the  
2516    delivery result from the sale system, including the final amount which may be a  
2517    zero amount.

2518    Req T215:    If the subsequent transactions are Deferred Payments a notification of the final  
2519    amount that shall not exceed the authorised amount (e.g., an Advice message)  
2520    shall be sent online immediately after the delivery result is received. This  
2521    notification shall also be sent to nullify the effects of the authorisation if the final  
2522    amount is zero (no delivery or a delivery result is not received in the configured  
2523    timeframe).

2524    Req T216:    If the subsequent transactions are Deferred Payments the POI shall send a  
2525    message to the sale system to indicate the transaction result.

2526    4.4.8.2.5    *Data Capture*

2527    Req T217:    The data captured for clearing of subsequent Recurring Payment transactions shall  
2528    contain specific information which identifies it as a Recurring Payment transaction  
2529    and indicates whether it is a Payment or a Deferred Payment.

2530    Req T218:    If the subsequent transactions are Deferred Payments Data Capture shall be  
2531    performed either as online capture through a completion message sent after each  
2532    transaction (referred to as notification message in T215) or through batch capture.

2533    Data Capture shall always include the final amount. If the final amount is zero Data  
2534    Capture is not required.

#### 2535 4.4.9 Quasi-Cash Payment

2536 For Quasi Cash Payment, Local Transactions are always Local Customer Present. Remote  
2537 Transactions are always e- or m-Commerce if performed at the Virtual POI, or MOTO if  
2538 performed at the Physical POI or Virtual Terminal.

2539 **TABLE 26** shows which combinations of Acceptance Technologies and Acceptance Environments  
2540 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2541 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>75</sup>
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2542 **TABLE 26: QUASI-CASH PAYMENT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

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

2543 The column "Requirement" in **TABLE 27** shows which Functions are not applicable (-) or which are  
2544 either mandatory (M), optional (O) or conditional (C) for the Quasi-Cash Payment Service and for  
2545 Local and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2546 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2547 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 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 <sup>69</sup>	C	M	M
• Cardholder Verification <sup>69</sup>	M	M	-
Authorisation	M	M	M
Referral <sup>70</sup>	O	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	C	C	C
Data Capture	M	M	M

2548 **TABLE 27: FUNCTIONS USED FOR QUASI-CASH PAYMENT**

2549 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2550 apply to the Quasi-Cash Payment Service for Local Card Transactions and Remote Card  
2551 Transactions (all Acceptance Environments).

2552 4.4.9.1 POI Application

2553 Req T219: The Quasi-Cash Payment shall follow the same process as the One-off Payment  
2554 Service for all available Acceptance Technologies, but using its own configuration.

2555 4.4.9.2 Cardholder Verification

2556 Req T220: 'No CVM Required' shall not be supported for Quasi-Cash Payment transactions.

2557 4.4.9.3 Authorisation

2558 Req T221: The Quasi-Cash Payment shall be authorised online and it shall be identified as a  
2559 Quasi-Cash Payment.

2560 4.4.9.4 Reversal

2561 Req T222: If the actual amount was authorised but items could not be delivered, the POI  
2562 shall receive an indication of this from the sale system. The POI shall then perform  
2563 a reversal to nullify the original authorisation.

2564 Req T223: If the actual amount was authorised but not all items could be delivered; the POI  
2565 shall receive an indication of this from the sale system, including the reduced  
2566 amount. The POI shall then perform a partial reversal. The captured data shall  
2567 always include the final amount.

2568 4.4.9.5 Data Capture

2569 Req T224: The data captured for clearing of a Quasi-Cash Payment shall identify it as a Quasi-  
2570 Cash Payment.



## 2571 4.5 Cash Services

2572 Only Local Card Transactions (Physical POI) are allowed for processing the Cash Services.

### 2573 4.5.1 ATM Cash Withdrawal

2574 An ATM is a specific Unattended POI supporting the ATM Cash Withdrawal Payment Service. In  
2575 this section, "Application" refers to a POI Application that supports the ATM Cash Withdrawal  
2576 Service.

2577 For ATM Cash Withdrawal, only unattended Local Customer Present Transactions are allowed.

2578 **TABLE 28** shows which combinations of Acceptance Technologies and Acceptance Environments  
2579 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2580 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 Customer Present)		
Chip with Contact	✗	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✗	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✗	✗	✗	✗
Contactless (Chip and Mobile)	✗	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2581 **TABLE 28: ATM CASH WITHDRAWAL: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

2582 The column "Requirement" in **TABLE 29** shows which Functions are not applicable (-) or which are  
2583 either mandatory (M), optional (O) or conditional (C) for the ATM Cash Withdrawal Service and  
2584 for Local and Remote Card Transactions using the respective Acceptance Environments Physical  
2585 POI (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for

2586 conditional Functions is described either in the general or in the Service specific description of  
2587 the Function.

Function	Requirement		
	Local Transactions	Remote Transactions	
	Physical POI (always Local Customer 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 <sup>69</sup>	C	-	-
• Cardholder Verification <sup>69</sup>	M	-	-
Authorisation	M	-	-
Referral <sup>70</sup>	-	-	-
Completion	M	-	-
(Partial) Reversal <sup>71</sup>	C	-	-
Data Capture	M	-	-

2588 **TABLE 29: FUNCTIONS USED FOR ATM CASH WITHDRAWAL**

2589 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2590 apply to the ATM Cash Withdrawal Service for Local Card Transactions (Physical POI).

#### 2591 4.5.1.1 Configuration

2592 Req T225: It shall be configured that the Chip with Contact Acceptance Technology shall be  
2593 supported (see Req T19) and that the Magnetic Stripe Acceptance Technology is  
2594 subordinate to the Chip with Contact Acceptance Technology (see Req T23).

2595    4.5.1.2    Transaction Initialisation

- 2596    Req T226:    The Welcome Screen shall be shown initially in the default language and English  
2597                    (or in the default language only if it is English).
- 2598    Req T227:    Transactions on the ATM shall be initiated by insertion or presentment of a  
2599                    Physical Card, presentment of a Mobile Device or by Customer interaction.

2600    4.5.1.3    Authorisation

- 2601    Req T228:    ATM Cash Withdrawal transactions shall be authorised online. Otherwise ATM  
2602                    transactions shall be declined.

