

**SEPA PAYMENT STANDARDISATION (SPS) “VOLUME”****STANDARDS’ REQUIREMENTS****BOOK 6****BEST PRACTICES FOR IMPLEMENTATION***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 6 – v10.5
Date of Version	27.11.2025
Reason for Issue	Public consultation
Reviewed by	EPSG Board – 25 November 2025
Produced by	EPSG Book 6 Expert Team
Owned and Authorised by	EPSG
Circulation	Public (draft for consultation release)

Change History of Book 6		
6.6.0	2012-2013	Working version of Book 6
7.6.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.6.1.0	2014-2015	Working version 2014-2015
7.6.1.05	11.02.2015 (published 10.03.2015)	Consultation version 2015
7.6.2.1	08.12.2015	EPC Published version - Volume v7.1
7.6.2.11- 7.6.2.99	16.12.2015-	Working Version 2015-2016
8.6.00	01.03.2017	ECSG Published version - Volume v8.0
8.6.40	07.11.2018	Board Approval version for Consultation as 8.5
8.6.50	17.12.2018	Public Consultation Release v8.5
8.5.1-2	03.07.2019-	Working Version: updates after Public Consultation
9.0	15.01.2020	ECSG Published Version – Volume 9.0
9.01 – 9.11	2020-2021	Working Version 2020-2021
9.11	15.12.2021	Public Consultation Release v9.5
10.0	01.10.2022	ECSG Published Version – Volume 10.0
10.01 – 10.19	2023-2025	Working Version towards v10.5
10.5	27.11.2025  (published in December 2025)	Public Consultation Release 10.5

## Table of Contents

<b>1. GENERAL .....</b>	<b>5</b>
1.1 Book 6 - Executive summary.....	5
1.1.1. Objectives .....	5
1.1.2. Structure of this book.....	6
1.2 Description of changes since the last version of Book 6 .....	7
<b>2. BEST PRACTICES FOR REGULATORY IMPLEMENTATION .....</b>	<b>8</b>
2.1. Introduction .....	8
2.2. IFR.....	8
2.2.1. Priority Selection and Choice of Application.....	8
2.2.2. Local Transactions - Physical POI.....	10
2.2.3. Remote - Virtual POI: Manual Entry by Cardholder.....	17
2.2.4. Language Preference during Choice of Application.....	19
2.2.5. Display on Brand and Product Type for Acceptance .....	19
2.2.6. Visual Product Identification .....	19
2.3. GDPR .....	20
2.3.1. [EMV 3DS] solutions and GDPR.....	20
2.4. PSD2 .....	21
2.4.1. Article 11 – Considerations for low value contactless transactions.....	21
2.4.2. Article 12 – Considerations for identifying unattended terminals for transport fares and parking fees .....	22
2.4.3. Acceptor Initiated Transactions .....	22
2.4.4. Transactions where the final amount is not known .....	25
2.5. EAA.....	25
2.5.1. EAA requirements.....	25
2.5.2. Examples of use cases as guidance to apply [EAA] .....	26
<b>3. GENERAL BEST PRACTICES FOR IMPLEMENTATION.....</b>	<b>28</b>
3.1. Selection of Payment Solution.....	28
3.1.1. Open-to-all (attended or unattended) POI.....	28
3.1.2. Payment Instrument selection first .....	29
3.1.3. Interface Technology Selection First.....	30
3.2. Guidelines based on ERPB recommendations on transparency for retail payment end-users .....	31
3.2.1. Commercial trade name .....	31
3.2.2. End-to-end data transmission standards for processing .....	32

36	3.3. Guidelines for non-standard card acceptance.....	32
37	3.3.1. Cardholder Verification Method – Signature .....	32
38	3.3.2. Magnetic Stripe Capture .....	33
39	3.4. Data Capture.....	33
40	3.4.1. Data capture for physical POI .....	33
41	Examples .....	34
42	3.5. Integration modes for Account Data Retrieval in Virtual POI environments.....	36
43	3.5.1. The redirect process .....	37
44	3.5.2. The IFRAME .....	37
45	3.5.3. The direct post .....	38
46	3.5.4. The JavaScript created form .....	39
47	3.5.5. The API .....	39
48	3.6. Stored Card Data and SRC in Virtual POI environments .....	40
49	3.6.1. Stored Card Data integration.....	40
50	3.6.2. SRC-Specific Integration Considerations .....	42
51	<b>4. BEST PRACTICES FOR IMPLEMENTATION PER PAYMENT CONTEXT .....</b>	<b>46</b>
52	4.1. Local Transaction .....	46
53	4.1.1. Chip with Contact.....	46
54	4.1.2. Chip and Mobile Contactless .....	62
55	4.2. Remote Transactions.....	66
56	4.2.1. e-and m-Commerce One-off Payment.....	66
57	<b>5. USE CASES .....</b>	<b>69</b>
58	5.1. Card Transactions .....	69
59	5.1.1. Introduction.....	69
60	5.1.2. Mobile Contactless .....	70
61	5.1.3. E and m commerce.....	82
62	5.2. Instant Credit Transfer Transactions .....	87
63	<b>6. FIGURES AND TABLES .....</b>	<b>90</b>
64		

## 1. GENERAL

### 1.1 Book 6 - Executive summary

#### 1.1.1. Objectives

Books 2 to 5 of the Volume describe all of the functional, data, security and conformance verification process requirements for Card payments services initiated in the SEPA area.

As not all requirements and Services described in Book 2 of the Volume are offered and supported in all implementations, common subsets of Services and requirements offered by the acceptors are identified as 'payment contexts'. A payment context is defined as "a set of functional and security requirements described in the Volume applicable to Payment Instruments and POIs in a specific 'transaction environment'".

Support of a particular payment context is optional. However, if a payment context is supported then all mandatory requirements defined in Book 6 relating to this context must be met.

This document will provide:

- Best practices to support the implementation of Regulatory requirements;
- General best practices for implementation and options applicable to the Payment Contexts;
- Specific best practices for implementation and options for each Payment Context;
- Use cases for contactless as well as e- and m-commerce transaction scenarios.
- 

Guidance per payment context is necessary because several implementations of the same service have evolved in the European markets. It is a prerequisite that all Payment stakeholders harmonise on the Volume requirements. If several implementation options are available for a context, the preferred option(s) will be indicated in Book 6.

Based on the volume of transactions or on specific sector or European market needs, a number of payment contexts have been defined. Currently,

The One-off Payment Service:

- Local with:
  - Chip with Contact;
  - Chip and Mobile Contactless.
- Remote with:

- 94                   ○ E- and m-Commerce
- 95                   ○ Mail Order Telephone Order
- 96   Deferred Payment Service:
- 97           • Local with:
- 98                   ○ Chip with Contact;
- 99   Pre-Authorisation Service:
- 100           • Local with:
- 101                   ○ Chip with Contact;
- 102   The creation and maintenance of implementation specifications are out of scope of this book.
- 103           **1.1.2.   Structure of this book**
- 104   Guidelines supporting the implementation of Regulatory requirements are contained in section 2.
- 105   The General best practices for implementation and options are defined in section 3 and specific
- 106   payment context guidelines are set out in section 4. Section 4 includes Volume conformant
- 107   requirements and implementation options. Section 5 contains the description of a number of use
- 108   cases to illustrate various payment transactions.
- 109   References, definitions of terms and abbreviations are provided in Book 1.
- 110

111 **1.2 Description of changes since the last version of Book 6**

112

113 Integration of Instant Credit Transfers (ICT).

114 Integration of best practices in relation to the Directive of the European Parliament and of the  
115 Council on the approximation of the laws, regulations and administrative provisions of the Member  
116 States as regards the accessibility requirements for products and services (COM/2015/0615 final -  
117 2015/0278 (COD)) – also known as European Accessibility Act [EAA].

118 Description of Selection of Payment Solution implementations and flows.

119 Guidelines based on ERPB recommendations for transparency for retail payment end-users.

120 Update of content and diagrams on integration modes for Account Data Retrieval and Stored Card  
121 Data and SRC in Virtual POI environments.

122 Update of best practices for implementation per payment context.

123 Update of existing use cases for Card Transactions and addition of use cases for ICT Transactions.

124

## 2. BEST PRACTICES FOR REGULATORY IMPLEMENTATION

### 2.1. Introduction

During the lifetime of The Volume, several pieces of legislation impacting SEPA for Cards have been published by European regulators. The EPSG (former ECSG), during maintenance updates to the Volume, have considered the regulations (listed below) and updated books accordingly. In addition, the guidelines contained within this section have also been produced.

The EPSG is of the opinion that the Volume does not contain any requirements that cause concern with complying with these regulations. However, it is the responsibility of all entities implementing the Volume requirements to ensure they meet their legal obligations.

This section describes best practices for implementation that have arisen due to the following pieces of legislation.

- Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on interchange fees for card-based payment transactions [IFR]
- Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC [PSD2]
  - Commission Delegated Regulation (EU) 2018/389 of 27 November 2017, supplementing [PSD2] with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication [RTS SCA/CSC]
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [GDPR]
- Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services (European Accessibility Act ))[EAA]

### 2.2. IFR

#### 2.2.1. Priority Selection and Choice of Application

This section describes implementation examples of the Acceptor's priority selection for their preferred application and the Cardholder's Choice of Application mechanism, as described in IFR article 8.6 [IFR], for local contact, local contactless and Remote Card transactions for EEA issued co-badged Cards using:

- An overriding option during the EMV payment process



- An override option using the upfront selection screen before the EMV payment process starts
- A Choice of Application by the Cardholder during the EMV payment process

The subsequent processing is not described as is out of scope of this section.

It is the Acceptor's decision which Cardholder's Choice of Application mechanism they implement. It is also their decision which priority selection and override mechanisms they implement.

The Acceptor's implementation options are not restricted to the examples shown in this section.

**Note: This is a non-exhaustive list of examples of priority selection implementation.**

A summary of all examples is illustrated:

		Type Choice of Application with override		
Environment	Acceptance Technology	Choice by Cardholder without Preference	Acceptor preference with override option upfront	Acceptor's pre-selection with override option once the transaction is started
Local Physical POI 2.2.1	- Chip with Contact 2.2.1.1	<b>Example 1:</b> Cardholder choice Text based interface (2.2.1.1.1)  <b>Example 2:</b> Cardholder choice Graphical interface (2.2.1.1.2)	<b>Example 3:</b> Upfront Acceptor preferred Brand preselection with override after Card insertion (2.2.1.1.3)	<b>Example 4:</b> Acceptor preferred selection with override during the EMV process (2.2.1.1.4)  <b>Example 5:</b> Acceptor preferred selection with override on the same screen using arrows during EMV process (2.2.1.1.5)  <b>Example 6:</b> Acceptor preferred selection with override on the same screen using graphical interface during EMV process (2.2.1.1.6)
Local Physical POI 2.2.1	- Chip with Contact, Chip & mobile Contactless 2.2.1.2		<b>Example 7:</b> Acceptor Pre-selection with override up front (2.2.1.2.1)	
Remote Virtual POI 2.2.2	- Manual Entry by Cardholder	<b>Example 10:</b> Cardholder selection using brand logos (2.2.2.1)		<b>Example 11:</b> Acceptor's priority selection using BIN/ IIN tables with a Cardholder's override mechanism (2.2.2.2)

**Figure 1: SUMMARY OF EXAMPLE IMPLEMENTATIONS OF CHOICE OF THE APPLICATION WITHIN BOOK 6**

## 2.2.2. Local Transactions - Physical POI

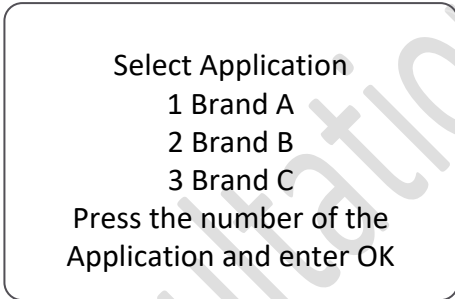
### 2.2.2.1. Contact - Choice by Cardholder without Acceptor Preference

#### 2.2.2.1.1. Example 1: Contact - Cardholder Choice - Text based interface

In this particular example, for a contact EMV transaction, the acceptor has not implemented a priority selection and the POI allows for Cardholder choice. The POI shall present all mutually supported co-badged Applications to enable Cardholder choice.

- Step 1:

When presented to the Cardholder, the Application name, and if available the Category of Card, should be accompanied by a number. This allows the Cardholder to choose the Application by using a key on the numeric keypad, corresponding to the number assigned to each Application mutually supported.

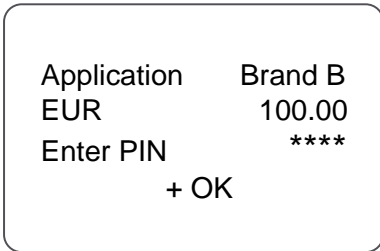


Select Application  
1 Brand A  
2 Brand B  
3 Brand C  
Press the number of the  
Application and enter OK

Figure 2: EXAMPLE 1 (STEP 1): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE

- Step 2:

The Cardholder is then asked to enter their PIN and validate the transaction.

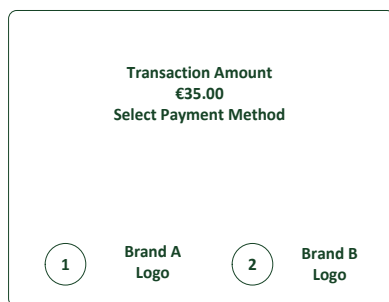


Application	Brand B
EUR	100.00
Enter PIN	****
+ OK	

Figure 3: EXAMPLE 1 (STEP 2): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE, INCLUDING THE SELECTED APPLICATION, TOTAL AMOUNT AND PIN ENTRY

#### 2.2.2.1.2. Example 2: Contact - Cardholder Choice - Graphical interface

If the Acceptor has no preference over which Application they wish the Cardholder to use then they may follow EMV processing, displaying all available co-badged Applications allowing the Cardholder to choose. If all Applications are displayed, it is recommended to display the brand logos associated with the Applications to provide visual assistance to the Cardholder (see Figure 4).



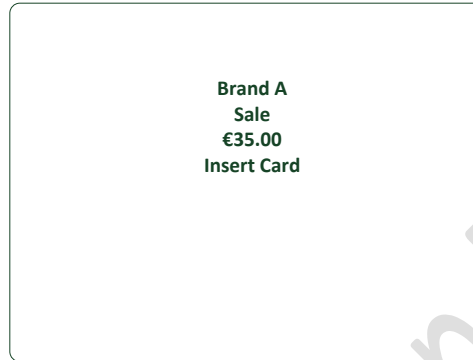
**Figure 4:** EXAMPLE 2: CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - GRAPHICAL INTERFACE

After having selected the preferred application by using a key on the numeric keypad, assigned to the brand logo displayed, the Cardholder is then asked to enter their PIN and validate the transaction (see step 2 of example 1).

2.2.2.1.3. Example 3: Contact - Upfront Acceptor preferred Brand preselection with override after Card insertion

- Step 1:

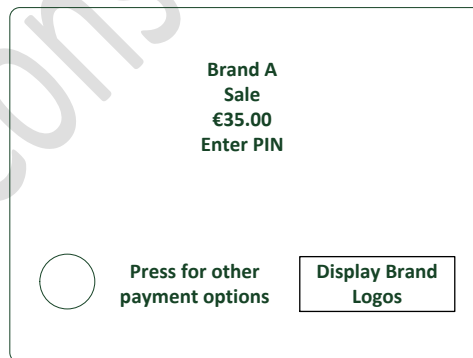
An Acceptor may have a preferred application and may wish to indicate to Cardholders their preferred application, prior to the co-badged Card being inserted (see **FIGURE 5**).



**Figure 5:** EXAMPLE 3 (STEP 1): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE

- Step 2:

On insertion of the Card, however, the Cardholder still has the right to override the Acceptor choice. The method of overriding the Acceptor choice is made clear to the Cardholder (see **FIGURE 6**).



**Figure 6:** EXAMPLE 3 (STEP 2): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE AFTER CARD INSERTION

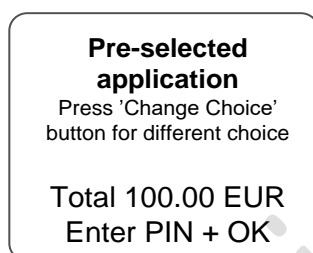
If the Acceptor's preferred application is not available on the Card then the Acceptor may steer the Cardholder to one of the available Applications or may allow the Cardholder to choose using any of the methods described in these examples. Once the Cardholder has confirmed the Application to be used for that transaction, normal EMV processing resumes.

2.2.2.1.4. Example 4: Contact - Acceptor preferred selection with override during the EMV process

If using an automatic mechanism which pre-selects the Acceptor's preferred co-badged Application, all the required information is displayed to the Cardholder on the POI's first screen in the following order:

1. The pre-selected Acceptor's Application,
2. The function for the Cardholder to override the Acceptor's pre-selection,

The above should be provided, if possible, at the first Cardholder confirmation prompt.



**Figure 7: EXAMPLE 4: CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE DURING THE EMV PROCESS - WITH THE TOTAL AMOUNT AND PIN ENTRY AS CVM<sup>2</sup>**

If the Cardholder wishes to override the Acceptor's pre-selection by pressing the indicated button on the key pad, the POI will display to the Cardholder all Card Applications mutually supported by the Card and the POI, either by listing them with corresponding numbers on the key pad (as in example 1), or showing the graphical brand logos associated with the Card Application with corresponding numbers on the key pad (as in example 2).

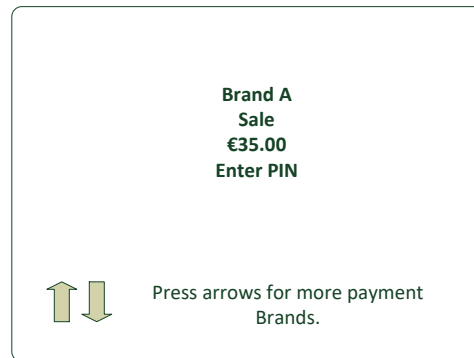
- The Acceptor may put their preferred application on top of the list as priority selection.
- The Cardholder will be able to accept or override the Acceptor's choice by selecting their preferred choice of Card Application, using a key on the numeric keypad assigned to the brand logo associated with the Card Application or Application name displayed, to start the payment process.

<sup>2</sup> If, in the current screen a specific button is being used to support another function, for example the yellow button for PIN entry-correction, then it is recommended to implement another button such as a 'Change Choice' button.

2.2.2.1.5. Example 5: Contact - Acceptor preferred selection with override on the same screen using arrows during EMV process

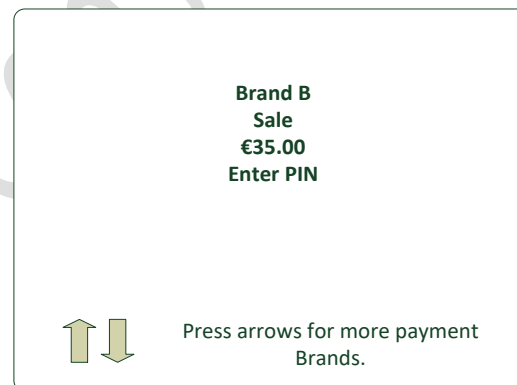
Acceptor pre-selection with override mechanism available on the same screen.

Acceptors may wish to steer Cardholders to the Acceptor's preferred co-badged Application but give access to all the available Applications on the same screen. A method of doing this is shown in **FIGURE 8**.



**Figure 8:** EXAMPLE 5 (STEP 1): CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE ON THE SAME SCREEN USING ARROWS

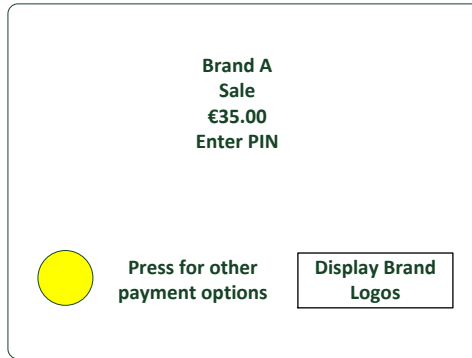
If the Cardholder does not wish to use the Acceptor's preferred application and uses the 'arrows' function the screen scrolls through the available brands associated with the Card Applications available(see **FIGURE 9**). Once the Cardholder has confirmed the Application to be used for that transaction, normal EMV processing resumes.



**Figure 9:** EXAMPLE 5 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING ARROWS

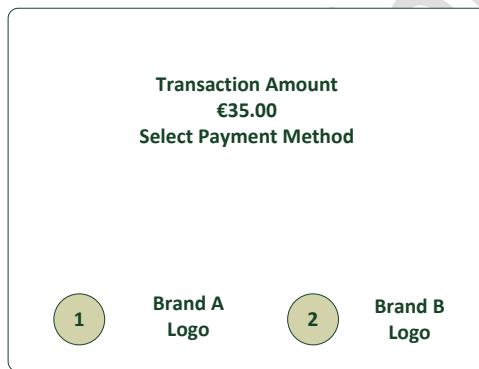
2.2.2.1.6. Example 6: Contact - Acceptor preferred selection with override on the same screen using graphical interface during EMV process

On presentation of the co-badged Card, the Acceptor chooses their preferred application, and presents it to the Cardholder for confirmation (see **FIGURE 10**). At the same time, it is made clear to the Cardholder that other payment options are available, and how to access the other options. If the Cardholder accepts the Acceptor choice, normal EMV processing resumes.



**Figure 10: EXAMPLE 6 (STEP 1): CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE ON THE SAME SCREEN USING GRAPHICAL INTERFACE**

If the Cardholder selects ‘other payment options’, all available Applications are listed (see Figure 11). The Acceptor may present their preferred application first. After having selected the preferred application by using a key on the numeric keypad, assigned to the brand logo displayed, the normal EMV processing resumes.



**Figure 11: EXAMPLE 6 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING GRAPHICAL INTERFACE**

#### 2.2.2.2. Contact and Contactless - Acceptor preselection with override upfront

##### 2.2.1.2.1. Example 7: Contact and Contactless - Acceptor Pre-selection with override up front

The Cardholder may perform a selection of a co-badged Card Application using an upfront selection screen presented by the POI whereas the actual selection occurs after the Card interacts with the POI.

The selection may be performed through (but not limited to):

- A ‘Corr’/yellow button with function keys
- Additional keys like Softkeys or touchpad-Keys next to the POI screen
- A virtual button on the touchscreen of the POI

284 When presented with the upfront selection screen, the Cardholder has two main options.

285 1. If they have a preference as to which Card payment Application to use:

286 a. They indicate to the POI their wish to have displayed the Card Applications available to  
287 use to pay by choosing the Corr / Yellow button, prior to the transaction being initiated  
288 (additional keys or virtual button may be provided).

289 b. After the Card has been read by the POI, either by inserting the Card or presenting the  
290 card or mobile device, the POI will display to the Cardholder all Card Applications  
291 mutually supported by the Card / mobile device and the POI.

292 • The Acceptor may put their preferred application on top of the list as priority  
293 selection either by listing them with corresponding numbers on the key pad (as in  
294 example 1), or showing the graphical brand logos associated with the Application  
295 with corresponding numbers on the key pad (as in example 2).

296 • The Cardholder will be able to accept or override the Acceptor's choice by selecting  
297 their preferred choice of Card Application to start the payment process.

298 • If the card was presented in a contactless mode an additional tap for the Choice of  
299 Application may be required after the Cardholder's preferred choice was selected,  
300 though the process is not described in the current release of the Volume.

301 2. If they have no preference on which Card payment Application is used:

302 a. They insert the Card or present the card or mobile device.

303 b. After the Card or mobile device has been read by the POI, the Acceptor's preferred  
304 application is automatically selected.

305 As this would be implemented for Chip contact and contactless Card payments upfront, after the  
306 above selection process is passed through, a standard EMV payment process will apply.

307 The Cardholder instructions regarding the upfront selection option are indicated on the POI display  
308 or through other means like a sticker when the POI display is limited (e.g., an unattended POI with  
309 only a two line display).

310 An example of the POI message using the yellow function keys button providing a Choice of  
311 Application to the Cardholder with an upfront selection screen is displayed in **FIGURE 12**.

**Purchase**  
**Amount xxx.xx EUR**  
**Insert or Present**  
**card**  
Press 'Change Choice'  
button for Choice of  
Application

312



Figure 12: EXAMPLE 7: CONTACT & CONTACTLESS - ACCEPTOR PRE-SELECTION WITH OVERRIDE UP FRONT

### 2.2.3. Remote - Virtual POI: Manual Entry by Cardholder

The method of using acceptance names and logos of payment brands in conjunction with BIN tables for Product Identification is an Acceptor implementation option.

Some implementation examples are illustrated in the following sections

#### 2.2.3.1. Example 10: Remote - Cardholder selection using brand logos

In this particular example the acceptor has not implemented a priority selection, consequently the Cardholder is presented with all supported payment methods.

The following steps apply:

- The Cardholder's choice is performed by selecting a Brand logo;
- The Cardholder manually enters the PAN, Expiry Date and Card Security Code (CSC);
- The Cardholder submits the payment information.

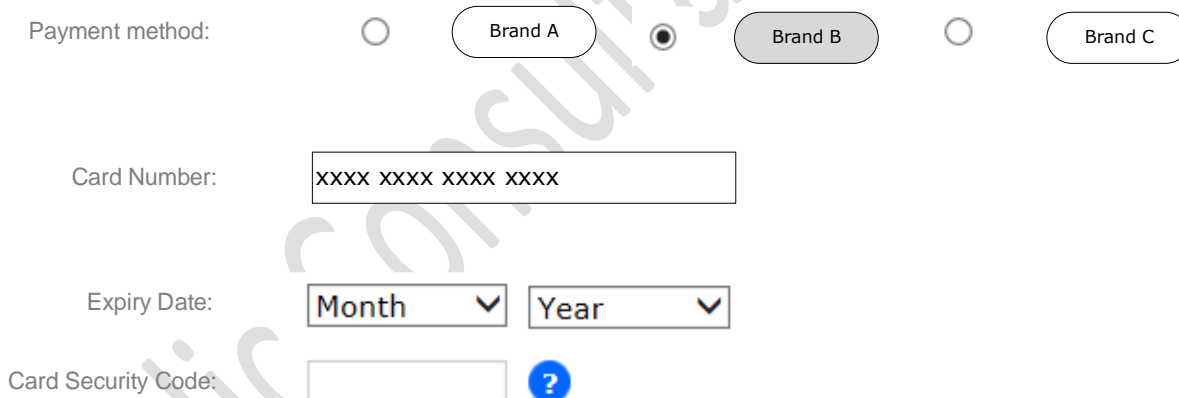


Figure 13: EXAMPLE 10: REMOTE - CARDHOLDER SELECTION USING BRAND LOGOS

#### 2.2.3.2. Example 11: Remote - Acceptor's priority selection using BIN / IIN tables with a Cardholder's override mechanism

##### Step 1: Card detail entry

The Acceptor displays all brands accepted. When choosing to pay by Card, the Cardholder is asked to input the PAN of the Card they wish to pay with.

Payment method: ☒ Card ☐ Digital wallet A ☐ Digital wallet B

Brand A Brand B Brand C

Card Number: 

Expiry Date:  

Card Security Code:  ?

**Figure 14: EXAMPLE 11 (STEP 1): REMOTE - CARD HOLDER ENTERS THEIR CARD DETAIL**

### Step 2: Acceptor product identification

If the Cardholder uses a cobadged Card, the Acceptor's Virtual POI uses IIN/BIN tables to identify the Card brand and category to determinate their preferred Card brand and category, and presents their preference to the Cardholder.

In case of returning Customer with their Card On File for the Acceptor, the Payment Brand selected by the Customer for their previous purchase may be presented as the first choice, with the possibility to change it.

Payment method: ☒ Card ☐ Digital wallet A ☐ Digital wallet B

Brand A Brand B Brand C

**Preferred Selected Card application**

Card Number:

Expiry Date:

Card Security Code:  ?

**Figure 15: EXAMPLE 11 (STEP 2): REMOTE - ACCEPTOR PRODUCT IDENTIFICATION**

### Step 3: the Cardholder exercises their override right

An option to change the Acceptor's (or Customer's) preference is provided to the Cardholder by choosing the "more choice" option. The Acceptor display all the supported Card brands and categories and may put their preferred Card brand and category on top of the list.

Payment method: ☒ Card ☐ Digital wallet A ☐ Digital wallet B

Card number: 4571 04xx xxxx xxxx

Valid through: Month Year

Security code:

Card application available for choice

Debit Brand B

Debit Brand C

Figure 16: EXAMPLE 11 (STEP 3): REMOTE - THE CARDHOLDER EXERCISES THEIR OVERRIDE RIGHT

#### 2.2.4. Language Preference during Choice of Application

When implementing the IFR choice of application for contactless transactions, there may be occasions when the acceptor would like to use the cardholders preferred language for the display, but the Language Preference data element (5F2D) is not immediately available.

An example would be when the POI reads the PPSE, discovers multiple mutually supported applications and wishes to present them to the cardholder for selection.

As the Language Preference is not available within the PPSE, the POI may know of other mechanisms for retrieving the language preference, for example by issuing a SELECT command for one of the returned applications in order to retrieve tag '5F2D' from the application's FCI, if present. However, these mechanisms are outside of the scope of this book and are not described further.

#### 2.2.5. Display on Brand and Product Type for Acceptance

The Acceptor shall display the accepted Brands. If not all Product Types of a Brand are accepted, the Cardholder shall be informed which Product Type(s) are not accepted per Brand. For Local Transactions, this shall be at the entrance of the shop and the POI. For Remote Transactions, this should be at the latest, on the payment page.

#### 2.2.6. Visual Product Identification

The appropriate Card category for Visual Product Identification shall be displayed on the Card or consumer device in English, as follows;

- Prepaid

- 369 • Debit
- 370 • Credit
- 371 • Commercial

372 If required by local regulation, the Card category may additionally be displayed in the local  
373 language.

374

## 375 **2.3. GDPR**

376 In the context of card based payments, the GDPR applies to all circumstances where personal data  
377 is provided or processed. However, due to the increased use of data in the [EMV 3DS] specification,  
378 further guidance when implementing those specifications is given below.

### 379 **2.3.1. [EMV 3DS] solutions and GDPR**

380 [EMV 3DS] (3-domain security) is strongly recommended for e-/m commerce transactions as a  
381 method of implementing Strong Customer Authentication (SCA). However, it should be understood  
382 3DS solutions may process data elements that are considered to be personal data under the GDPR.  
383 Data collected may include data of cardholders and merchants, and where merchants are sole  
384 traders, certain merchant data may be considered personal. All entities processing personal data  
385 in the context of 3DS solutions are individually responsible for identifying and complying with the  
386 relevant obligations under the GDPR. Accordingly, all entities should seek legal advice when  
387 considering the GDPR consequences of providing and processing data that may be considered to  
388 be personal data.

389

390 Specific principles to consider include:

- 391 • Lawful basis for processing: All entities should ensure they can rely on a lawful basis  
392 under the GDPR to process personal data in the context of 3DS solutions. For most of  
393 these solutions, all entities may rely on legal bases other than consent including legal  
394 obligation, contract and legitimate interest for using personal data for fraud prevention  
395 purposes.
- 396 • Purpose limitation: Data provided by merchants for 3DS authentication must not be  
397 used for any purpose other than authentication and fraud prevention. Specifically, this  
398 data should not be used for sales marketing or other purposes.
- 399 • Data storage and security: All entities should ensure that the requirements for data  
400 storage, security and international transfers under GDPR are applied to any personal  
401 data that is collected for 3DS solutions.
- 402 • Data minimisation: Data collected must be limited to what is necessary in relation to  
403 3DS authentication. Further data should not be collected if the available data allows for  
404 SCA.

- Transparency and Individual Rights: All entities should ensure that Terms and Conditions, Privacy Policies and Privacy Notices reflect the capturing and processing of data for fraud prevention purposes in the context of 3DS solutions. This includes information on purposes for processing their personal data, the retention periods for that personal data, and who it will be shared with. In addition, all entities should ensure that they can respond to individuals' requests under the GDPR.
- Accountability: Organizations must document data processing in the context of 3DS solution, ensure data protection impact assessment, where required, and consider privacy by design and by default measures.
- Where sensitive personal data may be collected for the purpose of 3DS solution, including biometric data such as fingerprint, facial features, or iris format, the entity involved is responsible for ensuring additional safeguards under the GDPR, such as for example obtaining explicit consent.

## **2.4. PSD2**

The following section provides guidelines for specific transaction types under [PSD2] - [RTS SCA/CSC].

### **2.4.1. Article 11 – Considerations for low value contactless transactions.**

Article 11 of [RTS SCA/CSC] introduces exemptions to Strong Customer Authentication (SCA) for contactless transactions.

One method for controlling the correct implementation of the contactless exemptions is for the Issuer to implement a host-based solution, using specific response codes indicating that SCA is required.

If this Response Code option is used, four possible transaction flows have been identified:

- SWITCH INTERFACE  
(Cardholder is asked to switch interface from contactless to contact)
- RE-PRESENT CARD AND ENTER PIN  
(Cardholder is asked to re-tap card and enter PIN)
- ENTER PIN WITHOUT A SECOND TAP  
(Cardholder is asked to enter PIN – initial transaction data will be used)
- DECLINE  
(There is no valid method of performing CVM with the device presented )

Another method of controlling the implementation of contactless exemptions is through the use of Card based controls, but this method is out of scope of The Volume.

Issuers will need to consider, inter alia, the following factors when deciding whether to use Issuer Host or Card based controls to manage contactless exemptions:

- Market capabilities – support of online/offline PIN
- Card capabilities – support of various CVM methods
- Form factor and device capabilities

#### **2.4.2. Article 12 – Considerations for identifying unattended terminals for transport fares and parking fees**

Article 12 of [RTS SCA/CSC] introduces exemptions to Strong Customer Authentication (SCA) for transactions performed on unattended terminals for transport fares and parking fees.

- Terminal Type may be used to identify the terminal as unattended.
- The following MCCs may be used to identify transport and parking sectors:
  - 4111 Transportation - Suburban and Local Commuter Passenger, including Ferries
  - 4112 Passenger Railways
  - 4131 Bus Lines
  - 4784 Bridge and Road Fees, Tolls
  - 4789 Transportation Services—not elsewhere classified
  - 7523 Automobile Parking Lots/Garages

Additional data may be used to identify transactions related to transport fares or parking fees.

#### **2.4.3. Acceptor Initiated Transactions**

The following subsection provides guidance on Acceptor Initiated Transactions, where 2.4.3.1 covers guidance on MITs and 2.4.3.2 covers Acceptor Initiated Transactions where merchants are the payer, i.e. refund services.

##### **2.4.3.1. Merchant Initiated Transactions**

The following section provides guidelines relevant to the implementation of Strong Customer Authentication (SCA) under PSD2 specific to Merchant Initiated Transactions (MITs). The guidelines are written for business, technology and payments managers responsible for the planning and implementation of PSD2 compliance policies and solutions within Issuers, Acquirers, Merchants, gateways and Vendors. It aims to provide readers with guidance to support business, process and infrastructure policy decisions needed to plan for the implementation of MITs.

The following guidelines apply when the Cardholder and Merchant establish the Merchant Initiated Transaction agreement (MIT Mandate) electronically. The establishing of ‘non-electronic’ mandates are outside of the scope of the Volume.

#### 2.4.3.1.1. Authorisation and Authentication flow

Cardholder signs up to a new agreement for future Merchant Initiated Transactions (MIT Mandate)
1. Merchant discloses to Cardholder appropriate T&Cs and follows other requirements associated with the future MIT type it will process. The Cardholder must explicitly accept the T&Cs for the agreement to proceed.
2. Acceptor/Merchant <b>requests an SCA</b> of the Cardholder by the Issuer for the “authenticated amount”.
3. Merchant <b>requests authorisation</b> from the Issuer for the amount due that day and stores the transaction ID of this Authorisation for later use as the Initial Tran ID in future MITs.  If an Authorisation is not necessary at the time of setting up the mandate, then SCA may be achieved through a zero amount “account status” type transaction. This type of functionality is supported in EMV 3DS 2.1 and above.  This first Authorisation is a transaction initiated by the Cardholder used to establish the agreement for future MITs. If the Authorisation is approved, the payment credentials can be stored for future use. If the credential is not stored, the details can be kept but only as long as required in order to complete the current transaction agreement (e.g. to process any industry specific MITs such as No-Shows).
Cardholder uses service leading to additional payments
4. The Acceptor/Merchant <b>initiates authorisation requests</b> future MITs. The initial transaction ID to use is the one generated in step 3. The amount in future MITs may vary from the original amount as long as the amount calculation method is disclosed to the Cardholder in the T&Cs of the established agreement. Any amount variance should not be a concern, as the transaction is an MIT and therefore is considered to be out of scope of SCA.



480                      2.4.3.1.2.      Types of Merchant Initiated Transactions

481      Below are examples of types of MITs. For clear definitions the reader can refer to Book 1 section  
482      3.3.

483

<b>Instalment</b>	Instalment payments describe a single purchase of goods or services billed to a Cardholder in multiple transactions over a period of time agreed by the Cardholder and Merchant.
<b>Recurring Payment</b>	Recurring Payments describe transactions where the Cardholder authorises an Acceptor to charge their account on a recurring basis and without a specified end date. Note that a recurring MIT transaction is initiated by the Merchant (payee) not the Cardholder (payer) and so is considered to be out of scope of PSD2.
<b>No- Show</b>	A No-show is a transaction where the Acceptor is enabled to charge for services which the Cardholder entered into an agreement to purchase, but did not meet the terms of the agreement.
<b>Staged Wallet funding</b>	The transaction to fund the Staged Wallet using a linked Card may be considered as a MIT, where the operator of the Staged Wallet is considered as the Acceptor.
These types of MITs occur where a transaction is initiated by the Acceptor under an existing established agreement.	

484                      2.4.3.2.      Refund transactions

485      Although Refunds are initiated by the Merchant, due to the different flow of funds, the Merchant  
486      is considered to be the Payer. As the merchant is the Payer, the PSD2 requirement that the Payer's  
487      PSP, i.e. the Acquirer, authenticates the Payer still applies. The following two factors can be used  
488      by the Acquirer to perform SCA of the Merchant for Refund transactions:

- 489              • Possession factor: Terminal ID in an Authorisation request message indicates to the  
490              Acquirer that the Merchant is in possession of the hardware that is assigned to the  
491              Merchant.
- 492              • Knowledge factor: before starting the session and initiating a Refund transaction, retail co-  
493              workers typically have to enter a password to access the systems that allow them to  
494              perform the initiation of refunds. Book 2 of the Volume requires that sensitive functions,  
495              such as Refunds have password protection as a configurable option. The use of this  
496              functionality is strongly recommended.



497 The PSP of the Merchant, the Acquirer, may therefore also apply exemptions under the RTS for  
498 the refund transactions, including the Article 17 exemption for Secure corporate payment  
499 processes and protocols.

#### 500 **2.4.4. Transactions where the final amount is not known**

501 There are a number of use cases where the final transaction amount is not known at the time the  
502 transaction is performed. Whilst this is not a new situation, PSD2 has introduced challenges related  
503 to strong customer authentication and the dynamic linking of transactions.

504

505 • In order to meet PSD2 requirements of SCA and dynamic linking in all circumstances, to  
506 minimise the amount of friction in the transaction, and to prevent the issuer from trying to  
507 authenticate the cardholder when they are no longer there, Merchants may implement  
508 MITs as described in section 2.4.3.1.1.

509 • If a Merchant is unwilling or unable to use MITs, in order to reduce declines, the Merchant  
510 should authorise and authenticate for a maximum amount, explaining to the Cardholder  
511 that this is an estimated amount and the final transaction amount may be lower. Note; if  
512 the final transaction amount is higher than the authenticated amount the transaction is  
513 likely to be declined by the Issuer because of the dynamic linking requirements.

514 • In order to meet dynamic linking requirements it is strongly recommended to perform  
515 authorisation and authentication at the same time and for the same amount.

516

### 517 **2.5. EAA**

#### 518 **2.5.1. EAA requirements**

519 Directive (EU) 2019/882 of the European Parliament and of The Council on the accessibility  
520 requirements for products and services [EAA] was adopted on 17 April 2019. The Directive aims to  
521 contribute to the proper functioning of the internal market by approximating laws, regulations and  
522 administrative provisions of the Member States as regards accessibility requirements for certain  
523 products and services by, in particular, eliminating and preventing barriers to the free movement  
524 of certain accessible products and services arising from divergent accessibility requirements in the  
525 Member States.

526 Article 15 of the Directives refers to harmonised standards for product accessibility requirements.  
527 The best currently available standard is ETSI's EN 301 549 V3.2.1 (2021-03) document [EN AR].

528 The EPSG intends to give examples of how accessibility requirements can be implemented in the  
529 use cases but cannot be exhaustive. The EPSG's intention is to provide guidance that could be used  
530 by the readers to make their own analysis for the actual implementation.

## 2.5.2. Examples of use cases as guidance to apply [EAA]

The purpose of this section is to illustrate how accessibility presumption of conformity (according to Article 15 of the Directive) can be achieved by applying the available requirements in the EN document.

### 2.5.2.1. Example 1 – Local Transaction – Physical POI – visually impaired person

Section 5.1.3 describes the non-visual access requirements applicable in this use case suggesting alternative ways to screen reading through assistive technologies (e.g. audio prompts of displayed information such as the transaction amount).

Section 8.4.1 describes the requirements for keyboard features allowing the input of the PIN number on the terminal.

The amount and any relevant information is spoken by the terminal using speech generation software so that the cardholder is made aware of the correct transaction details. After that, if requested, the cardholder can enter their PIN on the POI.

When a mechanical PIN-pad is provided, the cardholder will be guided by “the number five key tactilely distinct from the other keys of the keypad” (section 8.4.1). [Also see ISO 9564-1:2017 (E), Annex B.]

The Royal National Institute of Blind People [[www.rnib.org.uk](http://www.rnib.org.uk)] published a paper outlining how the cardholder will be guided by audible prompts (naturally not speaking out the actual figures for security reasons) to select the correct keys for the PIN when a touch-screen PIN-pad is used.



**FIGURE 17:** EXAMPLE OF ACCESSIBLE PIN PAD DESIGNED FOR ENHANCED READABILITY

“Finding a reference point can help to begin the transaction. Often this means starting in a corner and sliding the finger onto the screen to find the first number. Number 1 is found in the top-left corner. The numbers cannot be spoken for security reasons, so a beep can be heard instead. Then, keeping the finger on the screen, moving from this digit to the next digit, for example, move to the right from number 1 for number 2 on a standard telephone keypad, and another beep will be heard. The buttons cancel and OK are spoken so these can also be used as a reference point.

Once the correct digit has been found by listening to the beeps, the cardholder double taps anywhere on the screen to enter the digit. A sound will confirm that a digit has been entered and in most cases it’ll say how many digits have been entered. If the cardholder’s finger lifts off the screen by mistake, no digit is entered until double tapping.

568 After entering the PIN digits the cardholder moves the finger to the *enter* or *OK* button at the  
569 bottom right then lifts the finger and double taps anywhere on the screen to confirm the  
570 transaction.