2603    4.5.1.4    Completion

- 2604    Req T229:    To minimise the risk of the Customer leaving the Physical Card in the ATM; if the  
2605                    Customer did not confirm proceeding with more transactions after the Cash  
2606                    Withdrawal, then the card removal shall always be prompted prior to the cash  
2607                    delivery.
- 2608    Req T230:    If the Physical Card is inserted in the reader of an ATM with card capture capability  
2609                    and if the Customer does not retrieve the Card, the Card shall be retained.
- 2610    Req T231:    If the Physical Card is retained in response to the authorisation response message,  
2611                    an appropriate message shall be displayed to inform the Customer.
- 2612    Req T232:    An ATM shall not allow a declined transaction to be accepted.
- 2613    Req T233:    For ATM Cash Withdrawal transactions using the Contactless Acceptance  
2614                    Technology further transactions after the Cash Withdrawal are not allowed  
2615                    without new presentment of the Physical Card or Mobile Device.

2616    4.5.1.5    Reversal

- 2617    Req T234:    If the actual amount was authorised but cash could not be delivered, a reversal  
2618                    shall be performed to nullify the original authorisation.
- 2619    Req T235:    If the actual amount was authorised but only part of the requested cash could be  
2620                    prepared for delivery and if the ATM supports detection of partial delivery of cash,  
2621                    the ATM shall then perform a partial reversal. The captured data shall always  
2622                    include the final, reduced amount.

2623 **4.5.2 Cash Advance (Attended)**

2624 For Cash Advance, only attended Local Customer Present Transactions are allowed.

2625 **TABLE 30** shows which combinations of Acceptance Technologies and Acceptance Environments  
2626 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2627 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 Customer Present)	Unattended (not allowed)		
Chip with Contact	✓	✗	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✗	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✗	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2628 **TABLE 30: CASH ADVANCE: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

2629 The column "Requirement" in **TABLE 31** shows which Functions are not applicable (-) or which are  
2630 either mandatory (M), optional (O) or conditional (C) for the Cash Advance Service and for Local  
2631 and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2632 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2633 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 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 <sup>69</sup>	C	-	-
• Cardholder Verification <sup>69</sup>	M	-	-
Authorisation	M	-	-
Referral <sup>70</sup>	O	-	-
Completion	M	-	-
(Partial) Reversal <sup>71</sup>	C	-	-
Data Capture	M	-	-

2634 **TABLE 31: FUNCTIONS USED FOR CASH ADVANCE**

2635 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2636 apply to the Cash Advance Service for Local Card Transactions (Physical POI).

#### 2637 4.5.2.1 POI Application

2638 Req T236 The Cash Advance Service shall follow the same process as the One-off Payment  
2639 Service for all available Acceptance Technologies, but using its own configuration.

2640 4.5.2.2 Configuration

2641 Req T237: For Cash Advance, it shall be configured that the Chip with Contact Acceptance  
2642 Technology and/or the Contactless Acceptance Technology shall be supported  
2643 (see Req T19) and that the Magnetic Stripe Acceptance Technology is subordinate  
2644 to the Chip with Contact Acceptance Technology (see Req T23).

2645 Req T238: It shall be possible to configure per Application Profile, if the transaction amount  
2646 shall be checked against a minimum allowed amount and/or a maximum allowed  
2647 amount.

2648 4.5.2.3 Transaction Initialisation

2649 Req T239: For Cash Advance, the transaction amount (i.e. the authorised amount) shall be  
2650 available to the POI Application at Transaction Initialisation.

2651 4.5.2.4 Cardholder Verification

2652 Req T240: No CVM Required shall not be supported for the Cash Advance Service.

2653 4.5.2.5 Authorisation

2654 Req T241: Cash Advance transactions shall be authorised online. If the Referral Function is  
2655 activated and a Referral is received in the Authorisation Response message, the  
2656 Voice Authorisation process shall be followed. Otherwise Cash Advance  
2657 transactions shall be declined.

2658 4.5.2.6 Reversal

2659 Req T242: If the actual amount was authorised but cash could not be delivered, a reversal  
2660 shall be performed to nullify the original authorisation.

## 2661 4.6 Card Enquiry Services

### 2662 4.6.1 Card Validity Check

2663 For Card Validity Check, Local Transactions are Local Customer Present, which are attended or  
 2664 unattended, or Local AIT, which are attended. Remote Transactions are e- or m-Commerce if  
 2665 performed at the Virtual POI, or MOTO if performed at the Physical POI or Virtual Terminal, or  
 2666 Remote AIT.

2667 **TABLE 32** shows which combinations of Acceptance Technologies and Acceptance Environments  
 2668 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
 2669 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 Customer Present / Local AIT)	Unattended (Local Customer Present)		
Chip with Contact	✓/✗	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓/✗	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓/✗	✗	✗	✓/✗
Contactless (Chip and Mobile)	✓/✗	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>76</sup> /✗
Consumer Device with Browser over Internet	✗	✗	✓/✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓/✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗/✓	✗	✗/✓	✗/✓

2670 **TABLE 32: CARD VALIDITY CHECK: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

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

2671 The column "Requirement" in **TABLE 33** shows which Functions are not applicable (-) or which are  
2672 either mandatory (M), optional (O) or conditional (C) for the Card Validity Check Service and for  
2673 Local and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2674 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2675 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 Customer 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 <sup>69</sup>	C/-	C/-	O/-
• Cardholder Verification <sup>69</sup>	O/-	O/-	-
Authorisation	M	M	M
Referral <sup>70</sup>	-	-	-
Completion	M	M	M
(Partial) Reversal <sup>71</sup>	-	-	-
Data Capture	-	-	-

2676 **TABLE 33: FUNCTIONS USED FOR CARD VALIDITY CHECK**



2677 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2678 apply to the Card Validity Check Service for Local Card Transactions and Remote Card  
2679 Transactions (all Acceptance Environments).

2680 **4.6.1.1**     *POI Application*

2681 Req T243:     A Card Validity Check transaction shall be performed like a One-off Payment  
2682 transaction, but using its own configuration and without displaying and printing  
2683 the transaction amount.

2684 **4.6.1.2**     *Transaction Initialisation*

2685 Req T244:     For Card Validity Check, the authorised amount sent to the EMV Card Payment  
2686 Application shall be set to zero.

2687 **4.6.1.3**     *Authorisation*

2688 Req T245:     Card Validity Check transactions shall be authorised online. Otherwise Card  
2689 Validity Check transactions shall be declined.

2690 Req T246:     Card Validity Check transactions shall be identified as such in the online  
2691 authorisation request.

2692 **4.6.1.4**     *Data Capture*

2693 Req T247:     Card Validity Check transactions shall not be captured for "Financial Presentment".

2694 **4.6.2**       **Balance Enquiry**

2695 For Balance Enquiry, only Local Customer Present Transactions are allowed.

2696 **TABLE 34** shows which combinations of Acceptance Technologies and Acceptance Environments  
2697 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2698 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✗	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✗	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2699 **TABLE 34: BALANCE ENQUIRY: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

2700 The column "Requirement" in **TABLE 35** shows which Functions are not applicable (-) or which are  
2701 either mandatory (M), optional (O) or conditional (C) for the Balance Enquiry Service and for  
2702 Local and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2703 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2704 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 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 <sup>69</sup>	C	-	-
• Cardholder Verification <sup>69</sup>	M	-	-
Authorisation	M	-	-
Referral <sup>70</sup>	-	-	-
Completion	M	-	-
(Partial) Reversal <sup>71</sup>	-	-	-
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).

#### 4.6.2.1 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.

2712 4.6.2.2 Transaction Initialisation

2713 Req T249: For Balance Enquiry, the authorised amount sent to the EMV Card Payment  
2714 Application shall be set to zero.

2715 4.6.2.3 Authorisation

2716 Req T250: Balance Enquiry transactions shall be authorised online. Otherwise Balance  
2717 Enquiry transactions shall be declined.

2718 Req T251: Balance Enquiry transactions shall be identified as such in the online authorisation  
2719 request.

2720 Req T252: The balance of the Card Account shall only be retrieved from a positive  
2721 authorisation response.

2722 4.6.2.4 Completion

2723 Req T253: If the balance of the Card Account is retrieved from a positive authorisation  
2724 response, it shall be displayed to the Customer and printed on the Customer  
2725 receipt, if any.

2726 Req T254 If Balance Enquiry is performed in an attended Acceptance Environment, the  
2727 balance shall not be displayed to the attendant or printed on a merchant receipt.

2728 **4.7 Card Electronic Transfer**

2729 **4.7.1 Card Funds Transfer**

2730 For the Card Funds Transfer Service it has to be distinguished whether the Card Account is  
2731 credited or debited.

2732 A credit of the Card Account is only allowed from an account that may be accessed by the owner  
2733 of the Card Account to be credited. Such an account is called Funding Account. There may be  
2734 more than one Funding Account for a Card Account. If several Funding Accounts are defined for a  
2735 Card Account, one of these accounts shall be defined as default. The entity that processes  
2736 authorisations for the Card Account shall know the Funding Account(s) defined for the Card  
2737 Account and which is the default Funding Account. In addition, this entity shall be able to get  
2738 authorisation for debiting the Funding Account(s). It is out of scope how this is achieved.

2739 The Acceptor for the Card Funds Transfer is not involved in the funds transfer to or from the Card  
2740 Account but may receive a fee for offering the Service.

2741 For Card Funds Transfer, Local Transactions are always Local Customer Present. Remote  
2742 Transactions are always e- or m-Commerce.

2743 **TABLE** 36 shows which combinations of Acceptance Technologies and Acceptance Environments  
2744 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2745 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

**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 Customer 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 <sup>69</sup>	C	M	-
• Cardholder Verification <sup>69</sup>	M	M	-
Authorisation	M	M	-
Referral <sup>70</sup>	-	-	-
Completion	M	M	-
(Partial) Reversal <sup>71</sup>	C	C	-
Data Capture	C	C	-

2752 **TABLE 37: FUNCTIONS USED FOR CARD FUNDS TRANSFER**

2753 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2754 apply to the Card Funds Transfer Service for Local Card Transactions (Physical POI) and Card  
2755 based e- and m-Commerce transactions (Virtual POI).

2756 **4.7.1.1 POI Application**

2757 Req T255: The Card Funds Transfer shall follow the same process as the One-off Payment  
2758 Service for all available Acceptance Technologies, but using its own configuration.

2759 **4.7.1.2 Transaction Initialisation**

2760 Req T256: The Customer shall be able to select whether funds shall be transferred to the  
2761 Card Account from another account (Funding Account) or whether funds shall be  
2762 transferred from the Card Account to another account.

2763 Req T257: The Customer shall be able to select the transaction amount to be credited to or  
2764 debited from the Card Account.

2765 Req T258: If an EMV Card Payment Application or a (Mobile) Remote Card Payment  
2766 Application is used to process the Card Funds Transfer transaction, it is only for  
2767 the purpose of retrieving the Card Data, not to perform a complete EMV based  
2768 Card Transaction.

2769 **4.7.1.3 Account Data Retrieval**

2770 Req T259: If funds shall be transferred to the Card Account from a Funding Account the  
2771 Customer shall have the opportunity either to select the default Funding Account

2772		or to provide information to identify one of the other Funding Accounts, if any. If
2773		an EMV Card Payment Application or a (Mobile) Remote Card Payment Application
2774		is used to process the Card Funds Transfer transaction, this information may be
2775		retrieved from the Payment Application.
2776	Req T260:	If funds shall be transferred from the Card Account to another account the
2777		Customer shall have the opportunity to provide information to identify the
2778		account to be credited.
2779	Req T261:	After the Account Data Retrieval Function has obtained either the relevant Card
2780		Data (e.g., the Track 2 equivalent data), or the PAN together with the expiry date,
2781		the Acceptor may decide to raise a fee for the Card Funds Transfer Service.
2782		The Customer shall be informed of any fee to be paid to the Acceptor for the Card
2783		Funds Transfer and the Customer shall have the opportunity to accept or decline
2784		the conditions of the Card Funds Transfer.
2785	4.7.1.4	<u>Authorisation</u>
2786	Req T262:	Card Funds Transfer transactions shall be authorised online and shall be identified
2787		as Card Funds Transfer.
2788	Req T263:	The authorisation message shall identify the amount to be credited to or debited
2789		from the Card Account, the account to be debited or credited, and any fee raised
2790		by the Acceptor as an additional amount.
2791	4.7.1.5	<u>Data Capture</u>
2792	Req T264:	Data Capture for "Financial Presentment" is required only if the Acceptor raises a
2793		fee for the Card Funds Transfer.



#### 2794 4.7.2 Original Credit

2795 For Original Credit, Local Transactions are always Local Customer Present and attended. Remote  
2796 Transactions are always e- or m-Commerce.