571 There's also the option to cancel the transaction, by selecting the cancel button on the bottom left,  
572 before doing a double tap to confirm the cancellation."  
573 [[https://media.rnib.org.uk/documents/How to use an accessible touchscreen chip and PIN](https://media.rnib.org.uk/documents/How_to_use_an_accessible_touchscreen_chip_and_PIN_2022.pdf)  
574 [2022.pdf](https://media.rnib.org.uk/documents/How_to_use_an_accessible_touchscreen_chip_and_PIN_2022.pdf)]

575 2.5.2.2. Example 2 – Remote Transaction - Virtual POI – visually impaired person

576 Besides section 5 where generic requirements apply, section 9 of the EN document regarding web  
577 requirements will be used to define the conformity with the Directive.

578 2.5.2.3. Example 3 - ATM – visually impaired person

579 In this example, section 8.2, Hardware products with speech output, will have particular relevance  
580 in determining the conformity with the Directive.

581

582

### 3. GENERAL BEST PRACTICES FOR IMPLEMENTATION

#### 3.1. Selection of Payment Solution

A Payment Solution is defined as the combination of a Payment Instrument (e.g., Payment Card or Instant Credit Transfer), a Payment Brand, and an Acceptance Technology (such as NFC, Chip Contact, or QR Code). Given these components, there is considerable variability in how a Payment Solution may be presented and selected at the POI.

While the functional and technical requirements related to this topic are defined in Book 2, Book 6 provides additional guidance on implementation for ensuring interoperability, supporting the coexistence of different payment methods, optimising the user experience, and accommodating a wide range of acceptance scenarios.

The following selection trees are described as representative of common market implementations:

1. Open-to-all (attended or unattended) POI
2. Payment Instrument selection first
3. Interface technology selection first

It is understood that IFR provisions regarding the choice of application apply to Payment Solution selection scenarios for both contact-based and contactless (NFC) transactions conducted over card payment rails.

##### 3.1.1. Open-to-all (attended or unattended) POI

##### **Prerequisites:**

All accepted Payment Brands (for supported Payment Instruments) are clearly displayed and visible at the POI.

No (verbal) guidance is required.

The POI has the capability to simultaneously detect the presence of a Card onNFC/contactless and contact interfaces, to display a (multi-brand) QR Code and to read a QR Code. Additionally, the POI can in parallel receive the payment confirmation message (for a transaction with Merchant-presented QR Code option).

##### **Step 1: POI activation**

The Acceptor activates the payment interfaces by:

- Opening the NFC/contactless and contact interfaces, and simultaneously
- Displaying a dynamic, multi-brand QR Code on the terminal screen.

At this stage, the selected Payment Brand is not yet known to the POI.

##### **Step 2: Customer initiates the payment**

The Customer selects one of the available options:

619 **a. Cash (out of Volume scope)**

620 **b. Contact or contactless/NFC**

621 The Customer inserts the Card or taps the Card or Mobile Device in the dedicated area of the POI.

622 Based on the information exchanged via contact or NFC and entry point interaction, the Payment  
623 Brand is selected at this stage and the POI initiates the appropriate flow resulting in a Card  
624 Transaction or ICT Transaction where the ICT Transaction may be processed over card rails or ICT  
625 rails.

626 **c. Merchant-presented QR Code**

627 The Customer scans the QR Code displayed on the terminal, typically using a payment app in their  
628 Mobile Device. In some cases, scanning via smartphone camera may occur: the PISP typically  
629 provides the landing page where the QR Code directs the Customer for checkout.

630 The Customer initiates the ICT Transaction via the payment app or the flow enabled within the  
631 landing page.

632 The POI awaits payment confirmation and final approval.

633 **d. Consumer-presented QR Code**

634 The Customer uses their Mobile Device to (generate or retrieve and) present a QR Code to the  
635 Acceptor who scans it.

636 The POI initiates the corresponding ICT-based payment flow and awaits payment confirmation  
637 and final approval.

638

### 639 **3.1.2. Payment Instrument selection first**

#### 640 **Prerequisites:**

641 All accepted Payment Brands (for supported Payment Instruments) are clearly displayed and visible  
642 at the POI.

643 (Verbal) guidance is required.

644

#### 645 **Step 1: POI activation**

646 The Acceptor prompts the Customer to select the Payment Instrument first, e.g., the terminal  
647 shows cash/card/bank transfer icons inviting the Customer to click their choice. Based on the  
648 Customer's choice, the POI activates the appropriate flow.

649

#### 650 **Step 2: Customer initiates the payment**

651 **a. Cash (out of Volume scope)**

652 **b. Payment Card**

653 Contact or Contactless/NFC interface is activated.

654 Refer to the description for Contact or Contactless/NFC in the Open-to-all flow.

655 The payment results in a Card Transaction.

656 **c. ICT**

657 Contactless/NFC interface is activated. Refer to the description for Contactless/NFC in the Open-  
658 to-all flow.

659 A dynamic, multi-brand QR Code is presented on the terminal screen simultaneously. Refer to the  
660 description for Merchant-presented or Consumer-presented QR Code in the Open-to-all flow.

661 The payment results in an ICT Transaction that may be processed over card rails or ICT rails.

662

663 **3.1.3. Interface Technology Selection First**

664 **Prerequisites:**

665 All accepted Payment Brands (for supported Payment Instruments) must be clearly displayed and  
666 visible at the POI.

667 (Verbal) guidance is required.

668

669 **Step 1: POI Activation**

670 The Acceptor prompts the Customer to select the technology interface first (e.g., the teller at the  
671 attended POI asks the Customer whether they want to pay using contact, contactless, or QR Code)  
672 and activates the payment interfaces accordingly by:

- 673 • Opening the contact reader interface, or
- 674 • Opening the contactless/NFC interface, or
- 675 *Contact and contactless/NFC interfaces are usually opened simultaneously*
- 676 • Displaying a dynamic, multi-brand QR Code on the terminal screen, or
- 677 • Requesting the Customer to present a QR Code to a dedicated reader.

678 At this stage, the selected Payment Brand is not yet known to the POI.

679

680 **Step 2: Customer Initiates the Payment**

681 **a. If Contact or contactless/NFC**

682 Refer to the description for Contact or Contactless/NFC in the Open-to-all flow.

683 **b. If QR Code**

684 Refer to the description for Merchant-presented and Consumer-presented QR code in the Open-  
685 to-all flow.

686

### **3.2. Guidelines based on ERPB recommendations on transparency for retail payment end-users**

To improve identification of whom, where and when the Customer made a Payment based on Customer's Payment Account statement or corresponding application, the ERPB set up a working group to define recommendations.

#### **3.2.1. Commercial trade name**

The first ERPB recommendation on transparency for retail payment end-users outlines the following:

*"Consistently use commercial trade name and provide this name to all involved parties in the payment chain for use in client's payment account statements."*

It is critical that the Acceptor name used throughout the transactions is recognisable by the Cardholder so that transactions can be correctly identified. If the legal name is different from the Acceptor's commercial trade name, the legal name may be meaningless to the cardholder. The Acceptor name must be the name most prominently displayed by the Acceptor and by which Cardholders recognise the Acceptor.

For that reason, the following section provides examples and guidance on how such Commercial Trade Name may be used.

##### **3.2.1.1. Example One: Fuel station franchise**

A fuel station is a franchisee of a large retail chain. Accordingly, the retail chain name, brand, and colors are prominently displayed on the forecourt and inside the shop. The name of the franchisee is in the window on an A4 notice for legal reasons. The Acceptor name must be the name of the retail chain, possibly with an added indication of the location.

##### **3.2.1.2. Example Two: Online marketplaces (payment aggregator)**

A type of marketplace, also known as "payment aggregator", "facilitator", or "master merchant" is defined as an intermediary that processes and collects payments for merchants (sometimes called "sub-merchants", or "ultimate payees"). In this case it is recommended that the Acceptor's Commercial Trade Name (master merchant) appears on the payment followed by, if possible, e.g. "payment processed for" followed by the commercial trade name of the sub-merchant.



721 3.2.1.3. Example Three: Online marketplaces

722 Another type of marketplace is defined as an intermediary that does not process and collect  
723 payments. A Customer buys items from a supplier present on such marketplace, and the  
724 beneficiary (payee) of the payment is that supplier. It is recommended that in this case of  
725 marketplaces the name appearing on the payment account statement is formatted as commercial  
726 trade name of the ultimate payee (the supplier) and followed by e.g. “ - your order from”, followed  
727 by the commercial trade name of the marketplace on which the client placed the order.

728

729 **3.2.2. End-to-end data transmission standards for processing**

730

731 The fifth ERPB recommendation on transparency for retail payment end-users outlines the  
732 following:

733

734 *“Use standards and applications suitable for including identified data sets “end-to-end”. Upgrade  
735 or change these standards when necessary.”*

736 The ERPB document further detail the following guidance to secure data to be processed from an  
737 end-to-end perspective:

738 “All processing entities involved in the payment chain should use standards and applications that  
739 are able to collect and transmit the requested information from the beginning of the payment  
740 process to the end (payment account statement provided to the Customer). The technical  
741 protocols should be interoperable and should support the full data set as listed in these  
742 recommendations, end-to-end. The data fields should not be limited in character number such that  
743 they pose an obstacle to the successful transmission of this information.

744 The standards and applications should be adapted to the information needs of the Customer and  
745 not the contrary.

746 Considerations should be made to upgrade any protocols in current use that are unable to collect  
747 or transmit the information set out in these Recommendations. An alternative might be to migrate  
748 to standards that can collect and transmit this information.”

749 **3.3. Guidelines for non-standard card acceptance.**

750 **3.3.1. Cardholder Verification Method – Signature**

751 The European Banking Authority (EBA) has clarified that the capturing of a Cardholder’s signature  
752 on a paper slip cannot be considered as a behavioural biometric. Nor can a paper based signature  
753 constitute knowledge or possession. As a result, the capturing of a paper based signature cannot  
754 be used to meet Strong Customer Authentication requirements as defined in PSD2.



However, there may be legitimate needs for a Merchant to capture a signature, such as one leg in transactions or to support refund processes and so signature capture is described in The Volume.

### **3.3.2. Magnetic Stripe Capture**

Although Magnetic Stripe capture is not considered a secure method of performing card based transactions in SEPA, there may be legitimate business needs for a Merchant to read a magnetic stripe, such as one leg in transactions or fallback transactions and so magnetic stripe capture is described in The Volume.

## **3.4. Data Capture**

### **3.4.1. Data capture for physical POI**

The Terminal to Host Capture of Online/Offline Transactions is realised with one of the following mechanisms

- Capture by Authorisation;
- Capture through completion message;
- Capture by Batch/File;
- Or can be a combination of these three methods.

The following three configurations, called 'Modes' of the POI Acquirer Protocol are recommended:

Mode 1:

- Online Authorisation without capture for online transactions,  
Followed by/or
- Capture immediately after transaction finalisation regardless whether Authorisation was online or offline.

Mode 2:

- Online Authorisation without capture for online transactions,  
Followed by/or

- Capture by a batch transfer for a group of transactions regardless whether Authorisation was online or offline.

Mode 3:

- Capture with Authorisation for transactions Authorised online;
- Capture immediately after transaction finalisation if Authorisation was performed offline.

The method used is based on an agreement between Acceptor and Acquirer.

### Examples

For each Mode, the typical message flows below show when the Authorisation is performed online. If the Authorisation is performed offline, the online Authorisation request and response in the flows should be disregarded. In Mode 3, if the Authorisation is performed offline, an additional Financial Advice exchange must be executed to perform the Data Capture.

## Mode 1: Online Authorisation, Capture immediately after Transaction Completion

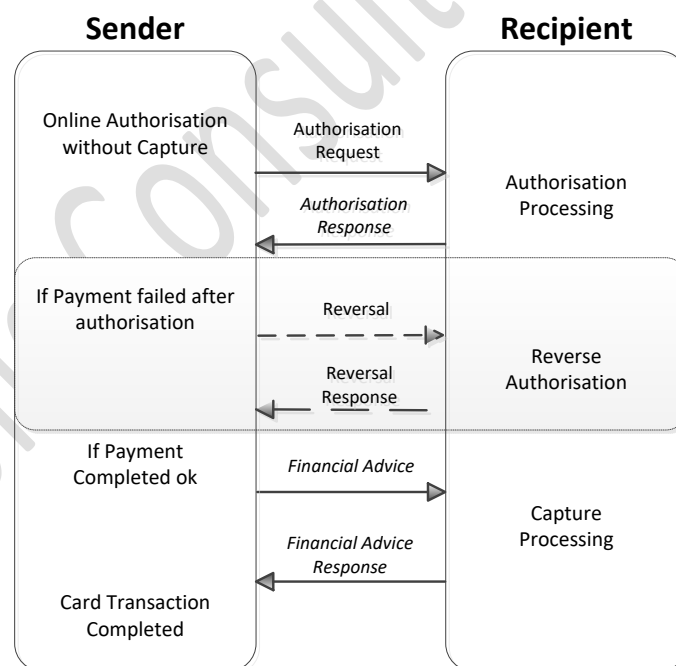


FIGURE 18: MODE 1

## Mode 2: Online Authorisation, Capture by Batch

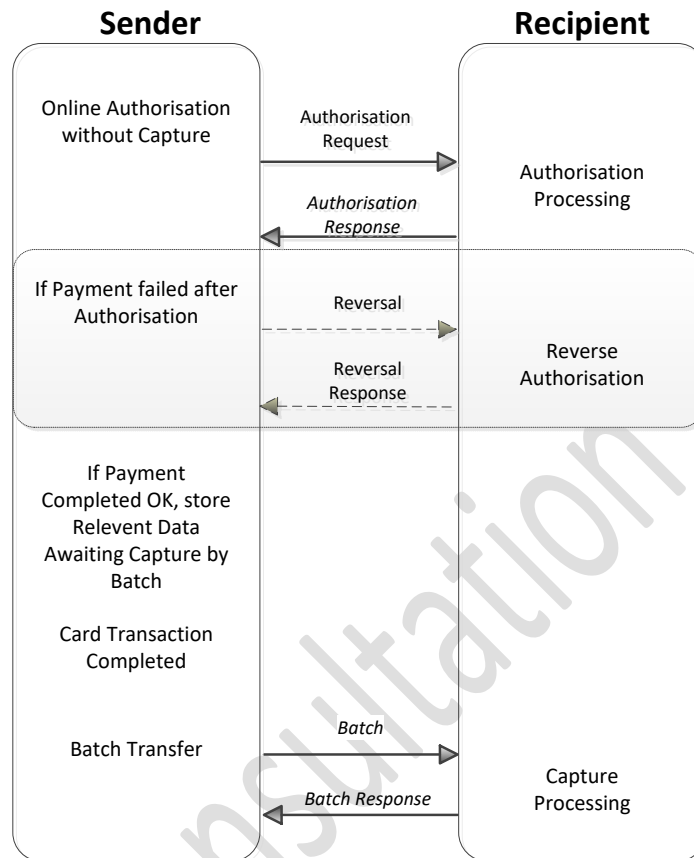


FIGURE 19: MODE 2

## Mode 3: Online Authorisation with Capture

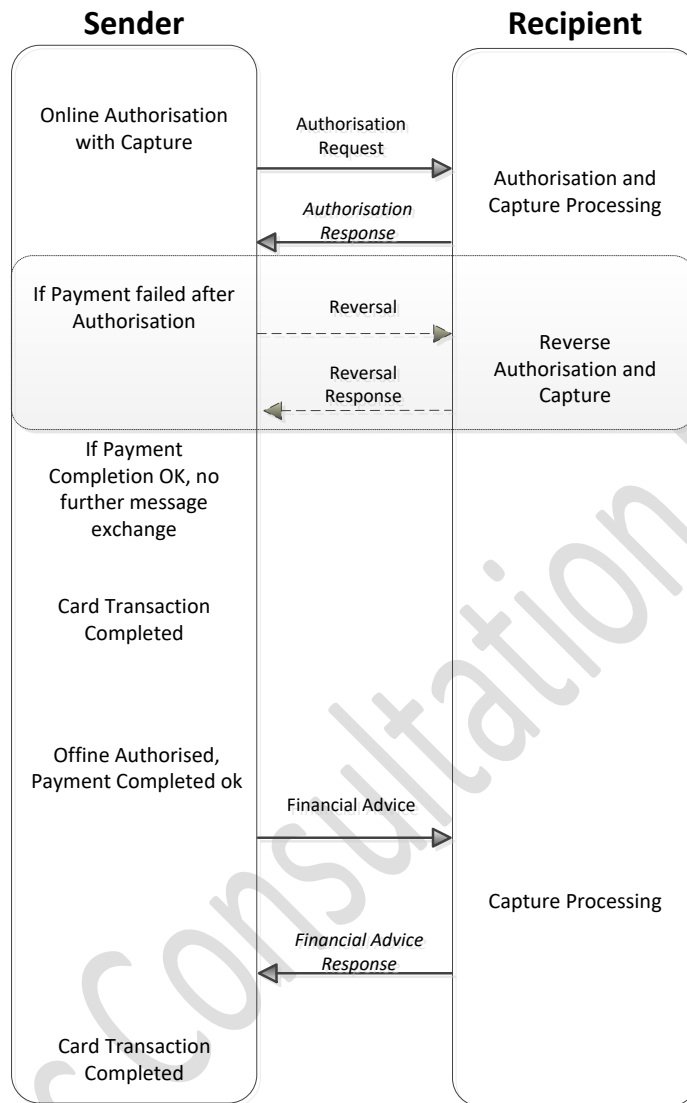


FIGURE 20: MODE 3

### 3.5. Integration modes for Account Data Retrieval in Virtual POI environments

The following examples are typical configurations representing integration modes between the Acceptor and the Third-Party Processor (TPP) for retrieving Account Data in a Virtual POI environment.

- The redirection process
- The iFrame
- The direct post
- The JavaScript created form
- The API (sometimes called the Merchant gateway)

For each of the configurations a stepwise description is provided below for the transmission of the Account Data in the case of E- and M- Commerce. In all these examples, the Customer provides Account Data through the selected Acceptance Technology (i.e. one among those available such as Manual Entry, digital wallet, or Stored Card Data or Consumer Device).

### 3.5.1. The redirect process

The following figure illustrates the different steps involved in the configuration whereby the Consumer Device is redirected to a TPP to request a payment page. This configuration imposes the lowest risk for the Acceptor.

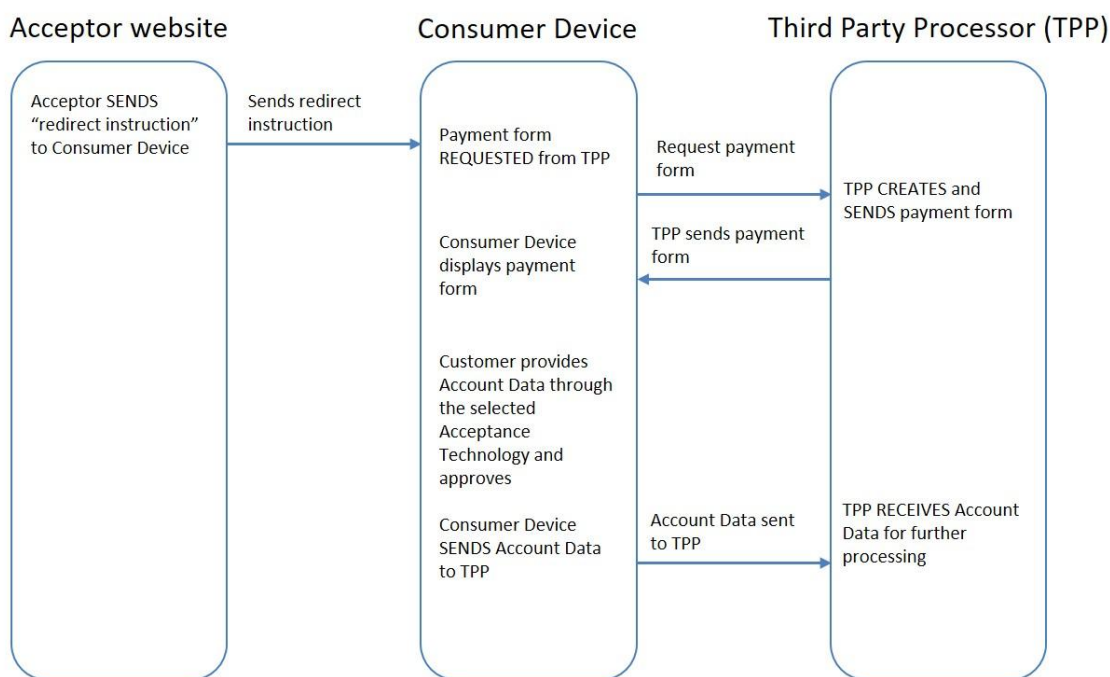


FIGURE 21: THE REDIRECT PROCESS

### 3.5.2. The IFRAME

The following figure illustrates the different steps involved in the configuration whereby the Consumer Device is redirected to a TPP to request a payment page via a so-called parent payment page obtained from the Acceptor's website.