2797 **TABLE 38** shows which combinations of Acceptance Technologies and Acceptance Environments  
2798 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2799 for the Original Credit 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 Customer Present)	Unattended (not allowed)		
Chip with Contact	✓	✗	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✗	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✗
Contactless (Chip and Mobile)	✓	✗	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✗
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated Application over Internet	✗	✗	✓	✗
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✗	✗

2800 **TABLE 38: ORIGINAL CREDIT: ACCEPTANCE TECHNOLOGIES AND ACCEPTANCE ENVIRONMENTS**

2801 The column "Requirement" in **TABLE 39** shows which Functions are not applicable (-) or which are  
2802 either mandatory (M), optional (O) or conditional (C) for the Original Credit Service and for Local  
2803 and Remote Card Transactions using the respective Acceptance Environments Physical POI  
2804 (attended and unattended), Virtual POI and Virtual Terminal. The condition (C) for conditional  
2805 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 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	-	-	-
• Card Authentication <sup>69</sup>	-	-	-
• Cardholder Verification <sup>69</sup>	-	-	-
Authorisation	O	O	-
Referral <sup>70</sup>	-	-	-
Completion	M	M	-
(Partial) Reversal <sup>71</sup>	C	C	-
Data Capture	M	M	-

2806 **TABLE 39: FUNCTIONS USED FOR ORIGINAL CREDIT**

2807 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2808 apply to the Original Credit Service for Local Card Transactions (Physical POI) and Card based e-  
2809 and m-Commerce (Virtual POI).

2810 4.7.2.1 POI Application

2811 Req T265: For Local Customer Present transactions the Original Credit Service shall not be  
2812 initiated by the Customer without the Acceptor being involved.

2813 Req T266: If the Chip with Contact Acceptance Technology or the Contactless Acceptance  
2814 Technology is used, it is only for the purpose of retrieving the Card Data for the  
2815 Original Credit transaction, not to perform a complete EMV based Card  
2816 Transaction. Therefore, EMV processing shall be followed until the Account Data  
2817 Retrieval Function has obtained either the Track 2 equivalent data, or the PAN  
2818 together with the expiry date. If Chip with Contact Acceptance Technology is used,  
2819 the EMV process shall be terminated by requesting a decline from the EMV Card  
2820 Payment Application.

2821 If a (Mobile) Remote Card Payment Application is used to process the Original  
2822 Credit transaction, the Payment Application processing shall be terminated after  
2823 the Account Data Retrieval Function has obtained either the relevant card data  
2824 (e.g., the Track 2 equivalent data), or the PAN together with the expiry date.

2825 If the Payment Application requires entry of an amount, the amount given to the  
2826 Payment Application during the Original Credit should be zero to avoid  
2827 unnecessary Card Risk Management.

2828 Req T267: The transaction amount shall be checked against a maximum allowed amount if  
2829 configured for the Application Profile. If the check fails, the transaction shall not  
2830 proceed.

2831 4.7.2.2 Configuration

2832 Req T268: The maximum amount and the allowed maximum amount that can be performed  
2833 without additional security (e.g., a supervisor password) shall be configurable for  
2834 the Original Credit Service.

2835 Req T269: It shall be configurable per Application Profile, whether the Original Credit is  
2836 performed online or not.

2837 4.7.2.3 Transaction Initialisation

2838 Req T270: The Original Credit amount shall be available to the POI Application at Transaction  
2839 Initialisation.

2840 4.7.2.4 Authorisation

2841 Req T271: If authorisation is required by the Application Profile, then the Original Credit shall  
2842 be authorised online.

2843 4.7.3 Prepaid Card - Loading & Unloading

2844 The Prepaid Card Loading Service requires that the Customer has provided funds to the issuer of  
2845 the Prepaid Card which is subsequently used to fund the load transaction. The Prepaid Card  
2846 Unloading Service requires that the issuer of the Prepaid Card has agreed which account of the  
2847 Customer shall be used to unload the prepaid Card Account.

2848 The Acceptor for the Prepaid Card - Loading & Unloading is not involved in the funds transfer to  
2849 or from the Prepaid Card account but may receive a fee for offering the Service.

2850 For Prepaid Card Loading, Local Transactions are always Local Customer Present. Remote  
2851 Transactions are always e- or m-Commerce if performed at the Virtual POI, or MOTO if  
2852 performed at the Physical POI or Virtual Terminal.

2853 **TABLE 40** shows which combinations of Acceptance Technologies and Acceptance Environments  
2854 used in Local and Remote Card Transactions are allowed (✓) or not allowed/not applicable (✗)  
2855 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 Customer Present)	Unattended (always Local Customer Present)		
Chip with Contact	✓	✓	✗	✗
Magnetic Stripe <sup>64</sup>	✓	✓	✗	✗
Manual Entry (by Acceptor) <sup>64</sup>	✓	✗	✗	✓
Contactless (Chip and Mobile)	✓	✓	✗	✗
Manual Entry (by Customer)	✗	✗	✗	✓ <sup>77</sup>
Consumer Device with Browser over Internet	✗	✗	✓	✗
Consumer Device with Dedicated	✗	✗	✓	✗

<sup>77</sup> 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-Commerce)	Physical POI or Virtual Terminal (always MOTO)
	Attended (always Local Customer Present)	Unattended (always Local Customer Present)		
Application over Internet				
Merchant-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Consumer-presented QR Code <sup>67</sup>	✗	✗	✗	✗
Stored Account Data <sup>68</sup>	✗	✗	✓	✗

**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 Customer 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 <sup>69</sup>	C	M	M
• Cardholder Verification <sup>69</sup>	M	M	M

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

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

2863

2864 In addition to the general requirements listed in Section 4.3, the following specific requirements  
2865 apply to the Prepaid Card - Loading & Unloading Service for Local Card Transactions and Remote  
2866 Card Transactions (all Acceptance Environments).

#### 2867 4.7.3.1 POI Application

2868 Req T272: The Prepaid Card - Loading & Unloading shall follow the same process as the One-  
2869 off Payment Service for all available Acceptance Technologies, but using its own  
2870 configuration.

#### 2871 4.7.3.2 Transaction Initialisation

2872 Req T273: The Customer shall be able to select whether the Prepaid Card shall be loaded or  
2873 unloaded.

2874 Req T274: The Customer shall be able to select the transaction amount to be loaded to or  
2875 unloaded from the Prepaid Card account.

2876 Req T275: If an EMV Card Payment Application or a (Mobile) Remote Card Payment  
2877 Application is used to process the Prepaid Card - Loading & Unloading transaction  
2878 the amount given to the Payment Application during the Prepaid Card - Loading &  
2879 Unloading shall be set to zero to avoid unnecessary Card Risk Management.

#### 2880 4.7.3.3 Account Data Retrieval

2881 Req T276: After the Account Data Retrieval Function has obtained either the relevant Card  
2882 Data (e.g., the Track 2 equivalent data), or the PAN together with the expiry date,

2883 the Acceptor may decide to raise a fee for the Prepaid Card - Loading & Unloading  
2884 Service.

2885 The Customer shall be informed of any fee to be paid to the Acceptor for the  
2886 Prepaid Card - Loading & Unloading and the Customer shall have the opportunity  
2887 to accept or decline the conditions of the Prepaid Card - Loading & Unloading.

2888 4.7.3.4 Authorisation

2889 Req T277: Prepaid Card - Loading & Unloading transactions shall be authorised online and  
2890 shall be identified as Prepaid Card - Loading & Unloading.

2891 Req T278: The authorisation message shall identify the amount to be loaded or unloaded and  
2892 any fee raised by the card acceptor as an additional amount.

2893 4.7.3.5 Data Capture

2894 Req T279: Data Capture for "Financial Presentment" is required only if the Acceptor raises a  
2895 fee for the Prepaid Card - Loading & Unloading.

2896    **4.8        Additional Features**

2897    **4.8.1      One-off Payment with Increased Amount**

2898    Req T280:    One-off Payment with Increased Amount shall be restricted to the One-off  
2899                    Payment Service at the attended Physical POI.

2900    Req T281:    Any extra amount shall be included in the transaction amount before or during  
2901                    Transaction Initialisation.

2902    Req T282:    The extra amount shall be displayed separately for transaction confirmation and  
2903                    printed on the receipt, if any.

2904    **4.8.2      One-off Payment with Cashback**

2905    Req T283:    All requirements applicable to the One-off Payment Service shall also apply to  
2906                    One-off Payment with Cashback. Requirements that are specific for One-off  
2907                    Payment with Cashback are listed below.

2908    Req T284:    One-off Payment with Cashback shall be restricted to the One-off Payment Service  
2909                    at the attended Physical POI.

2910    Req T285:    For a One-off Payment with Cashback, the transaction amount shall be the sum of  
2911                    the payment amount and the Cashback amount.

2912    Req T286    The Cashback amount shall be identified separately in the authorisation and  
2913                    settlement messages.

2914    Req T287:    For a One-off Payment with Cashback transaction, the Cashback amount to be  
2915                    confirmed shall be displayed to the Customer in one of the following ways:

2916                    • Payment amount, Cashback amount and (total) transaction amount shall be  
2917                    displayed in this order. This method is preferred and shall be used if the  
2918                    display size permits.

2919                    • Cashback amount and (total) transaction amount shall be displayed.

2920    Req T288:    Customer confirmation of the Cashback amount shall be implicit with the  
2921                    confirmation of the transaction amount.

2922    Req T289:    For attended POIs that support One-off Payment with Cashback, it shall be  
2923                    possible to configure per Application Profile to support the addition of a Cashback  
2924                    amount or not.



- 2925 Req T290: For attended POIs that support One-off Payment with Cashback, it shall be  
2926 possible to configure per Application Profile a maximum Cashback amount.
- 2927 Req T291: For attended POIs that support One-off Payment with Cashback, it shall be  
2928 possible to configure whether the POI Application supports magnetic stripe  
2929 processing for One-off Payment with Cashback.
- 2930 Req T292: One-off Payment with Cashback transactions shall be authorised online.
- 2931 Req T293: The POI Application shall support handling of an authorisation response indicating  
2932 the payment part is authorised but the Cashback is not.
- 2933 Req T294: If a receipt is printed for a One-off Payment with Cashback transaction, then in  
2934 addition to the data listed in Req T94 the following data shall also be printed:
- 2935 • Payment amount
  - 2936 • Cashback amount
- 2937 **4.8.3 One-off Payment with Purchasing or Corporate Card Data**
- 2938 Req T295: For a POI Application that supports One-off Payment with Purchasing or Corporate  
2939 Card Data it shall be configurable per Application Profile whether this additional  
2940 feature is activated for One-off Payment.
- 2941 Req T296: If a POI Application supports One-off Payment with Purchasing or Corporate Card  
2942 Data and if this additional feature is activated the POI shall be able to distinguish a  
2943 purchasing or corporate Card Data, from Card Data of other products in that  
2944 scheme.
- 2945 Req T297: If a One-off Payment transaction is performed with Card Data for which the One-  
2946 off Payment with Purchasing or Corporate Card Data is activated in the POI  
2947 Application, the additional data required for clearing of One-off Payments with  
2948 Purchasing or Corporate Card Data shall be stored and captured at the POI.

2949     **4.8.4     One-off Payment with Aggregated Amount**

2950     Req T298:     When batch capture is used, if allowed by scheme rules, the One-off Payment  
2951                   transactions may be aggregated by the acceptor before sending the transactions  
2952                   to the acquirer for capture.

2953     Req T299:     When online capture methods are used, if allowed by scheme rules, only the  
2954                   Acquirer may aggregate the One-off Payment transactions.

2955     Req T300:     The maximum amount of the aggregated One-off Payment transactions shall be  
2956                   defined by Scheme rules.

2957     Req T301:     EMV Card Payment Application and (Mobile) Remote Card Payment Application  
2958                   based One-off Payment transactions shall be aggregated separately from One-off  
2959                   Payment transactions based on other Acceptance Technologies.

2960     Req T302:     For aggregated EMV Card Payment Application or (Mobile) Remote Card Payment  
2961                   Application based One-off Payment transactions, the cryptogram of the last  
2962                   aggregated transaction shall be sent together with the data elements used to  
2963                   calculate it.

2964     Req T303:     The aggregation can only be made for the One-off Payment transactions with the  
2965                   same PAN, the same merchant and for a maximum period of time. The maximum  
2966                   period of time is defined by scheme rules.