827

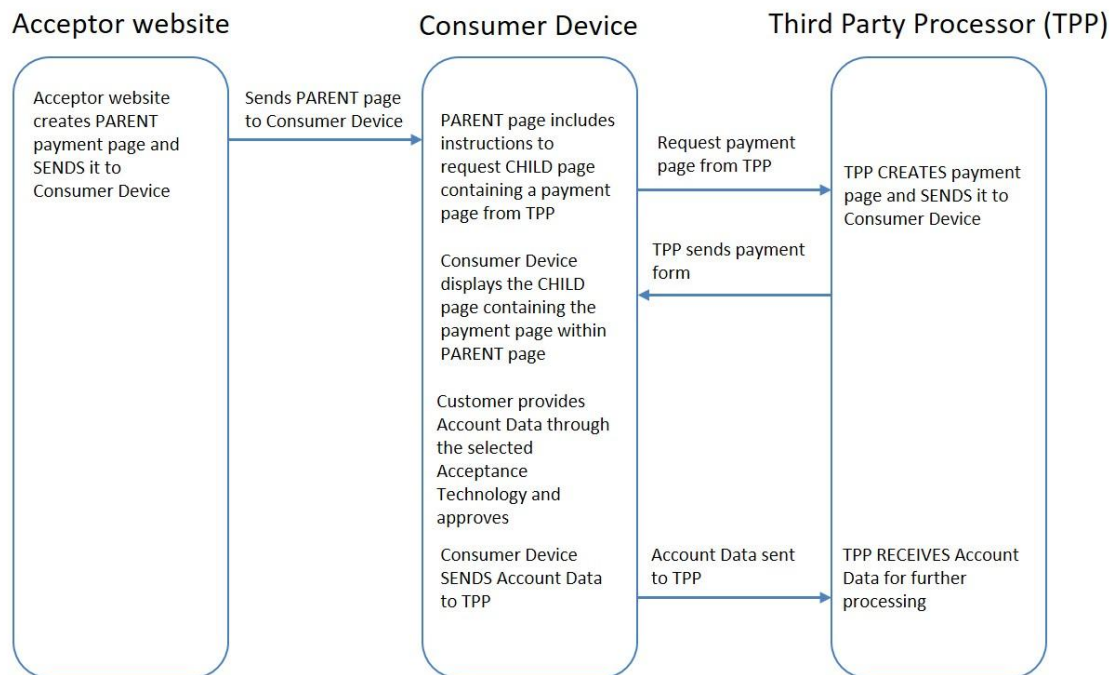


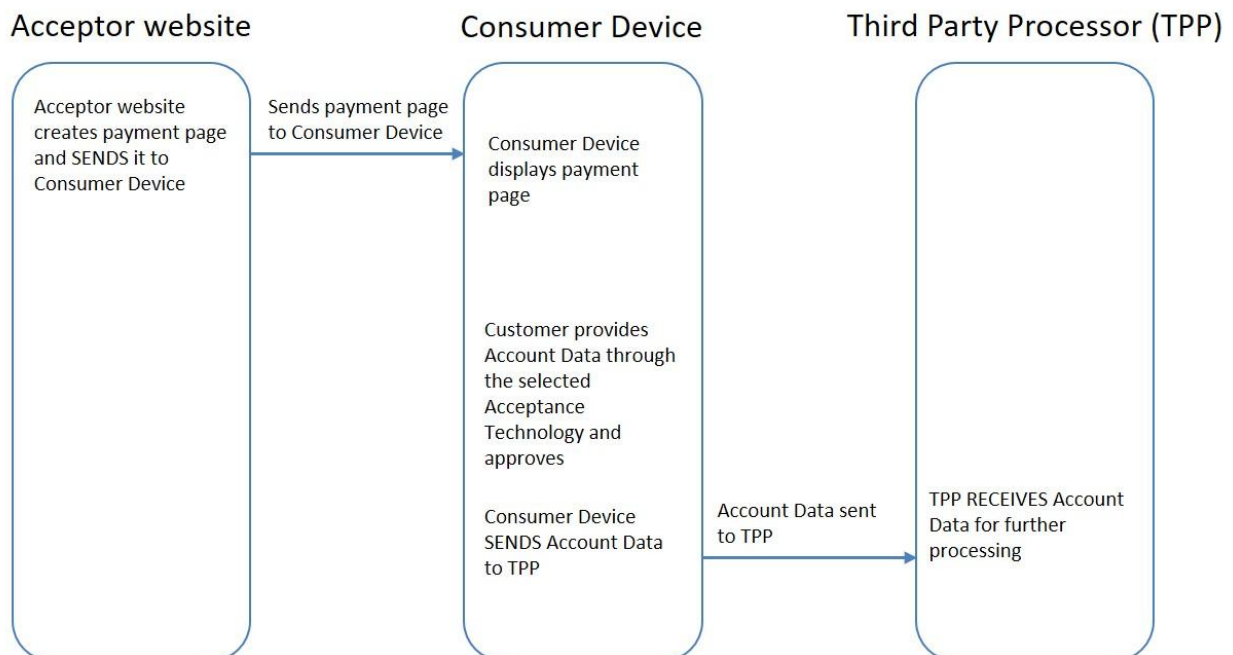
FIGURE 22: THE IFRAME

828

829

### 830 3.5.3. The direct post

831 The following figure illustrates the different steps involved in the configuration whereby the  
832 Consumer Device is displaying the payment page. This configuration is also sometimes referred to  
833 as “browser API” or “silent post”.



834

FIGURE 23: THE DIRECT POST

### 3.5.4. The JavaScript created form

The following figure illustrates the different steps involved in the configuration whereby the Customer is presented with a form created in JavaScript within the payment page.

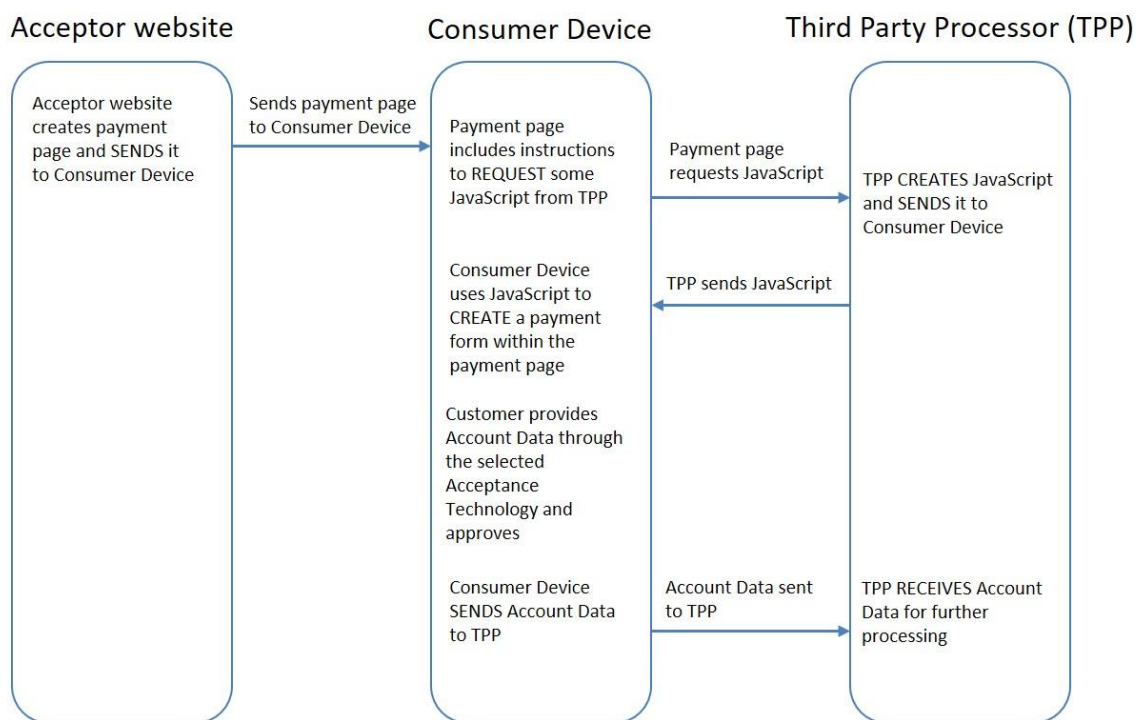


FIGURE 24: JAVASCRIPT CREATED FORM

### 3.5.5. The API

The following figure illustrates the different steps involved in the configuration whereby a so-called acceptor gateway is sending data from the Acceptor to the TPP in a specific format (e.g., XML).

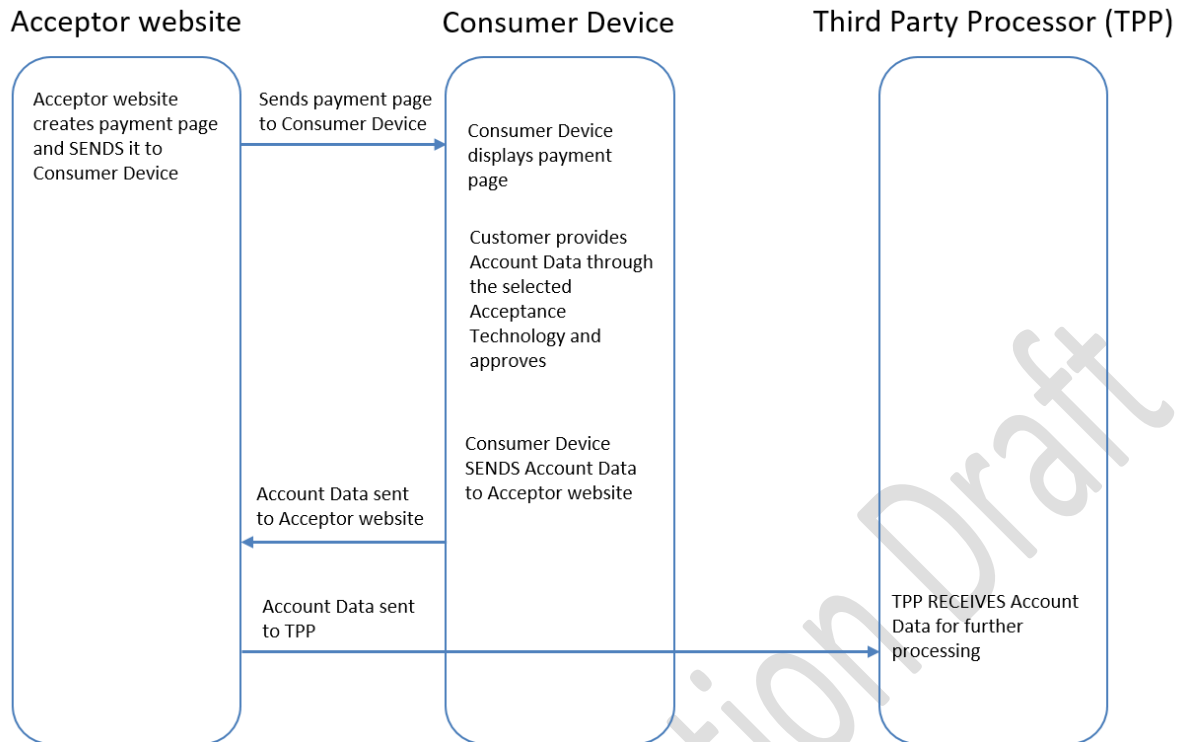


FIGURE 25: THE API

### 3.6. Stored Card Data and SRC in Virtual POI environments

#### 3.6.1. Stored Card Data integration

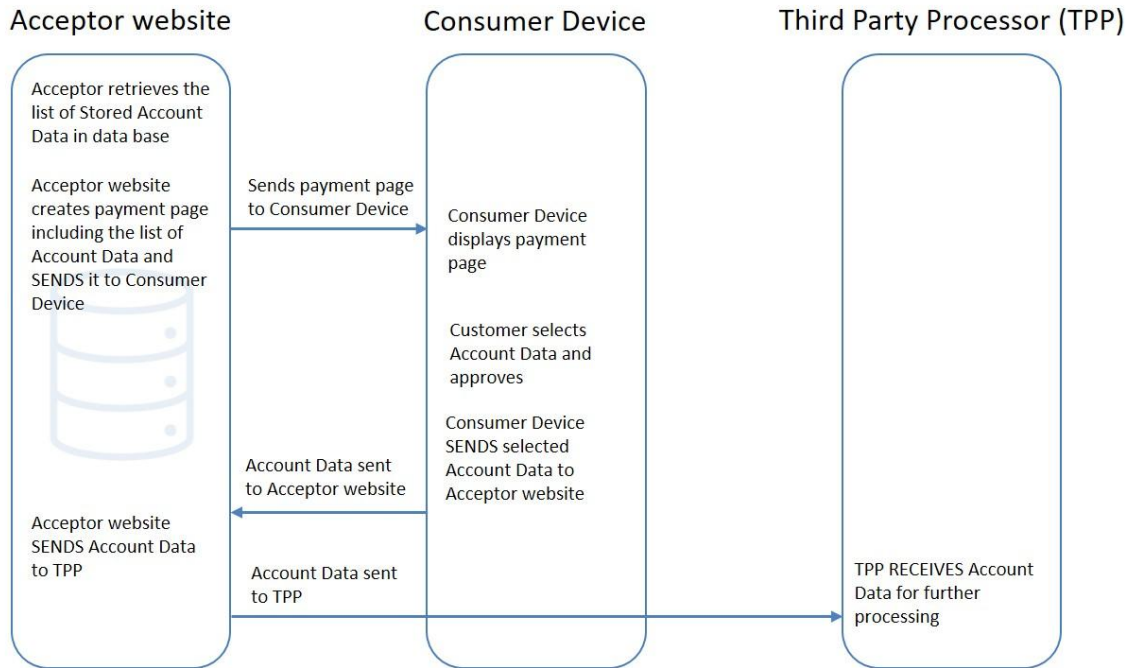
With Stored Card Data, the Acceptors securely store Customer credentials for future use (i.e. future transactions initiated by the Customer, or MITs). This functionality may be used with all integration modes outlined in Section 3.5. However, the location of the Stored Card Data may differ depending on the chosen integration mode :

- Acceptor storage
- TPP storage
- Shared storage

##### 3.6.1.1. Acceptor storage

In this approach, the Acceptor directly stores Card Data, resulting in greater control over the payment experience, but introducing significant impacts regarding management of compliance with PCI DSS requirements (including encryption of sensitive data, strict access controls and possibly tokenization). This approach is commonly used with API integration mode.

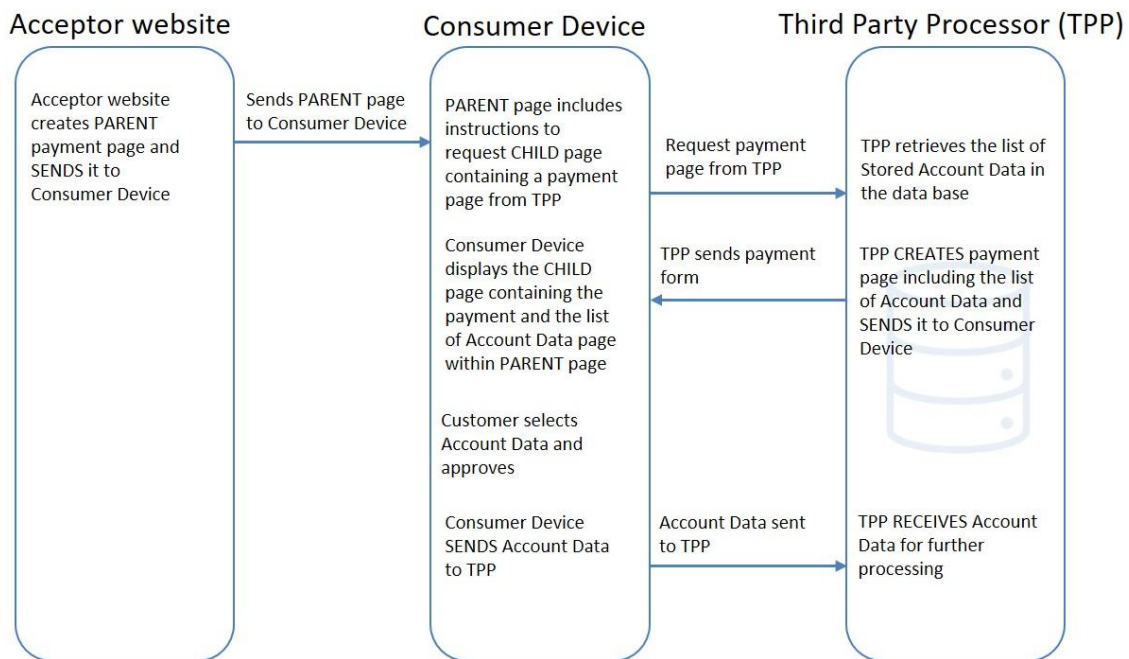




**FIGURE 26:** EXAMPLE OF ACCEPTOR STORAGE IN API INTEGRATION MODE

### 3.6.1.1. TPP storage

In this approach, the Acceptor entirely delegates Card Data storage to the TPP, minimizing its PCI DSS obligations. The TPP handles security responsibilities. This approach is commonly used with integration modes like iFrame and URL Redirection.

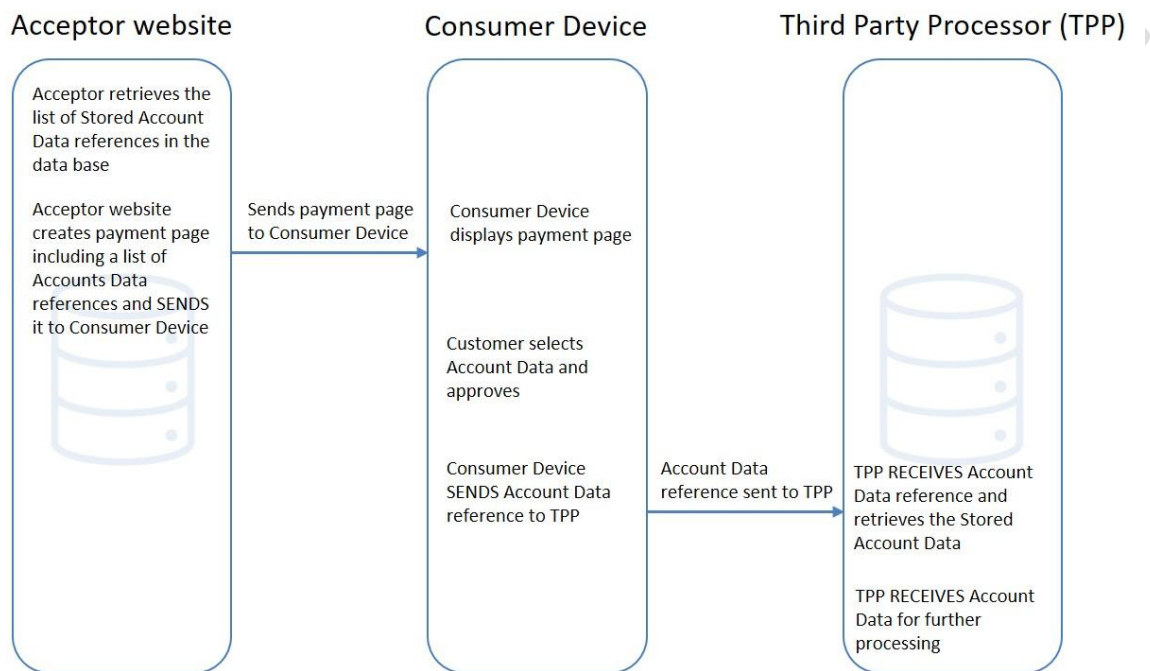


**FIGURE 27:** EXAMPLE OF TPP STORAGE IN iFRAME INTEGRATION MODE

873

874 **3.6.1.2. Shared storage**

875 In this approach, both the Acceptor and the TPP share responsibilities for Card Data storage. The  
876 TPP typically stores sensitive data and provide to the Acceptor non-sensitive references such as  
877 tokens or aliases to be stored. In addition, the Acceptor may store additional non-sensitive data to  
878 allow the Customer to identify the Card to be used (e.g. last four digits,...). This approach balances  
879 control and security for the Acceptor.



880

881 **FIGURE 28: EXAMPLE OF SHARED STORAGE IN DIRECT POST INTEGRATION MODE**

882

883 **3.6.2. SRC-Specific Integration Considerations**

884 SRC aims at minimising the number of times Customers enter their Account Data. But unlike  
885 traditional models where Acceptors store Account Data, SRC shifts data storage and management  
886 to SRC entities. This reduces the Acceptor's security obligations shifting them to the SRC entities.

887 Key participants in SRC data storage:

- 888 • SRC System: Stores SRC profiles, including Customer identity and related information.
- 889 • Digital Card Facilitator (DCF) : Primarily responsible for storing and providing Customer data  
890 such as billing/shipping addresses, and other details linked to a specific Customer identity.

891 SRC implementations may integrate with Payment Tokenisation, replacing the PAN with a Payment  
892 Token. In this configuration, the SRC System acts as a Token Requestor to the Token Service  
893 Provider (TSP).

Note: In the following flows, we consider that:

- The initiation and recognition phases are already performed and the Customer is recognised.
- The DPA is the entity enabling the initial interaction of a Customer with an Acceptor. It can be any payment-enabled application such as an Acceptor Website, or a Payment Application on the Consumer Device.
- The SRCI corresponds to the Third Party Processor (TPP).
- The headers in blue correspond to the roles of the participants in the SRC specifications.

### 3.6.2.1. SRC Checkout

The following figure illustrates the standard SRC Checkout where the checkout process is orchestrated and facilitated by the SRC System.