2967     **4.8.5     One-off Payment with Deferred Authorisation**

2968     Req T304:     With the exception of Completion and Data Capture, all requirements applicable  
2969                   to the One-off Payment Service shall also apply to One-off Payment with Deferred  
2970                   Authorisation. Requirements that are specific for One-off Payment with Deferred  
2971                   Authorisation are listed below.

2972     Req T305:     One-off Payment with Deferred Authorisation shall be restricted to the One-off  
2973                   Payment Service at the Physical POI.

2974     Req T306     It shall be possible for the attendant or the sale system to request the subsequent  
2975                   One-off Payment or One-off Payments to be performed with Deferred  
2976                   Authorisation.

2977     Req T307     It shall be configurable whether all One-off Payments are performed with  
2978                   Deferred Authorisation.

2979     Req T308:     It shall be configurable whether Deferred Authorisation, in case unable to go  
2980                   online is detected during a One-off Payment transaction, is not initiated, or is  
2981                   initiated automatically, or is only initiated after confirmation by an Attendant.

2982	Req T309:	It shall be configurable which of the Acceptance Technologies supported for One-off Payment are allowed for Deferred Authorisation.
2983		
2984	Req T310:	It shall be possible to activate/deactivate Deferred Authorisation for One-off Payment per Application Profile.
2985		
2986	Req T311:	A minimum and a maximum amount for One-off Payment with Deferred Authorisation shall be configurable per Application Profile.
2987		
2988	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.
2989		
2990		
2991	Req T313:	It shall be configurable per Application Profile whether Deferred Authorisation shall only be allowed for Payment Application based transactions if Offline Data Authentication was successfully performed.
2992		
2993		
2994	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.
2995		
2996		
2997		
2998		
2999		
3000		If necessary according to the Application Profile configuration, confirmation of an attendant shall be requested for Deferred Authorisation.
3001		
3002	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.
3003		
3004		
3005		
3006		
3007	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 (display and receipt, if any).
3008		
3009		
3010	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 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.
3011		
3012		
3013		
3014		
3015		
3016	Req T318:	If Deferred Authorisation has been performed for an EMV Card Payment Application or (Mobile) Remote Card Payment Application based transaction, the
3017		

3018 cryptogram of the original transaction together with the data elements used for its  
3019 calculation shall also be used for Data Capture.

#### 3020 **4.8.6 Dynamic Currency Conversion (DCC)**

3021 DCC is an additional feature which may be used for One-off Payment and Cash Services.

3022 Req T319: It shall be configurable per Application Profile, whether DCC is supported.

3023 Req T320: To perform DCC, the POI or attendant shall give the Customer the choice of  
3024 currency to be used, the cardholder billing currency or the card acceptor's  
3025 currency.

3026 To make this choice, before confirming the One-off Payment, the Customer shall  
3027 be informed of

- 3028 • The original transaction amount in the card acceptor's currency,
- 3029 • The transaction amount in the cardholder billing currency,
- 3030 • The conversion rate (ratio) used to calculate the amount in the cardholder  
3031 billing currency and
- 3032 • The total currency conversion charges as a percentage mark-up over the latest  
3033 available euro foreign exchange reference rates issued by the European  
3034 Central Bank (ECB).

3035 Req T321: If the POI is used to offer the choice to the Customer the following items shall be  
3036 displayed to the Customer:

- 3037 • The original transaction amount in the card acceptor's currency together with  
3038 an indication of the currency,
- 3039 • The transaction amount in the cardholder billing currency together with an  
3040 indication of the currency,
- 3041 • The conversion rate (ratio) between these two amounts and
- 3042 • The total currency conversion charges as a percentage mark-up over the latest  
3043 available euro foreign exchange reference rates issued by the European  
3044 Central Bank (ECB),

3045 And the Customer shall have the opportunity to select the currency the  
3046 transaction will be performed in.

3047 Req T322: If the Customer selects the transaction amount in the cardholder billing currency,  
3048 then the total transaction amount and, if applicable, a Cashback amount shall be

- 3049 in the cardholder billing currency. Cash obtained from the card acceptor in the  
3050 process of Cashback shall be in the card acceptor's currency.
- 3051 Req T323: If the Customer has selected the transaction amount in the cardholder billing  
3052 currency, the amounts shall be conveyed to the Customer in both the cardholder  
3053 billing currency and the card acceptor's currency. The conversion rate used and  
3054 the mark-up over the latest available euro foreign exchange reference rates issued  
3055 by the European Central Bank (ECB) shall also be included.
- 3056 Req T324: If the Customer has selected the transaction amount in the cardholder billing  
3057 currency and if a transaction receipt is being produced, the amounts shown on the  
3058 receipt shall be expressed in the cardholder billing currency and in the card  
3059 acceptor's currency. The conversion rate used and the mark-up over the latest  
3060 available euro foreign exchange reference rates issued by the European Central  
3061 Bank (ECB) shall also be included.
- 3062 Req T325: If for a Contact EMV Card Payment Application or (Mobile) Remote Card Payment  
3063 Application based transaction, data from the Contact EMV Card Payment  
3064 Application or (Mobile) Remote Card Payment Application are needed to  
3065 determine the cardholder billing currency, then the transaction shall be started  
3066 with the card acceptor's currency. If after the retrieval of the necessary data the  
3067 Customer has selected the transaction amount in the cardholder billing currency,  
3068 then the Contact EMV Card Payment Application or (Mobile) Remote Card  
3069 Payment Application based transaction shall be re-started without further  
3070 Customer interaction with the previously selected Payment Application.
- 3071 **4.8.7 Surcharging/Rebate**
- 3072 Surcharging/Rebate is an additional feature which may be used for One-off Payment and Cash  
3073 Services.
- 3074 Req T326: For the One-off Payment Service, any kind of surcharge/rebate shall be part of the  
3075 agreed total sales amount.<sup>78</sup>
- 3076 Req T327: If a surcharge/rebate is applied at the ATM for a Cash Withdrawal, the  
3077 surcharge/rebate shall be displayed to the Customer prior to authorisation, and  
3078 the Customer shall have the opportunity to abort the transaction or to continue  
3079 with the understanding of a surcharge/rebate being applied.
- 3080 Req T328: For a Cash Withdrawal with surcharge/rebate, the transaction amount shall be the  
3081 total of the withdrawal amount and the surcharge/rebate amount.