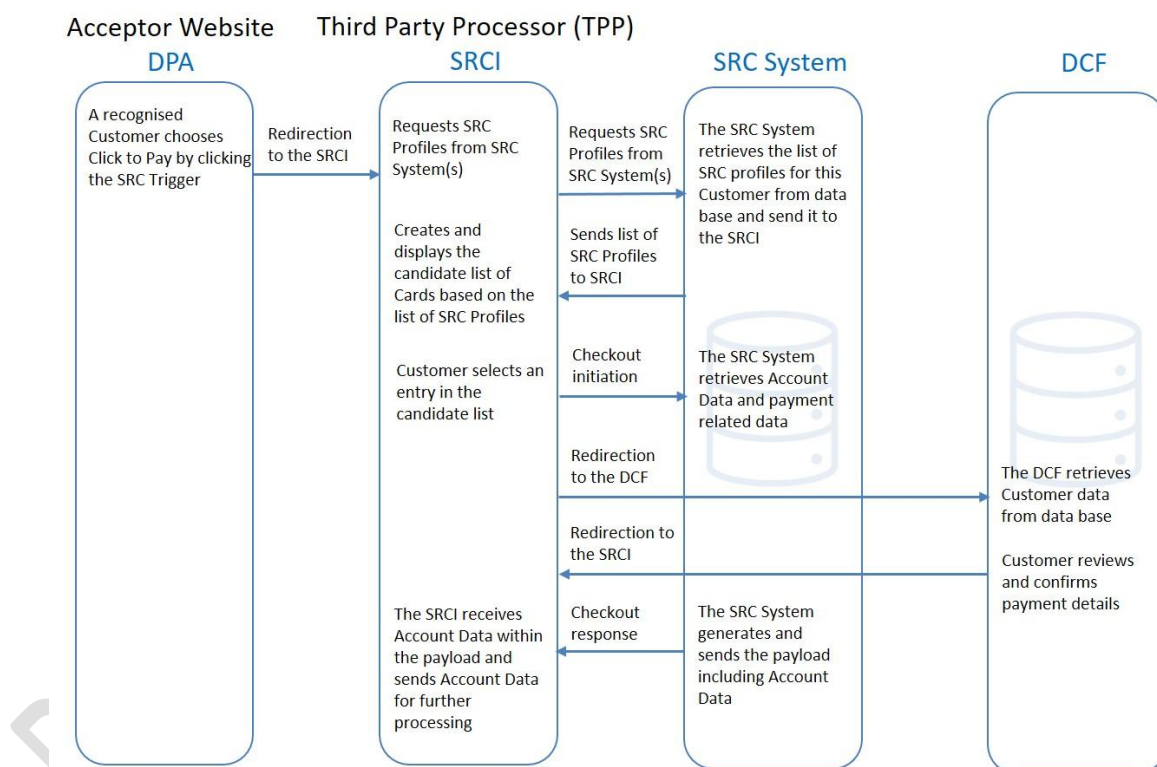


FIGURE 29: SRC CHECKOUT

### 3.6.2.2. Merchant Checkout

In addition to the standard SRC Checkout illustrated above, the SRC specifications offer the flexibility to support alternative Acceptor-driven checkout experiences (Merchant Checkout) where the Acceptor takes on several roles by acting as both SRC Initiator (SRCI) and Digital Card Facilitator (DCF), in addition to the role of Digital Payment Application (DPA).

#### 3.6.2.2.1. Merchant Orchestrated Checkout

The following figure illustrates the Merchant Orchestrated flow, where a purchase experience is fully integrated within the Acceptors' current checkout, allowing them to control the user experience and manage recognition of Customer. In this configuration, the Acceptor acts as DCF and is responsible for storing Customer data such as billing/shipping addresses.

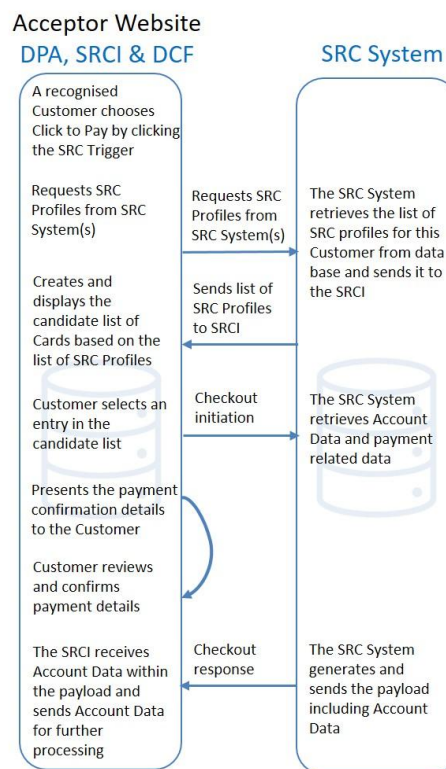
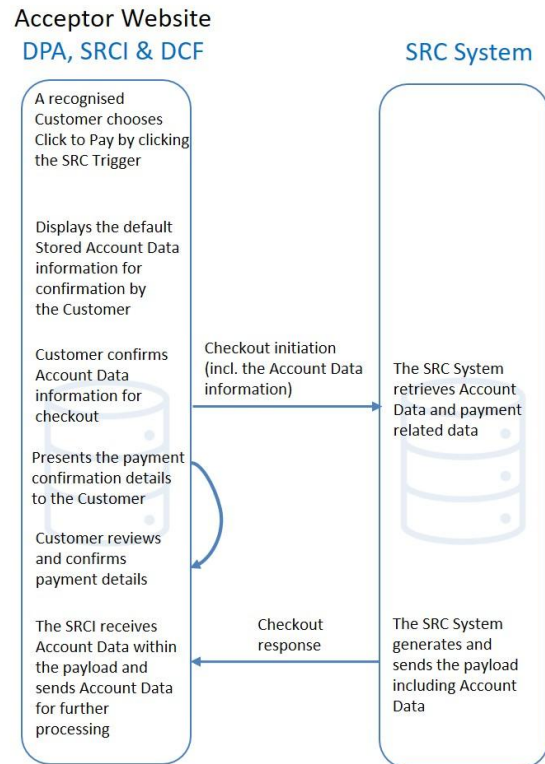


FIGURE 30: MERCHANT ORCHESTRATED CHECKOUT

#### 3.6.2.2.2. Merchant Digital Card On File Checkout

The following figure illustrates the Merchant Digital Card-On-File Checkout, where a purchase experience allows the Customer to designate a Card enrolled with a SRC System, which becomes their default digital Card stored by this specific Acceptor. In this configuration, the Acceptor also stores Account Data information from the designated digital Card and invokes the SRC System to obtain the payload for the transaction.



**FIGURE 31: MERCHANT DIGITAL CARD-ON-FILE CHECKOUT**

## 4. BEST PARCTICES FOR IMPLEMENTATION PER PAYMENT CONTEXT

This section provides guideline for implementation for each payment context (Local and Remote), including functional and security aspects required by Books 2 and 4 of this Volume. For detailed requirements, please refer directly to these Books.

### 4.1. Local Transaction

#### 4.1.1. Chip with Contact

##### 4.1.1.1. One-off Payment

##### 4.1.1.1.1. Definition of the payment context

The POI is a Physical POI which could be standalone or integrated with the sales system. For unattended the POI is always integrated with the sales system.

For contact chip transactions SCA is required with exemptions as described in PSD2, e.g. for unattended POI used for Transport and Parking.

The following table describes the characteristics of this context from an Acceptance perspective:

Characteristics of the context	Attended	Unattended	
	with Cardholder Verification	with Cardholder Verification	without Cardholder Verification
Acceptance Technology	Chip Contact shall be supported as a minimum by the Physical POI		
Card and Cardholder present	Y		
Final amount known	Y		
Authorisation	Authorisation may either be online or offline		
Data Capture	All 3 modes defined in section 3.4 are applicable		
Attendant Present	Y	N	
EMV Offline Card Authentication	SDA not supported Offline with Online capability POI: DDA and CDA required Online only POI: DDA optional and CDA optional (recommended)		
Cardholder Verification Method	PIN mandatory	PIN mandatory	“No CVM Required” mandatory

Table 32: Local Transaction Contact Payment - Acceptance Characteristics

949 The following table describes the characteristics of this context from an Issuance perspective:

Characteristics of the context	with Cardholder Verification	without Cardholder Verification
Acceptance Technology	Chip Contact shall be supported as a minimum by the Card Application	
Authorisation	The Card Application shall support Online Authorisation and in addition may support Offline Authorisation	
Card Authentication	<p>For all newly issued and replacement Cards</p> <p>SDA not permitted</p> <p>DDA optional</p> <p>CDA mandatory</p> <p>XDA mandatory if ECC is supported</p>	
Cardholder Verification Method	PIN mandatory	"No CVM Required" mandatory <sup>6</sup>

950 **Table 33:** Local Transaction Contact Payment - Issuance Characteristics

<sup>6</sup> For Cards that do not support "No CVM Required", Issuers may receive an authorisation message containing "Cardholder Verification was not successful". It is up to the issuer to authorise or decline this message.

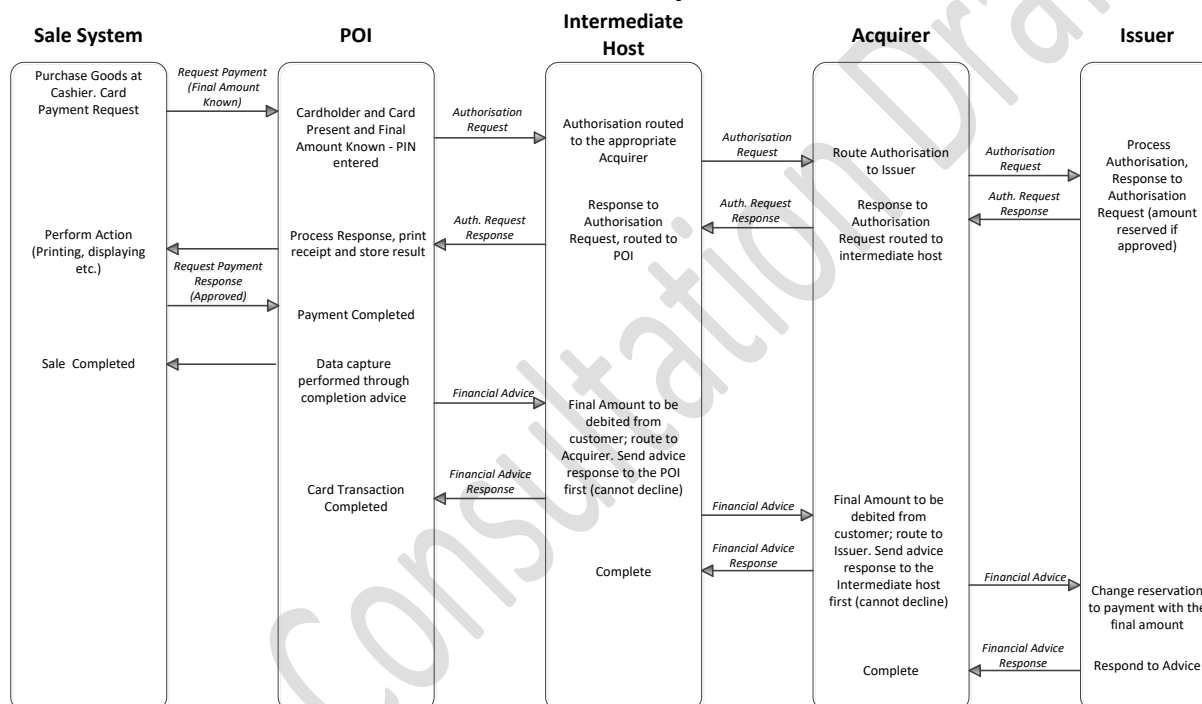


#### 4.1.1.1.2. Example of Message Flows

##### 4.1.1.1.2.1. Example of Message Flow - Attended with PIN

Two sample message flows are described below as examples of common implementations. In the Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes only. The physical location of the stored data is an implementation option of the Acceptor and may be different from the location of the POI.

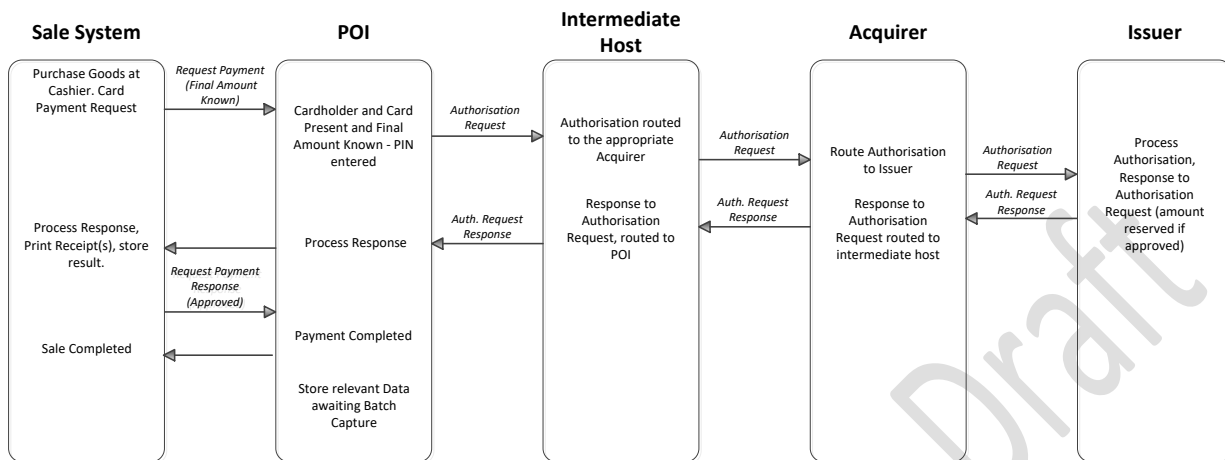
### Payment in attended environment, Cardholder is present, Cardholder Verification performed and final amount known. Capture immediately after Transaction Completion.



**FIGURE 34:** EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION



## Payment in attended environment, Cardholder is present, Cardholder Verification performed and final amount known. Capture by Batch.

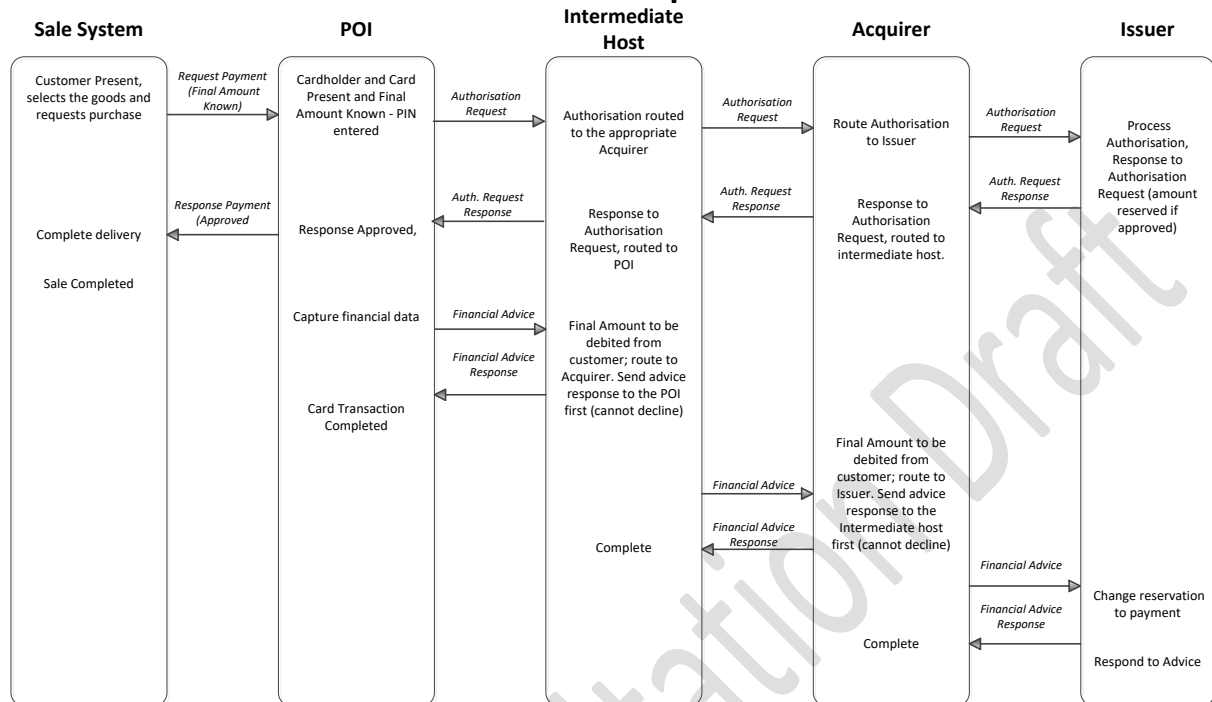


**FIGURE 35:** EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

### 4.1.1.1.2.2. Example of Message Flow - Unattended with PIN

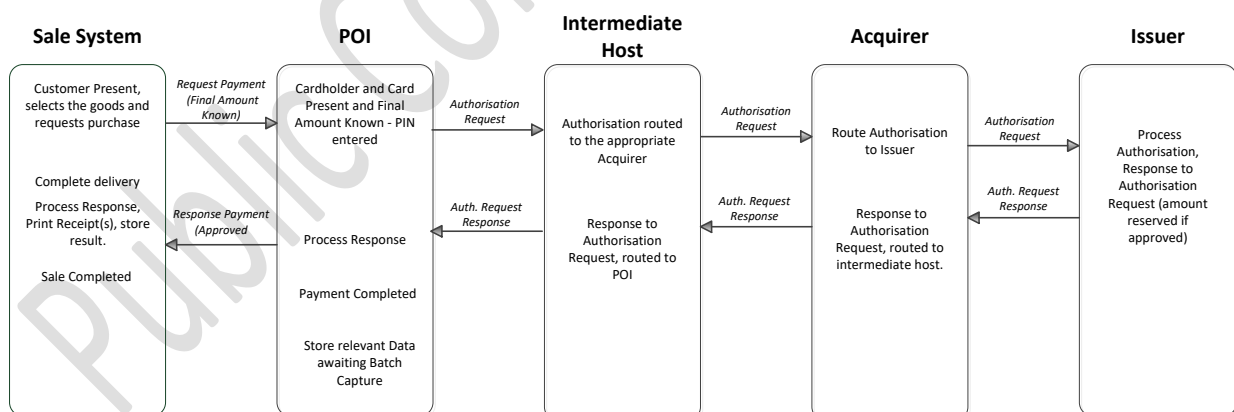
Two sample message flows are described below as examples of common implementations. In the Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes only. The physical location of the stored data is an implementation option of the Acceptor and may be different from the location of the POI.

**Payment in unattended environment, Cardholder is present, Cardholder Verification performed and final amount known. Capture immediately after transaction completion.**



**Figure 36: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION**

**Payment in unattended environment, Cardholder is present, Cardholder Verification performed and final amount known, Capture by Batch**

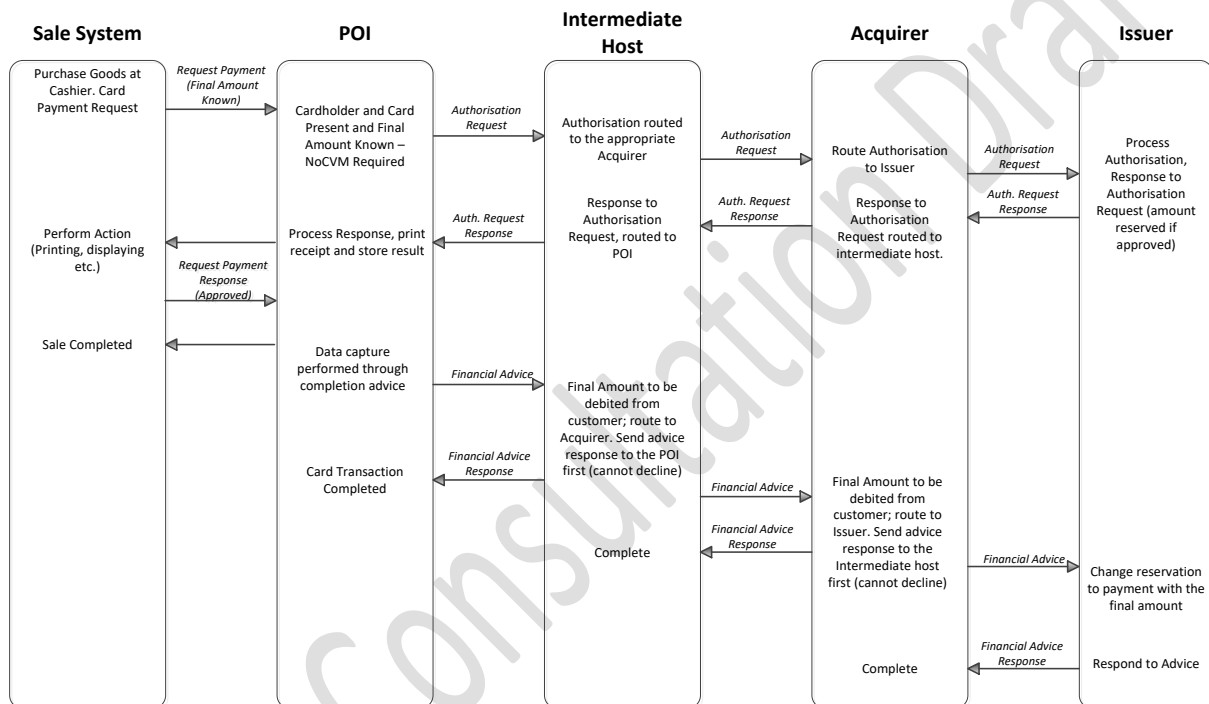


**Figure 37: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN, CAPTURE BY BATCH**

#### 4.1.1.1.2.3. Example of Message Flow - Unattended with “No CVM Required”

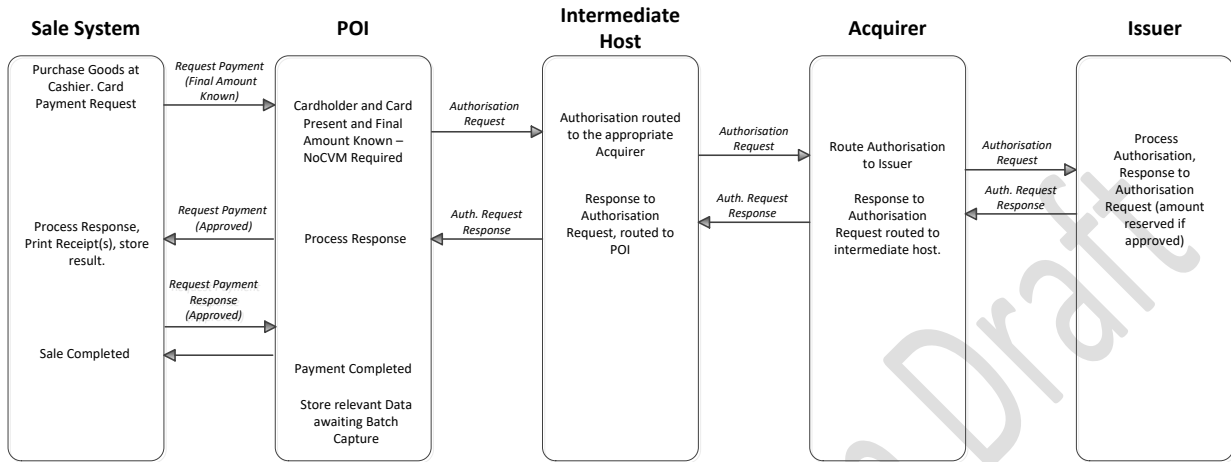
Two sample message flows are described below as examples of common implementations. In the Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes only. The physical location of the stored data is an implementation option of the Acceptor and may be different from the location of the POI.