---

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

## 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:

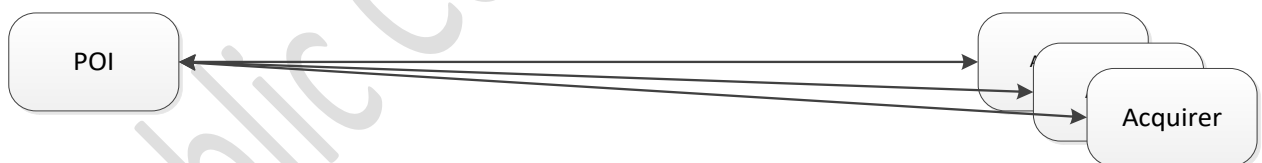
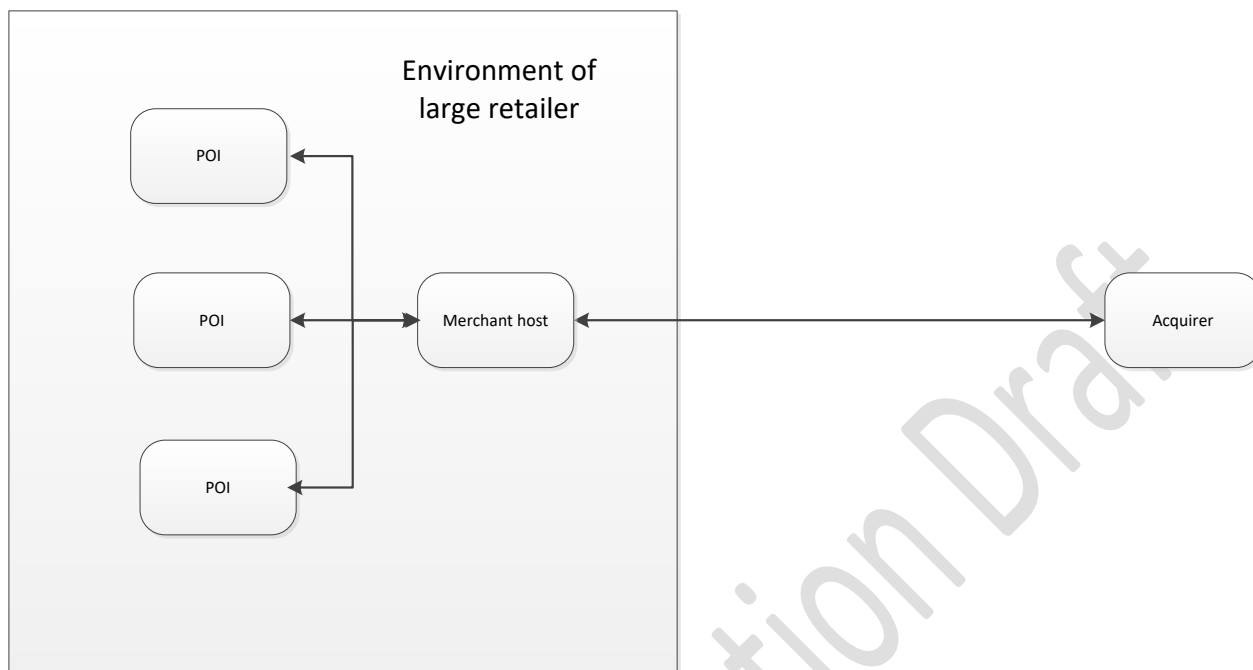