### Payment with ‘No CVM Required’ in unattended environment, Cardholder present and final amount known. Capture immediately after Transaction Completion



**Figure 38: EXAMPLE FLOW: PAYMENT WITH ‘NO CVM REQUIRED’ IN UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION.**

## Payment with 'No CVM Required' in attended or unattended environment, Cardholder present and final amount known. Capture by Batch.



**Figure 39:** EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

991 4.1.1.2. Deferred Payment

992 4.1.1.2.1. Definition of the payment context

993 This context is used in environments where the final amount to be paid for the goods or services is  
994 not known by the acceptor at the time online authorisation is performed. The final amount is  
995 known on completion of delivery.

996 The POI is a Physical POI which could be standalone or integrated with the sales system. For  
997 unattended the POI is always integrated with the sales system.

998 The following table describes the characteristics of this context from an Acceptance perspective:

Characteristics of the context	Attended	Unattended	
	with Cardholder Verification	with Cardholder Verification	without Cardholder Verification
Acceptance Technology	Chip Contact shall be supported as a minimum by the Physical POI		
Card and Cardholder present	Y		
Final amount known	N (at the time of authorisation)		
Authorisation	Authorisation shall always be online Partial approval shall be supported by Acquirers and Acceptors The Physical POI shall either be online only or offline with online capability		
Data Capture	Modes 1 and 2 as defined in section 0 are applicable <sup>7</sup>		
Attendant Present	Y	N	
EMV Online Authentication.	Required		
EMV Offline Card Authentication	SDA optional from 2020 <sup>8</sup> Offline with Online capability POI: DDA and CDA required Online only POI: DDA optional and CDA optional (recommended)		
Cardholder Verification Method	PIN required	PIN required	“No CVM Required” required

999 **Table 40:** Local Transaction Deferred Payment - Acceptance Characteristics

<sup>7</sup> Mode 3 is not applicable as, at the time of Authorisation, the final amount is not known.

<sup>8</sup> SDA is still required by some non SEPA general purpose Card schemes

1000 The characteristics of this context from an Issuance perspective are the same as described for  
1001 payment, see table 4:

1002 The flow described below will provide all necessary information to the issuer allowing them to  
1003 adjust any reserved amount with the final amount, thereby avoiding Cardholder complaints.

1004 This service enables the acceptor to:

- 1005 • Request an authorisation from the issuer to get a maximum amount available for the  
1006 transaction where the amount requested may be chosen by the acceptor or Cardholder;
- 1007 • Obtain a full approval, or a partial approval when the Cardholder has insufficient funds for  
1008 the amount requested;
- 1009 • Complete the delivery of goods or use of service to be paid up to the approved amount within  
1010 a limited time frame (e.g., 20 minutes for petrol);
- 1011 • Inform the issuer of the payment of these goods or services with the final amount that is less  
1012 than or equal to the authorised amount in real time.

1013 This service is usually used at petrol stations, attended and unattended. The following rules apply:

- 1014 1) The amount that is requested to be authorised online is the maximum amount that may be  
1015 required;
- 1016 2) In order to avoid transactions being unnecessarily declined, Issuers shall support partial  
1017 approval in responses when the “Cardholder Available Funds” is lower than the amount  
1018 requested;
- 1019 3) All parties in the protocol chain shall forward and/or act on online advice messages (or  
1020 reversal), including zero amounts, so that the Cardholder Available Funds shall be adjusted  
1021 in real time. If additional messages (e.g., batch clearing messages) are received, they shall  
1022 be correctly handled”.

#### 1024 4.1.1.2.2. Example of Message Flows

1025 Two sample message flows are described below as examples of common implementations. In the  
1026 Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes  
1027 only. The physical location of the stored data is an implementation option of the Acceptor and may  
1028 be different from the location of the POI.

## Deferred Payment Card Message Flow. Capture immediately after Transaction Completion, using the financial advice

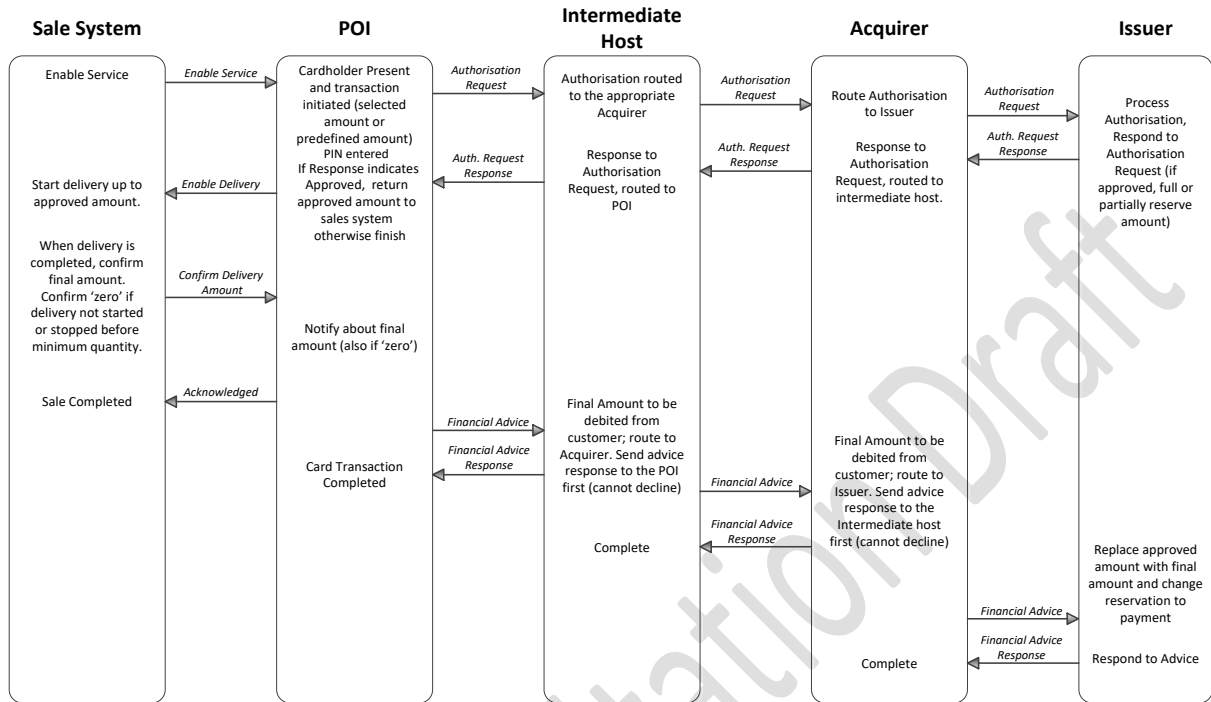
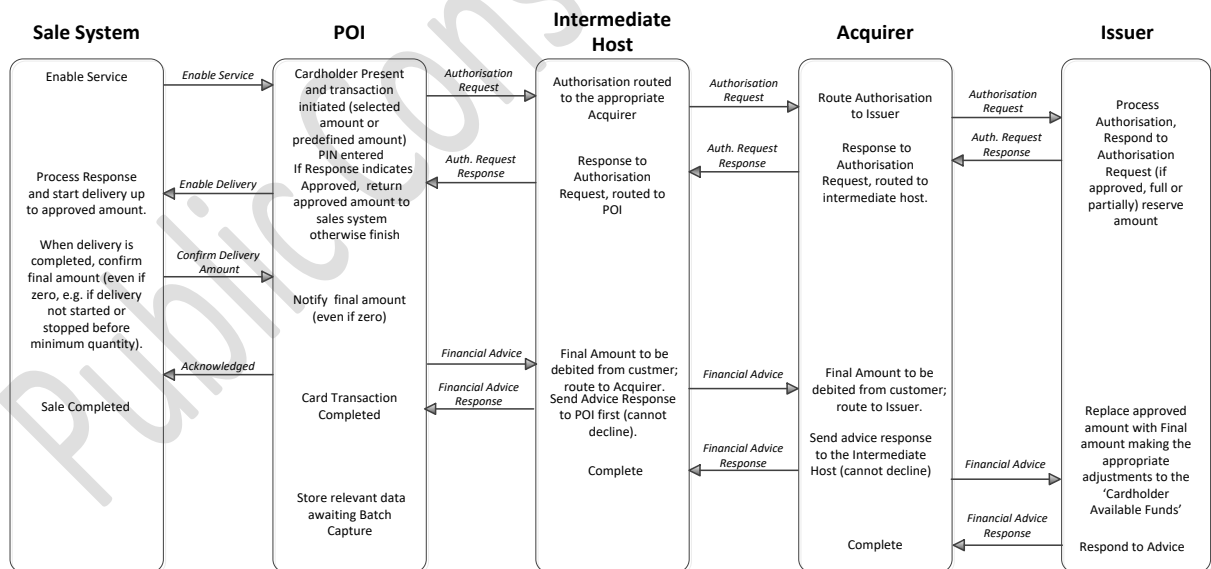


FIGURE 41: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

## Deferred Payment Card Message Flow, Capture by Batch.



Footnote to Issuer: if separate batch clearing is used, do not show sale twice.

FIGURE 42: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE BY BATCH

1034 4.1.1.3. Pre-Authorisation Services

1035 4.1.1.3.1. Definition of the payment context

1036 This payment context is used in an environment where the final amount is not known but a  
1037 guarantee of payment is required for the Acceptor. This context allows:

- 1038 • The Acceptor to reserve an estimated amount until the final amount is known.
- 1039 • The Issuer to more efficiently manage the Cardholder Available Funds in real-time, by  
1040 either reserving or releasing funds.

1041 A Pre-Authorisation Service is used to reserve the funds for an estimated amount. Thereafter, the  
1042 estimated amount can be increased or decreased using an Update Pre-Authorisation Service. A  
1043 Payment Completion Service is used to finalise the transaction when the final amount is known.

1044 In the event that the amount pre-authorised is not used, the previously authorised amount(s) must  
1045 be released by the Cancellation Service. In this case Payment Completion shall not follow.

1046 This context is mostly used for e.g., hotels and car hire, etc.

1047 In most cases the same Card is used for Pre-Authorisation and Payment Completion. However, if  
1048 a different Card is used for Payment Completion, then any amounts authorised on the other  
1049 Card(s) used for Pre-Authorisation shall be removed using the Cancellation Service.

1050 The POI is a Physical POI which could either be a standalone device or a device integrated with the  
1051 point of sale. For unattended the POI is always integrated into the Sales system.

1052 The Pre-Authorisation services may either be performed as Card Present or Card Not Present  
1053 transactions.

1054 The following table describes the characteristics of this context from an Acceptance perspective:

Characteristics of the context	Attended	Unattended
Acceptance Technology	Chip Contact shall be supported as a minimum by the Physical POI	
Card and Cardholder present	Y/N	
Final amount known	N	
Authorisation	Authorisation shall be online. The Physical POI shall either be offline with online capability or online only	
Data Capture	NA	



Characteristics of the context	Attended	Unattended
Attendant Present	Y	N
EMV Online Card Authentication.	Required	
EMV Offline Card Authentication	SDA optional from 2020 <sup>9</sup> Offline with Online capability POI: DDA and CDA required Online only POI: DDA and CDA optional (recommended)	
Cardholder Verification Method	PIN Mandatory	PIN Mandatory

1055 **Table 43:** Local Transaction Pre-Authorisation and Update Pre-Authorisation Service - Acceptance Characteristics

<sup>9</sup> SDA is still required by some non SEPA general purpose Card schemes.

Characteristics of the context	Attended	Unattended
Acceptance Technology	Chip Contact shall be supported as a minimum by the Physical POI	
Card and Cardholder present	Y/N	
Final amount known	Y	
Authorisation	NA for payment completion	
Data Capture	Modes 1 and 2 as defined in section 0 are applicable <sup>10</sup>	
Attendant Present	Y	N
EMV Online Card Authentication.	NA for payment completion	
EMV Offline Card Authentication	NA for payment completion	
Cardholder Verification Method	NA for payment completion	

**Table 44:** Local Transaction Payment Completion Service - Acceptance Characteristics

The characteristics of this context from an Issuance perspective are the same as described for payment, see table 11:

#### Card Services

The Pre authorisation Services will consist of two or more of the following steps:

- A Pre-Authorisation to reserve funds when the final amount is not known;
- Update Pre-Authorisation(s)<sup>11</sup> to increase or decrease the pre-authorised amount if, prior to completion, the pre-authorised amount;
  - Is insufficient to cover the estimated final amount.
  - Is more than that required to cover the estimated final amount, to reduce the reserved amount(s) including, if necessary, to zero.
- Payment completion for an equal or lesser amount than the amount previously Authorised when the final amount is known

Or

- As soon as it is known that a Pre-Authorisation and any Update Pre-Authorisations linked to it will not be used, the previously authorised amount(s) must be released by a Cancellation, that cancels the Pre-Authorisation and any Update Pre-Authorisation linked to it.

In this case Payment Completion shall not occur.

As the Pre-Authorisation service consists of two or more steps, they are linked together using a unique identifier (UID). This UID is included in the Pre-Authorisation response message and reused in subsequent transactions.

An update Pre-Authorisation cannot occur after a payment completion.

Issuers shall adjust the 'Cardholder Available Funds' in real time by acting upon Pre-Authorisation, update Pre-Authorisation(s), payment completion and cancellation.

Acceptors shall:

- Process a Pre-Authorisation or update Pre-Authorisation if the amount is estimated;
- Process an update-Pre-Authorisation if the estimated amount is greater or less than that originally authorised, alternatively the authorisation may be cancelled if the final amount is zero.
- Only process the payment completion equal to or less than the accumulated authorised amount(s).

---

<sup>10</sup> If Authorisation is used for Payment Completion, Mode 3 may also be used for Data Capture.

<sup>11</sup> Multiple update Pre-Authorisation(s) may be used in this scenario.

1088

1089

#### 4.1.1.3.2. Example of Message Flows

1090

1091

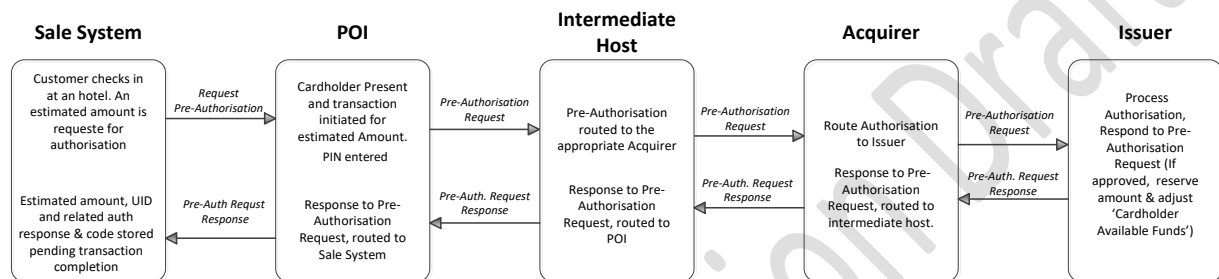
1092

1093

Four sample message flows are described below as examples of common implementations. In the Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes only. The physical location of the stored data is an implementation option of the Acceptor and may be different from the location of the POI.

1094

#### Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount, cardholder present: Pre-Authorisation



In the Pre-Authorisation request the presence of the UID is optional. In the pre-authorisation response the presence of UID is mandatory

#### No Data Capture

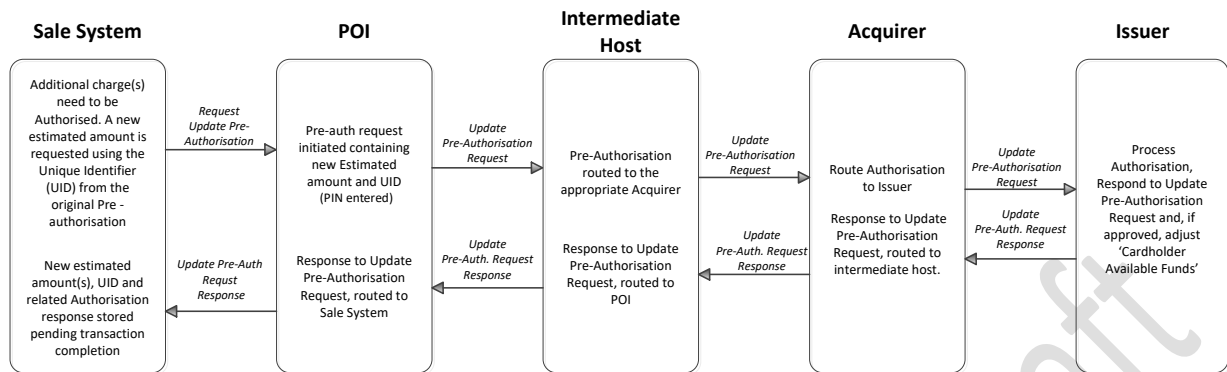
1095

1096

1097

**Figure 45: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT, CARDHOLDER PRESENT: PRE-AUTHORISATION**

## Pre-Authorisation Services in an attended or unattended environment to reserve an estimated amount: Update Pre-authorisation

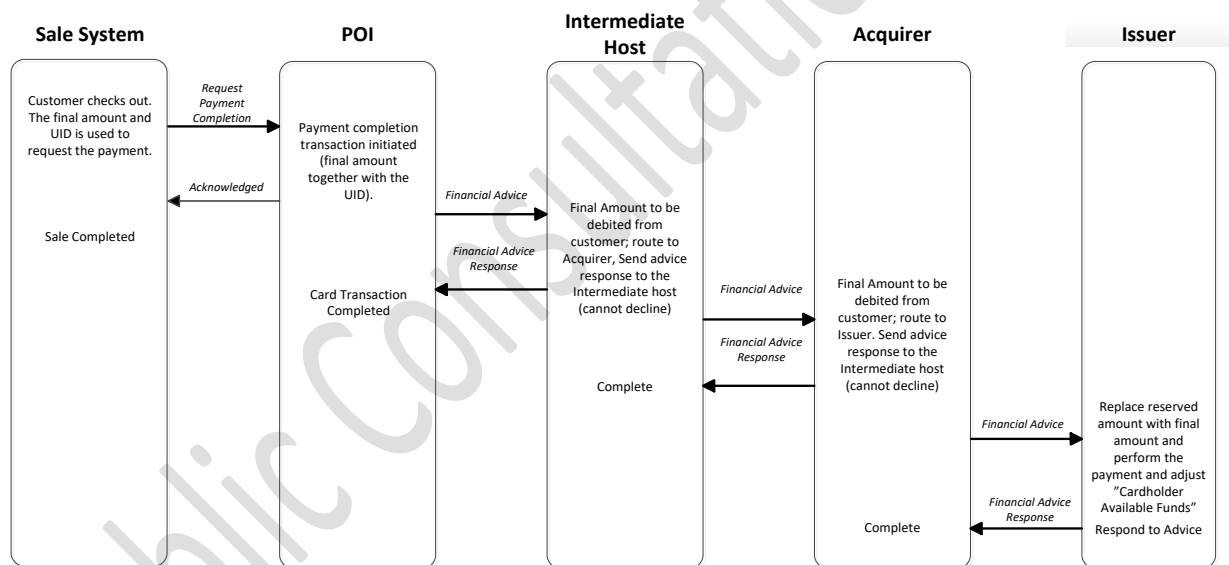


In the Update Pre-Authorisation request and response the presence of the UID is mandatory.

### No Data Capture

**Figure 46:** EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AN ESTIMATED AMOUNT: UPDATE PRE-AUTHORISATION

## Pre-Authorisation services in an attended or unattended environment to reserve and secure an amount: Payment Completion. Capture immediately after Transaction Completion.

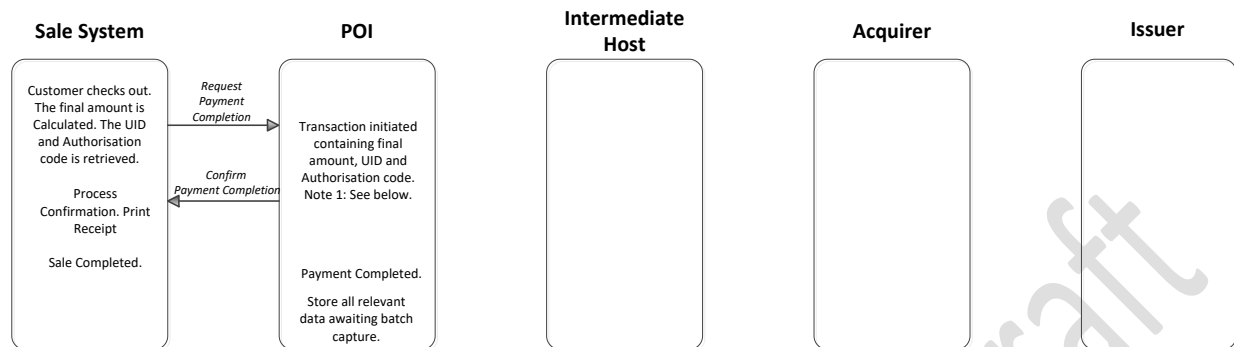


In the Payment completion the presence of the UID is mandatory.

**Figure 47:** EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

1104

## Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount: Payment Completion. Capture by Batch



In the Payment completion the presence of the UID is mandatory.

1: Final amount check to ensure it equals or is within the configurable percentage allowed:  
If greater, an additional update Pre-Authorisation Request is performed as described in the update Pre-Authorisation.  
If less an adjustment is processed to adjust the Cardholders 'Cardholder Available Funds'

1105

1106

1107

**Figure 48: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN  
AMOUNT: PAYMENT COMPLETION. CAPTURE BY BATCH**

1108

### 4.1.2. Chip and Mobile Contactless

1109

1110

1111

For Chip and Mobile Contactless only One-off Payment is described. The description for Deferred Payment and Pre-Authorisation Services based on Chip and Mobile Contactless can be derived accordingly from the respective descriptions in section 4.1.1.

1112

1113

#### 4.1.2.1. One-off Payment

1114

##### 4.1.2.1.1. Definition of the payment context

1115

1116

This payment context is used for contactless transactions initiated by a Physical Card or a Mobile Contactless Application on a Mobile Device.

1117

1118

The POI is a Physical POI which could be standalone or integrated with the sales system. For unattended the POI is always integrated with the sales system.

1119 The following table describes the characteristics of this context from an Acceptance perspective:

Characteristics of the context	Attended	Unattended
Acceptance Technology	Chip or Mobile Contactless	
Card and Cardholder present	Y	
Final amount known	Y	
Authorisation	Authorisation may either be online or offline The Physical POI shall either be offline with online capability or online only However, it is recommended to be offline with online capability	
Data Capture	All 3 modes defined in section 3.4 are applicable	
Attendant Present	Y	N
EMV Online Card Authentication.	Required	
EMV Offline Card Authentication	Offline with Online capability POI: CDA or fDDA required Online only POI: CDA or fDDA required	
Cardholder Verification Method	Online PIN CDCVM No CVM Required Signature <sup>12</sup>	Online PIN CDCVM No CVM Required

1120 **Table 49:** Local Transaction Contactless Payment - Acceptance Characteristics

1121 The following table describes the characteristics of this context from an Issuance perspective:

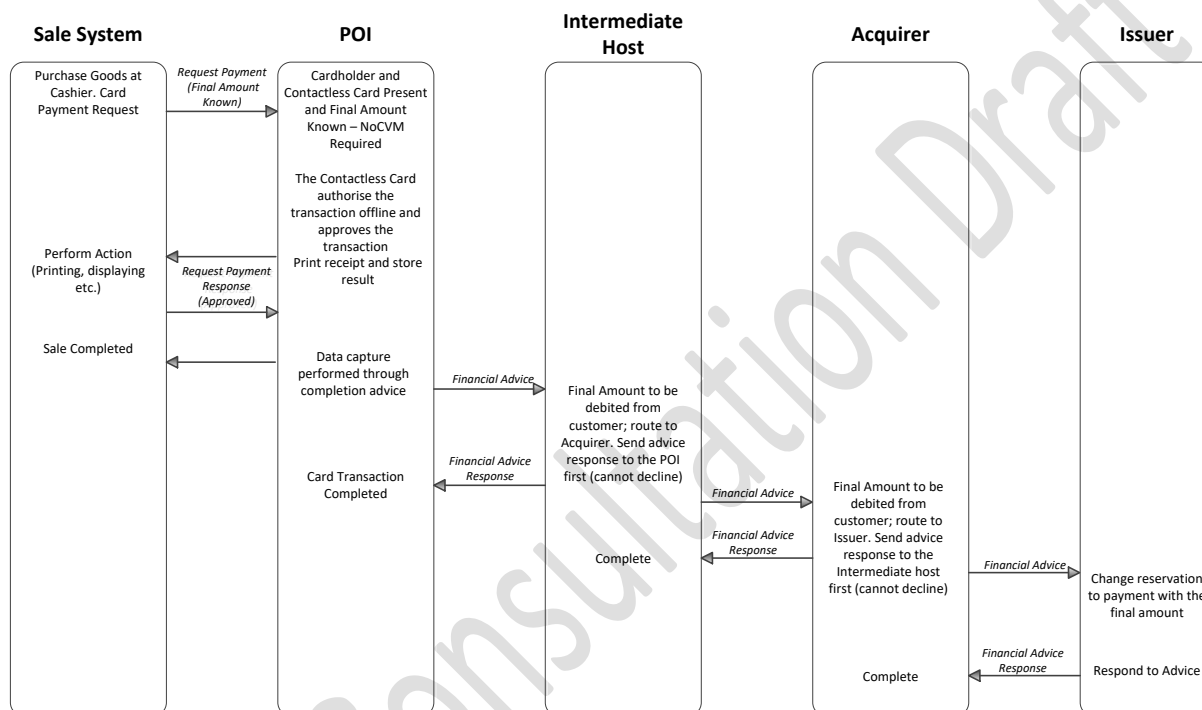
Authorisation	The Card Application shall support Online Authorisation and in addition may support Offline Authorisation
Card Authentication	CDA or fDDA required BDHLA mandatory if ECC is supported
Cardholder Verification Method	Online PIN CDCVM No CVM Required Signature

1122 **Table 50:** Local Transaction Contactless Payment - Issuance Characteristics

#### 4.1.2.1.2. Example of Message Flows

Four sample message flows are described below as examples of common implementations. In the Capture by Batch diagram, the data is shown as stored in the POI. This is for illustration purposes only. The physical location of the stored data is an implementation option of the Acceptor and may be different from the location of the POI.

#### **Contactless Payment (Offline Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture immediately after Transaction Completion**

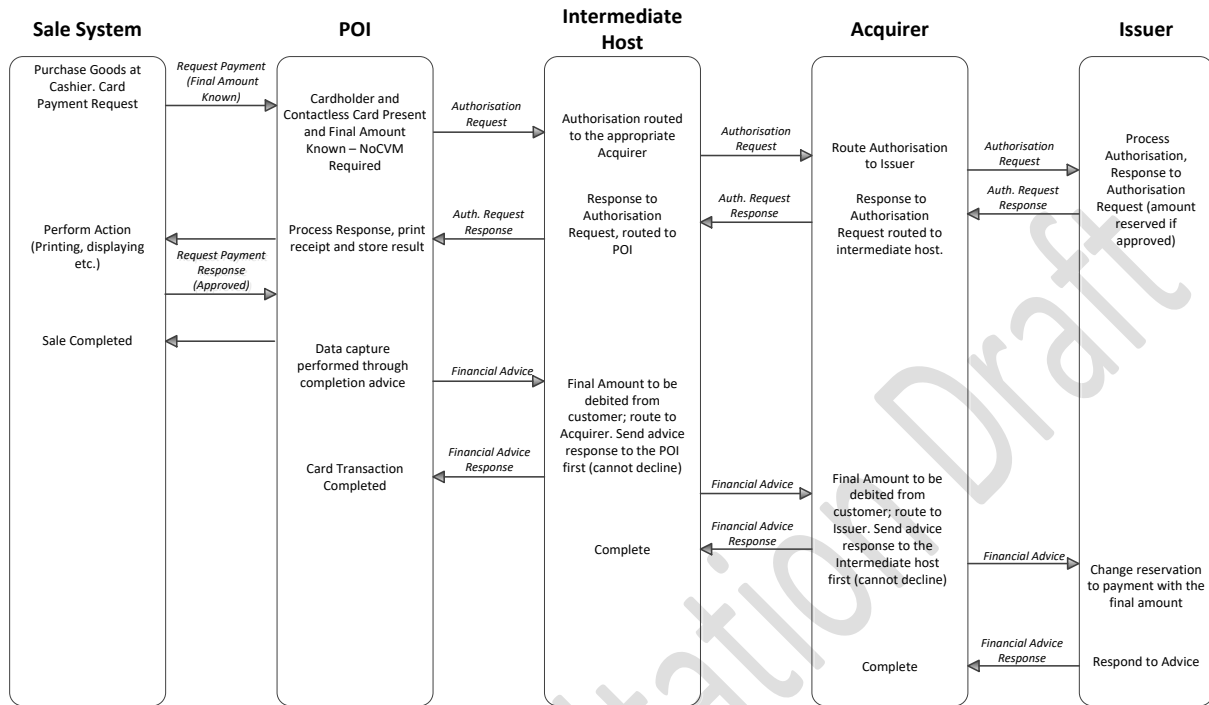


**Figure 51: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION**

<sup>12</sup> for acceptance of Cards which do not support online PIN.

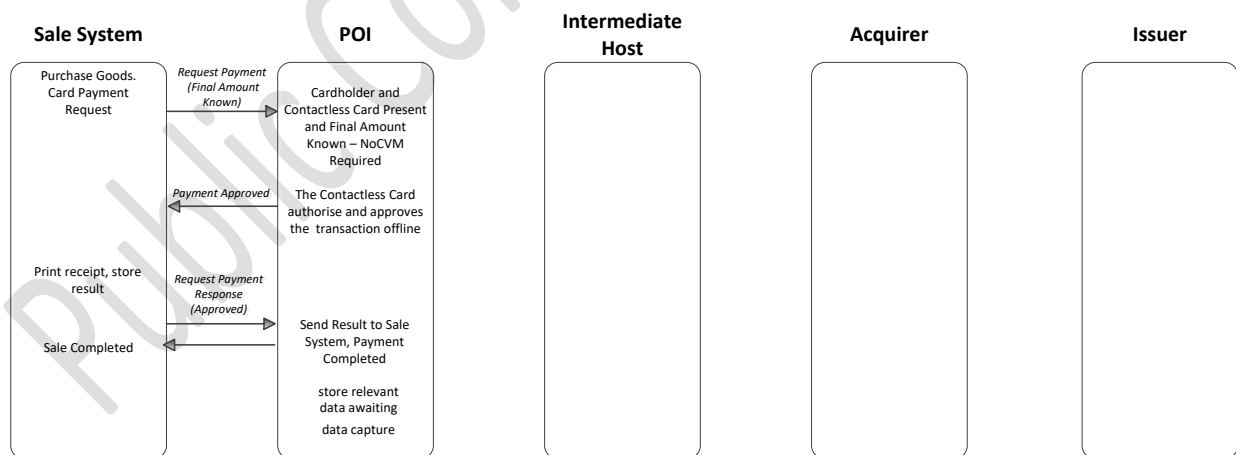


**Contactless Payment (Online Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture immediately after Transaction Completion**



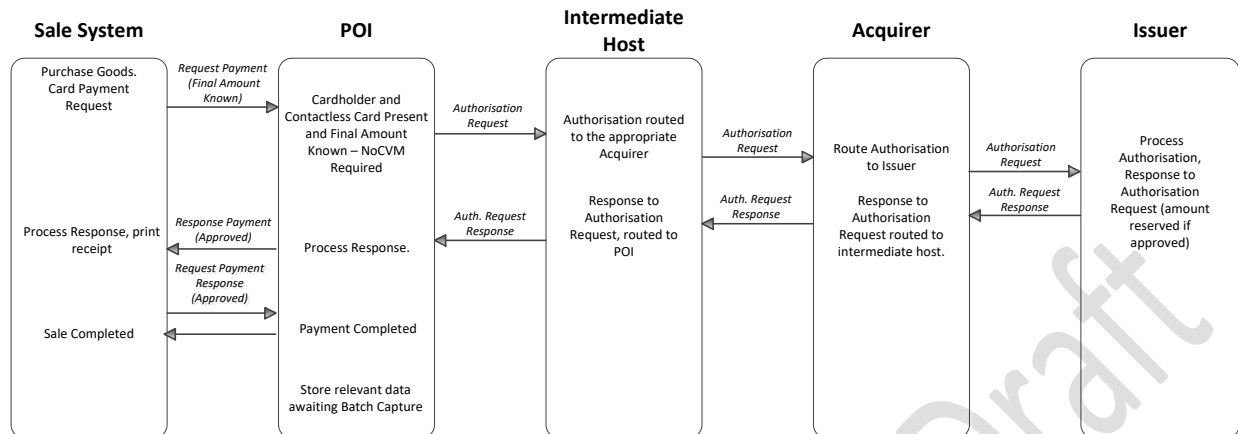
**Figure 52: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION**

**Contactless Payment (Offline Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture by Batch**



**Figure 53: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH**

**Contactless Payment (Online Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture by Batch**



**Figure 54: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH**

## 4.2. Remote Transactions

### 4.2.1. e-and m-Commerce One-off Payment

#### 4.2.1.1. Definition of the payment context

The POI is a Virtual POI which supports a payment page to enter relevant payment related Card Data. This may be integrated with the Acceptor website or hosted externally on a payment gateway, typically hosted by a third party. The relevant payment data is transferred from the payment page via the payment gateway to the Acquirer. The Virtual POI may also facilitate redirection services to support “direct” remote Authentication of the Customer by the Issuer via an authentication server.

1153 The following table describes the characteristics of this context from an Acceptance perspective:

Characteristics of the context	Virtual POI
Acceptance Technology	Consumer Device with Browser over Internet Consumer Device with Dedicated Application over Internet
Payment Device	Remotely
Final amount known	Y
Authorisation	Authorisation shall be online The Virtual POI shall be online
Data Capture	All 3 modes defined in section 3.4 are applicable
Authentication	<p>Risk-Based Authentication to decide whether SCA is required or not (optional, but requires redirection to the Issuer domain)</p> <p>Static Authentication for low risk payments (see [EBA])</p> <p>For SCA, at least two authentication factors of different types (possession, knowledge, inherence) from the following list shall be used, in accordance with regulatory requirements:</p> <ul style="list-style-type: none"> <li>• Dynamic authentication <sup>13</sup> (Possession factor under SCA)</li> <li>• Mobile Code (m-commerce) or Personal Code (e-commerce) (Knowledge factor under SCA)</li> <li>• Biometrics via Sensor on Card or Biometrics on Consumer Device (Inherence factor under SCA)</li> </ul> <p>Redirection to the Issuer domain may occur</p>

1154

<sup>13</sup> Note that some of the methods used for dynamic authentication also facilitate Cardholder authentication (e.g., OTP in some implementations). Redirection to the Issuer domain may occur.

**Table 55:** Remote Transaction One-off Payment - Acceptance Characteristics

The following table describes the characteristics of this context from an Issuance perspective:

Characteristics of the context	Virtual POI
Final amount known	Y
Authorisation	The (M)RP Application if present in the consumer device shall support Online Authorisation and in addition may support Offline Authorisation
Card Authentication	Static authentication for low risk payments (see [EBA]) Dynamic Authentication <sup>14</sup>
Risk-Based Authentication	Optional, but requires redirection to the Card issuer domain
Cardholder Verification Method	At least one of the following CVM shall be supported <ul style="list-style-type: none"> <li>Mobile Code (m-commerce) or Personal Code (e-commerce)</li> <li>PIN on additional authentication device (does not involve virtual POI)</li> </ul>

**Table 56:** Remote Transaction One-off Payment - Issuance Characteristics

#### 4.2.1.2. Card services

Service	Issuers	Schemes	Acquirers	Acceptors
<b>Payment</b>	Required	Required	Required	Required
<b>Cancellation</b>	Optional	Optional	Optional	Optional
<b>Refund</b>	Optional	Optional	Optional	Optional

**Table 57:** CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

<sup>14</sup> Any dynamic authentication in combination with a CVM will provide “Strong Customer Authentication” as defined in the EBA Guidelines for the Security of Internet Payments [EBA].

## 5. USE CASES

### 5.1. Card Transactions

#### 5.1.1. Introduction

In this section a number of use cases will be described to illustrate mobile contactless transactions. The following table provides an overview of the possible combinations for contactless transactions:

	No CVM	Online PIN	CDCVM
Online transaction	Card and Mobile Contactless	Card and Mobile Contactless	Mobile Contactless
Offline transaction	Card and Mobile Contactless <sup>15</sup>		Mobile Contactless

Below, some use cases are presented as diagrams with a description of the different steps involved. They map as follows into this table:

	No CVM	Online PIN	CDCVM
Online transaction	Use case 2	Use case 3	Use Case 5
Offline transaction	Use case 4		Use case 1

<sup>15</sup> With appropriate risk management in the MCP Application.

## 5.1.2. Mobile Contactless

### 5.1.2.1. Use case 1: Mobile Contactless - Single Tap - Offline transaction - Offline CVM

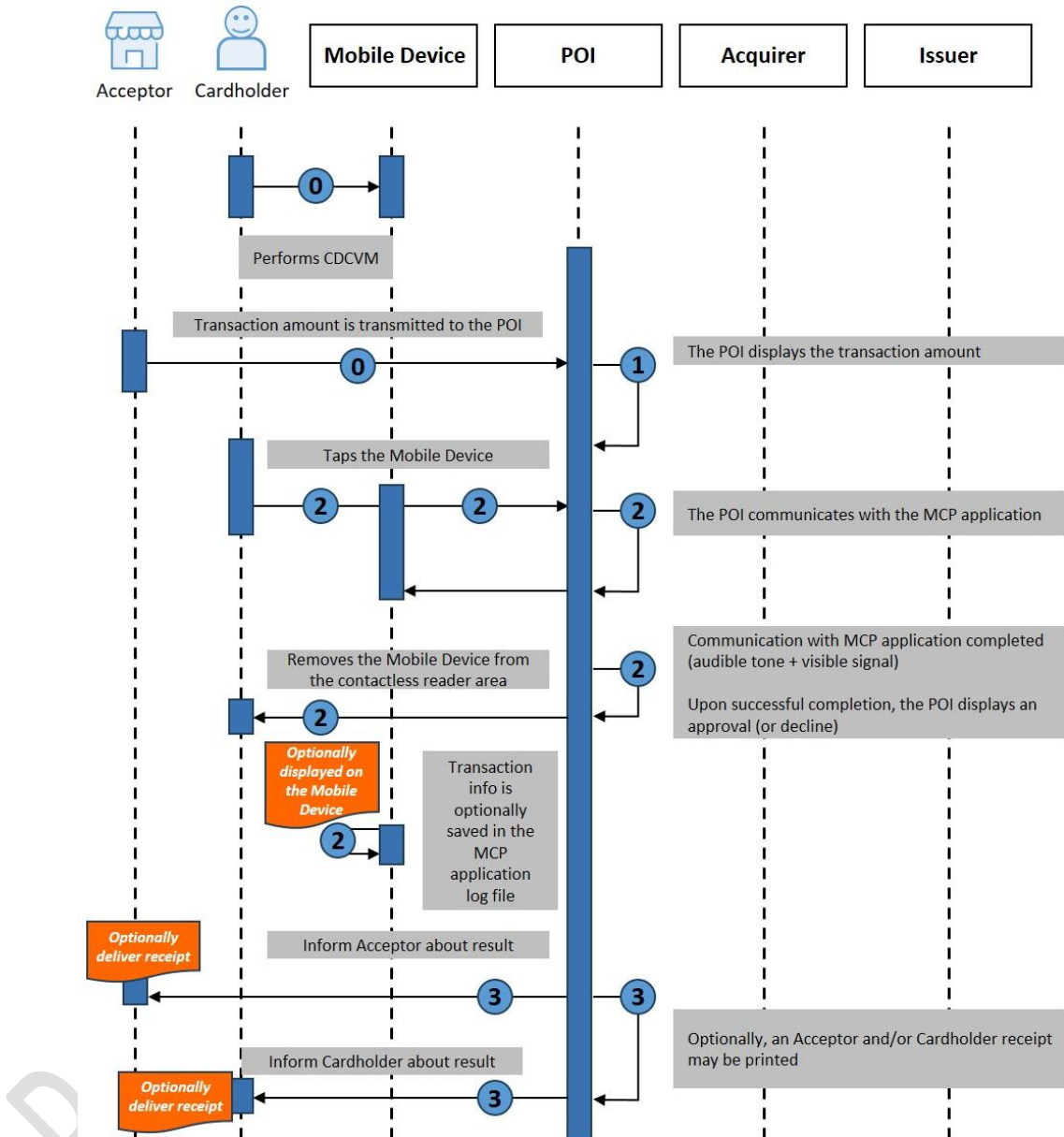


Figure 58: Single Tap - offline transaction - offline CVM

**Step 0 (Pre-requisite)**

- The Cardholder either selects a payment Card via a dedicated menu on their mobile device for the payment or the default payment Card (preselected on the Cardholder's mobile device) is automatically used for the payment.
- Cardholder is verified by the used CDCVM and the MCP Application is informed of the result.
- The transaction amount is transmitted to the POI.

**Step 1**

- The transaction amount is displayed on the POI.
- The POI requests to present a Card.