FIGURE 43: POI DIRECTLY CONNECTED TO SEVERAL ACQUIRERS

3103 **Environment of large retailer:**



3104

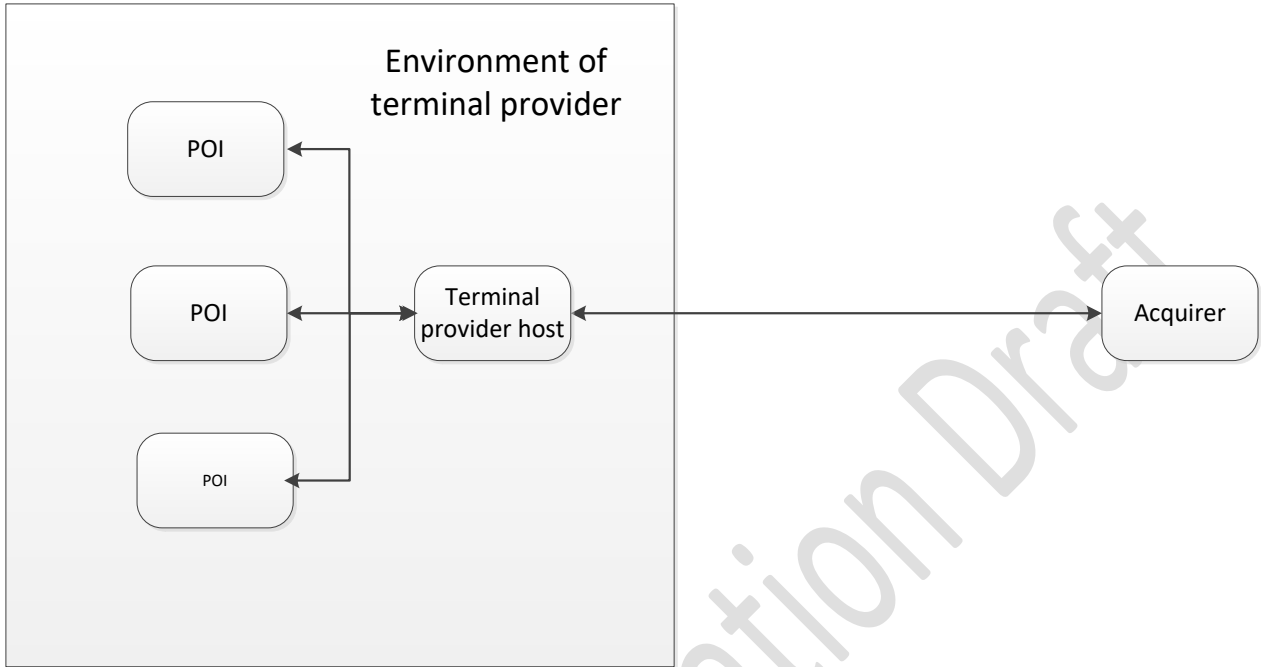
3105

**FIGURE 44: ENVIRONMENT OF LARGE RETAILER**

3106

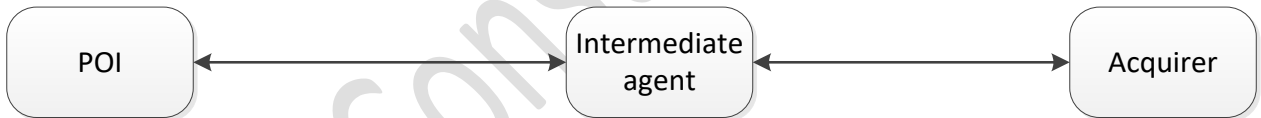
3107

3108 **Environment of a terminal provider:**



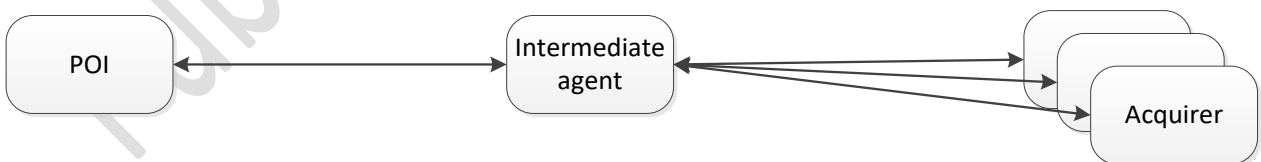
3109  
3110 **FIGURE 45: ENVIRONMENT OF A TERMINAL PROVIDER**

3111 **Environment with an intermediate agent:**



3112  
3113 **FIGURE 46: ENVIRONMENT WITH AN INTERMEDIATE AGENT**

3114  
3115 **Intermediate host connected to several acquirers:**



3116  
3117 **FIGURE 47: INTERMEDIATE HOST CONNECTED TO SEVERAL ACQUIRERS**

3118



3119	Req P1:	The T2A protocols shall support the Payment Services as described in this document.
3120		
3121	Req P2:	For implemented services, the protocols shall support all corresponding Data Elements as defined in Book 3.
3122		
3123	Req P3:	The protocols shall be independent of the communication channel.
3124	Req P4:	The protocols shall support SEPA conformant schemes but should not exclude non SEPA conformant schemes.
3125		
3126	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.
3127		
3128		
3129	Req P6:	The protocols shall support a unique message identification, so to be able to detect duplicate messages.
3130		
3131	Req P7:	The T2A protocols shall be designed to accommodate all types of POI architectures relevant to the Acceptance Environment.
3132		
3133	Req P8:	The T2A protocols shall support one of the following capture modes for transactions:
3134		
3135		• Online capture through the authorisation message
3136		• Online capture through a separate completion message
3137		• Batch capture through file transfer, or transaction by transaction
3138	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.
3139		
3140		
3141	Req P10:	The T2A protocols shall be designed to allow POIs to process transactions with different acquirers.
3142		

## ANNEX 1 - FIGURES AND TABLES

3144	Table 1: Usage of Acceptance Environments and Payment Devices for Local Transactions	11
3146	Table 2: Usage of Acceptance Environments and Payment Devices for Remote Transactions	12
3148	Table 3: Categorisation of Services by AIT and Customer Present Transaction	13
3149	Table 4: Book 2 Scope	19
3150	Table 5: Mapping of Acceptance Technologies to Payment Devices	19
3151	Figure 6: POI Application - Logical Structure and Configuration Parameters	32
3152	Table 7: One-off Payment: Acceptance Technologies and Acceptance Environments	76
3153	Table 8: Functions used for One-off Payment	76
3154	Table 9: Refund: Acceptance Technologies and Acceptance Environments	81
3155	Table 10: Functions used for Refund	82
3156	Table 11: Cancellation: Acceptance Technologies and Acceptance Environments	85
3157	Table 12: Functions used for Cancellation	86
3158	Table 13: Pre-Authorisation Services: Acceptance Technologies and Acceptance Environments	90
3160	Table 14: Functions used for Pre-Authorisation and Update Preauthorisation	91
3161	Table 15: Functions used for Payment Completion	95
3162	Table 16: Deferred Payment: Acceptance Technologies and Acceptance Environments	97
3163	Table 17: Functions used for Deferred Payment	98
3164	Table 18: No-Show: Acceptance Technology and Acceptance Environments	101
3165	Table 19: Functions used for No-Show	102
3166	Table 20: Instalment Payment: Acceptance Technologies and Acceptance Environments for First Transaction	104
3168	Table 21: Functions used for first Transaction of an Instalment Payment	105

3169	Table 22: Functions used for Subsequent Transactions of an Instalment Payment	107
3170	Table 23: Recurring Payment: Acceptance Technologies and Acceptance	
3171	Environments for First Transaction	109
3172	Table 24: Functions used for First Transaction of a Recurring Payment	110
3173	Table 25: Functions used for Subsequent Transactions of a Recurring Payment	112
3174	Table 26: Quasi-Cash Payment: Acceptance Technologies and Acceptance	
3175	Environments	114
3176	Table 27: Functions used for Quasi-Cash Payment	115
3177	Table 28: ATM Cash Withdrawal: Acceptance Technologies and Acceptance	
3178	Environments	117
3179	Table 29: Functions used for ATM Cash Withdrawal	118
3180	Table 30: Cash Advance: Acceptance Technologies and Acceptance Environments	120
3181	Table 31: Functions used for Cash Advance	121
3182	Table 32: Card Validity Check: Acceptance Technologies and Acceptance	
3183	Environments	123
3184	Table 33: Functions used for Card Validity Check	124
3185	Table 34: Balance Enquiry: Acceptance Technologies and Acceptance Environments	126
3186	Table 35: Functions used for Balance Enquiry	127
3187	Table 36: Card Funds Transfer: Acceptance Technologies and Acceptance	
3188	Environments	130
3189	Table 37: Functions used for Card Funds Transfer	131
3190	Table 38: Original Credit: Acceptance Technologies and Acceptance Environments	133
3191	Table 39: Functions used for Original Credit	134
3192	Table 40: Prepaid Card Loading: Acceptance Technologies and Acceptance	
3193	Environments	137
3194	Table 41: Functions used for Prepaid Card - Loading & Unloading	138
3195	Figure 42: POI connected directly to an acquirer host	146
3196	Figure 43: POI directly connected to several acquirers	146

3197	Figure 44: Environment of large retailer	147
3198	Figure 45: Environment of a terminal provider	148
3199	Figure 46: Environment with an intermediate agent	148
3200	Figure 47: Intermediate host connected to several acquirers	148
3201		

Public Consultation Draft