**Step 2**

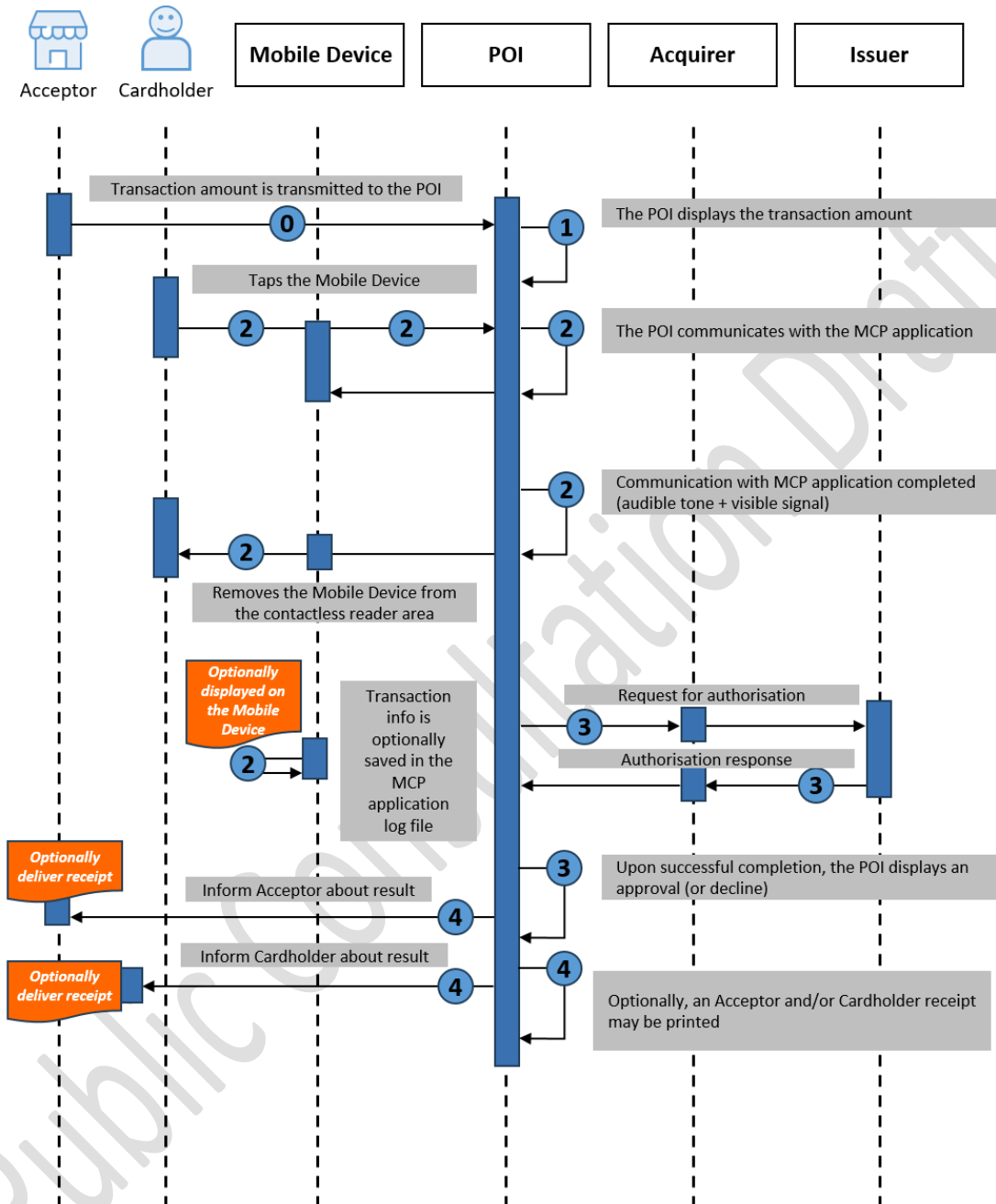
- The Cardholder taps their Mobile Device on the contactless reader area. (The Cardholder holds their Mobile Device close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application using the PPSE.
- The POI and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters.
- An audible tone and/or visible signal then indicate that the Mobile Device - POI interaction is completed. After this, subsequently, the Mobile Device may be removed from the contactless reader area.
- An offline Card authentication/ transaction authorisation is performed by the POI.
- After processing the offline authorisation, the POI displays an approval or decline.
- Information about the current transaction is optionally saved in the MCP Application log file.
- Information about the current transaction is optionally displayed on the Mobile Device.

**Step 3**

- The Acceptor is informed about the result of the transaction.
- The Cardholder is informed about the result of the transaction.
- An Acceptor and/or Cardholder receipt may be printed.

1205 5.1.2.2. Use case 2: Mobile contactless - Single Tap - Online transaction - no CVM

1206



1207 **Figure 59:** Single Tap - Online transaction - no CVM

1208



**Step 0 (Pre-requisite)**

- The Cardholder either selects a payment Card via a dedicated menu on their mobile device for the payment or the default payment Card (preselected on the Cardholder's mobile device) is automatically used for the payment.
- The transaction amount is transmitted to the POI.

**Step 1**

- The transaction amount is displayed on the POI.
- The POI requests to present a Card.

**Step 2**

- The Cardholder taps their Mobile Device on the contactless reader area. (The Cardholder holds their Mobile Device close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application using the PPSE.
- The POI and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined that no CVM is required.
- An audible tone and/or visible signal then indicate that the Mobile Device - POI interaction is completed. After this, subsequently, the Mobile Device may be removed from the contactless reader area.
- An offline Card authentication is optionally performed by the POI.
- An online Card authentication / transaction authorisation is performed by the POI.
- Information about the current transaction is optionally saved in the MCP Application log file.
- Information about the current transaction is optionally displayed on the Mobile Device.

**Step 3**

- After processing the online authorisation, the POI displays an approval or decline.

**Step 4**

- The Acceptor is informed about the result of the transaction.
- The Cardholder is informed about the result of the transaction.

1239

- An Acceptor and/or Cardholder receipt may be printed.

1240

1241

Public Consultation Draft

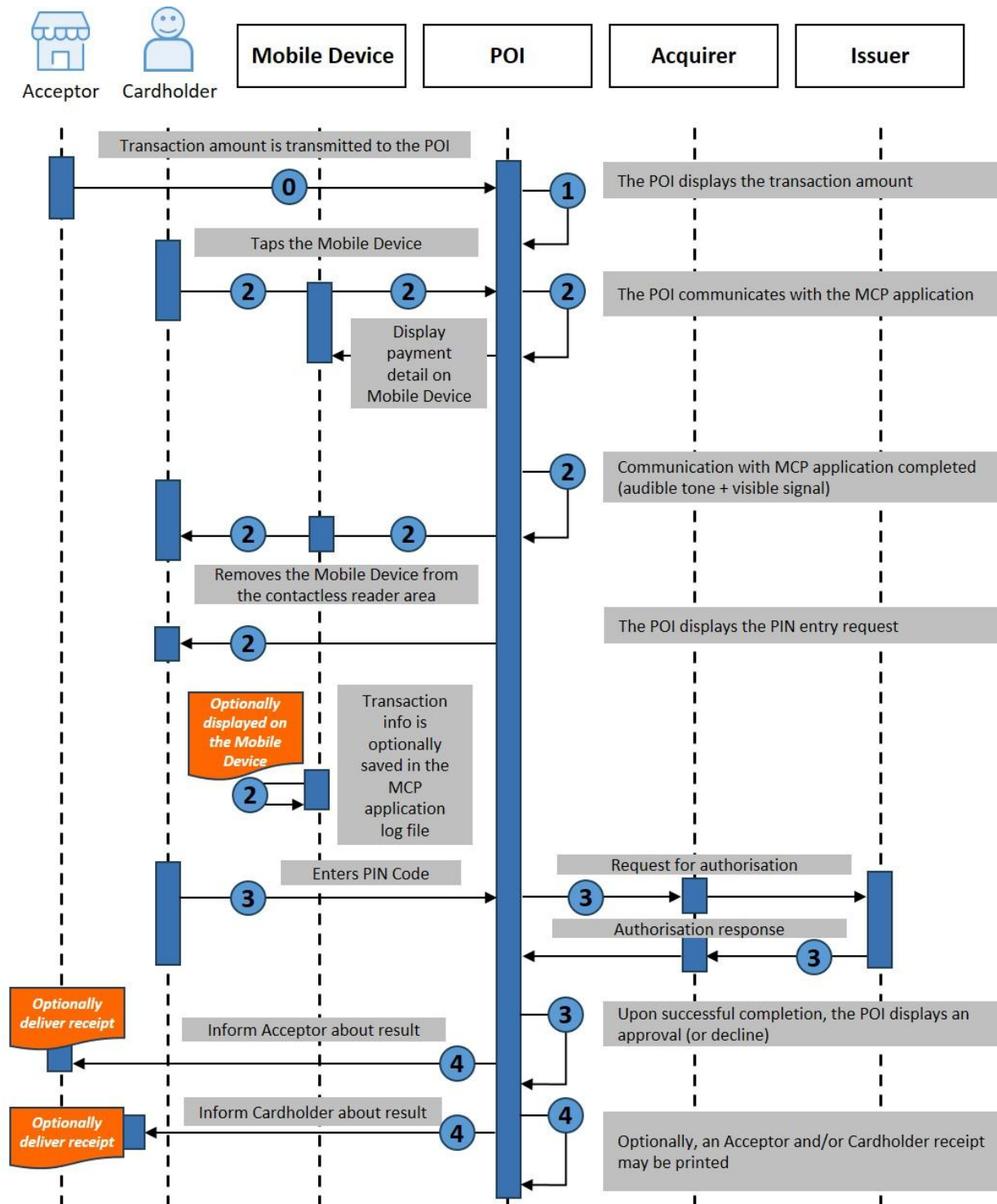
5.1.2.3. Use case 3: Mobile contactless - Single Tap - Online transaction - Online CVM


Figure 60: Single Tap - Online transaction - Online CVM

**1246      Step 0 (Pre-requisite)**

- 1247                      • The Cardholder either selects a pPayment Card via a dedicated menu on his/her Mobile  
1248                      Device for the payment or the default Payment Card (preselected on the Cardholder's  
1249                      Mobile Device) is automatically used for the payment.

- 1250                      • The transaction amount is transmitted to the POI.

**1251      Step 1**

- 1252                      • The transaction amount is displayed on the POI.

- 1253                      • The POI requests to present a Card.

**1254      Step 2**

- 1255                      • The Cardholder taps their Mobile Device on the contactless reader area. (The  
1256                      Cardholder holds their Mobile Device close to the contactless reader area until an  
1257                      audible tone and/or a visible signal takes place).

- 1258                      • The POI uses the contactless technology and selects the appropriate MCP Application  
1259                      using the PPSE. The contactless reader and MCP Application mutually determine  
1260                      appropriate processing for the transaction, including analysing and applying relevant  
1261                      risk management parameters. In this case, related to CVM, it is determined that an  
1262                      online CVM (PIN code on the POI) is required.

- 1263                      • An audible tone and/or visible signal then indicate that the Mobile Device - POI  
1264                      interaction is completed. After this, subsequently, the Mobile Device may be removed  
1265                      from the contactless reader area.

- 1266                      • A display message on the POI requests the Cardholder to enter their PIN code.

- 1267                      • An offline Card authentication is optionally performed by the POI.

- 1268                      • Information about the current transaction is optionally saved in the MCP Application  
1269                      log file.

- 1270                      • Information about the current transaction is optionally displayed on the Mobile Device.

**1271      Step 3**

- 1272                      • The Cardholder checks the purchase amount and enters their PIN code on the POI.

- 1273                      • An online Card authentication / transaction authorisation is performed by the POI.

- 1274                      • After processing the online authorisation, the POI displays an approval or decline.

1275

**Step 4**

- The Acceptor is informed about result of the transaction.
- The Cardholder is informed about result of the transaction.
- An Acceptor and/or Cardholder receipt may be printed.

Public Consultation Draft

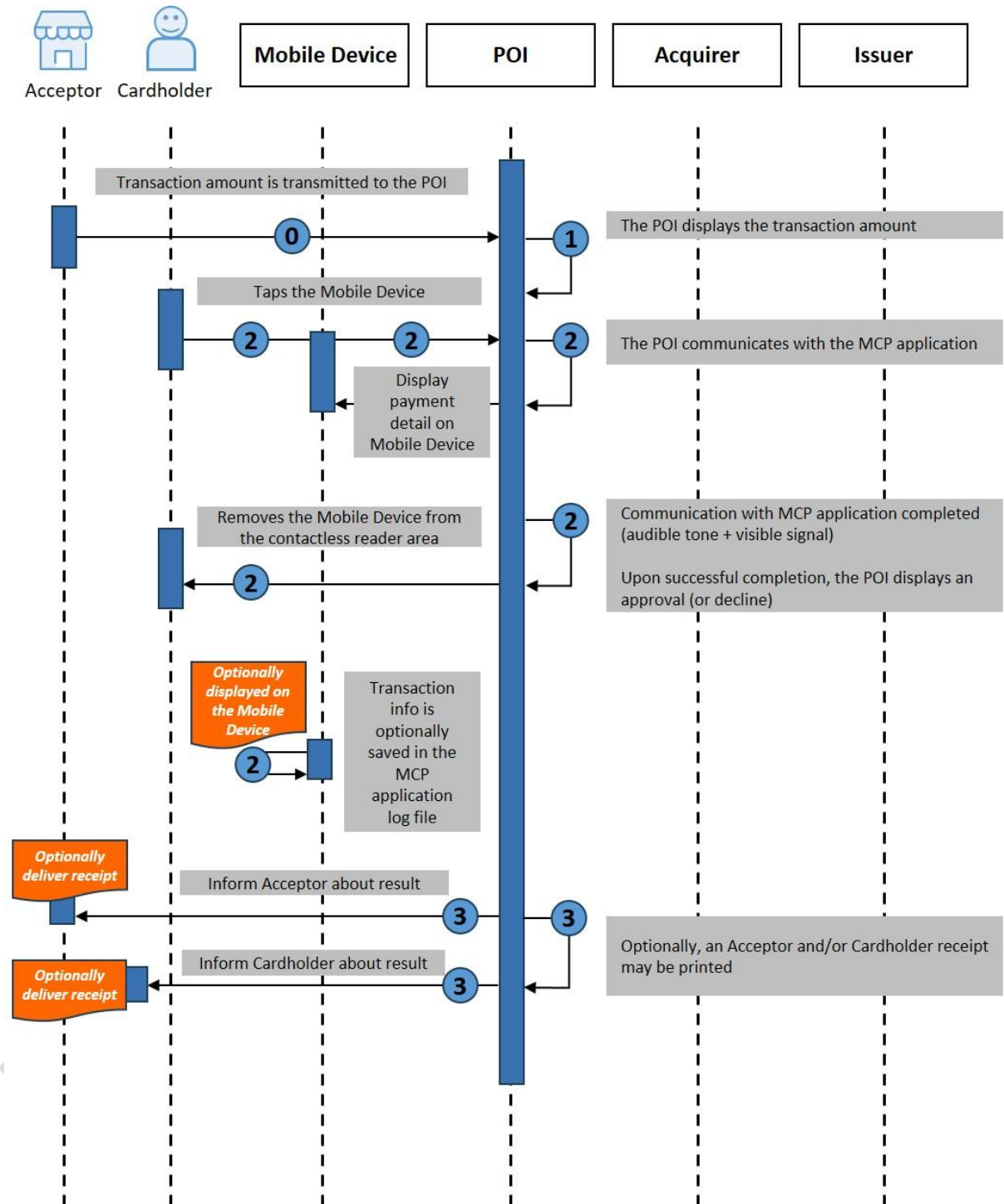
1280 5.1.2.4. Use case 4: Mobile Contactless - Single Tap - Offline transaction - no CVM


Figure 61: Single Tap - Offline transaction - no CVM

**Step 0 (Pre-requisite)**

- The Cardholder either selects a Payment Card via a dedicated menu on his/her Mobile Device for the payment or the default Payment Card (preselected on the Cardholder's Mobile Device) is automatically used for the payment.
- The transaction amount is transmitted to the POI.

**Step 1**

- The transaction amount is displayed on the POI.
- The POI requests to present a Card.

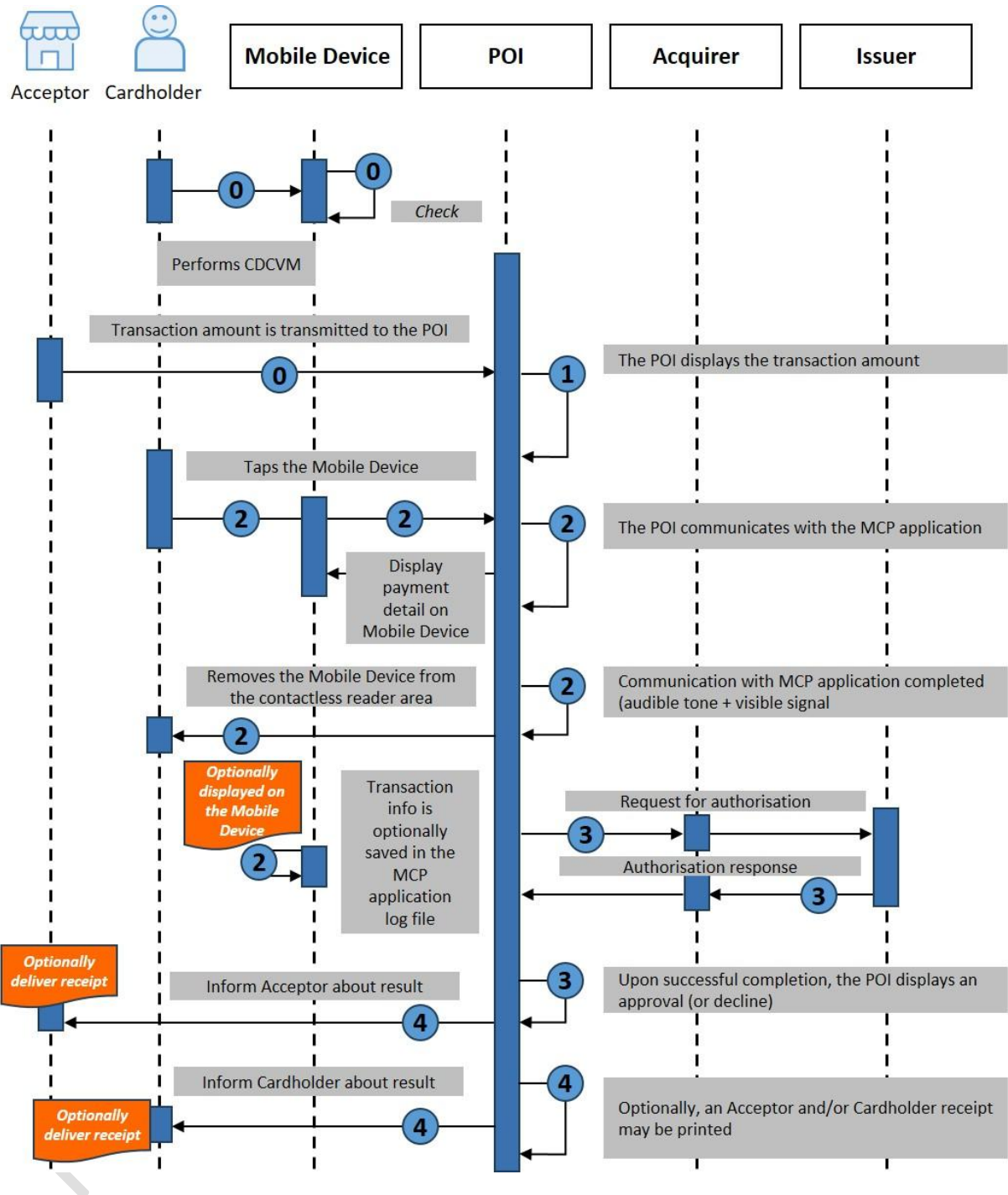
**Step 2**

- The Cardholder taps their Mobile Device on the contactless reader area. (The Cardholder holds their Mobile Device close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application using the PPSE. The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters.
- An audible tone and/or visible signal then indicate that the Mobile Device - POI interaction is completed. After this, subsequently, the Mobile Device may be removed from the contactless reader area.
- An offline Card authentication/ transaction authorisation is performed by the POI.
- After processing the offline authorisation, the POI displays an approval or decline.
- Information about the current transaction is optionally saved in the MCP Application log file.
- Information about the current transaction is optionally displayed on the Mobile Device.

**Step 3**

- The Acceptor is informed about the result of the transaction.
- The Cardholder is informed about the result of the transaction.
- An Acceptor and/or Cardholder receipt may be printed.

1314 5.1.2.5. Use case 5: Mobile contactless - Single Tap - Online transaction - CDCVM



1315

1316

1317

Figure 62: Single Tap - Online transaction - CDCVM



**Step 0 (Pre-requisite)**

- The Cardholder either selects a Payment Card via a dedicated menu on their Mobile Device for the payment or the default Payment Card (preselected on the Cardholder's Mobile Device) is automatically used for the payment.
- The Cardholder performs CDCVM which is verified by the MCP Application.
- The transaction amount is transmitted to the POI.

**Step 1**

- The transaction amount is displayed on the POI.
- The POI requests to present a Card.

**Step 2**

- The Cardholder taps their Mobile Device on the contactless reader area. (The Cardholder holds their Mobile Device close to the contactless reader area until an audible tone and/or a visible signal takes place).
- The POI uses the contactless technology and selects the appropriate MCP Application using the PPSE. The contactless reader and MCP Application mutually determine appropriate processing for the transaction, including analysing and applying relevant risk management parameters. In this case, related to CVM, it is determined by the MCP Application that an offline CDCVM is required and has been performed.
- An audible tone and/or visible signal then indicate that the Mobile Device - POI interaction is completed. After this, subsequently, the Mobile Device may be removed from the contactless reader area.
- An online Card authentication/ transaction authorisation is performed by the POI.
- After processing the online authorisation, the POI displays an approval or decline.
- Information about the current transaction is optionally saved in the MCP Application log file.
- Information about the current transaction is optionally displayed on the Mobile Device.

**Step 3**

- After processing the online authorisation, the POI displays an approval or decline.

**Step 4**

- The Acceptor is informed about the result of the transaction.

1348       • The Cardholder is informed about the result of the transaction.

1349       • An Acceptor and/or Cardholder receipt may be printed..

1350

1351       **5.1.3.    E and m commerce**

1352               5.1.3.1.    SCA-exempted e- & m-commerce with Static Authentication - No CVM

1353   In this scenario, illustrated in the figure below, the Customer uses their Consumer Device to  
1354   conduct a payment to an Acceptor, which is providing goods or services (e.g., mobile content). In  
1355   this scenario, no CVM method is used.

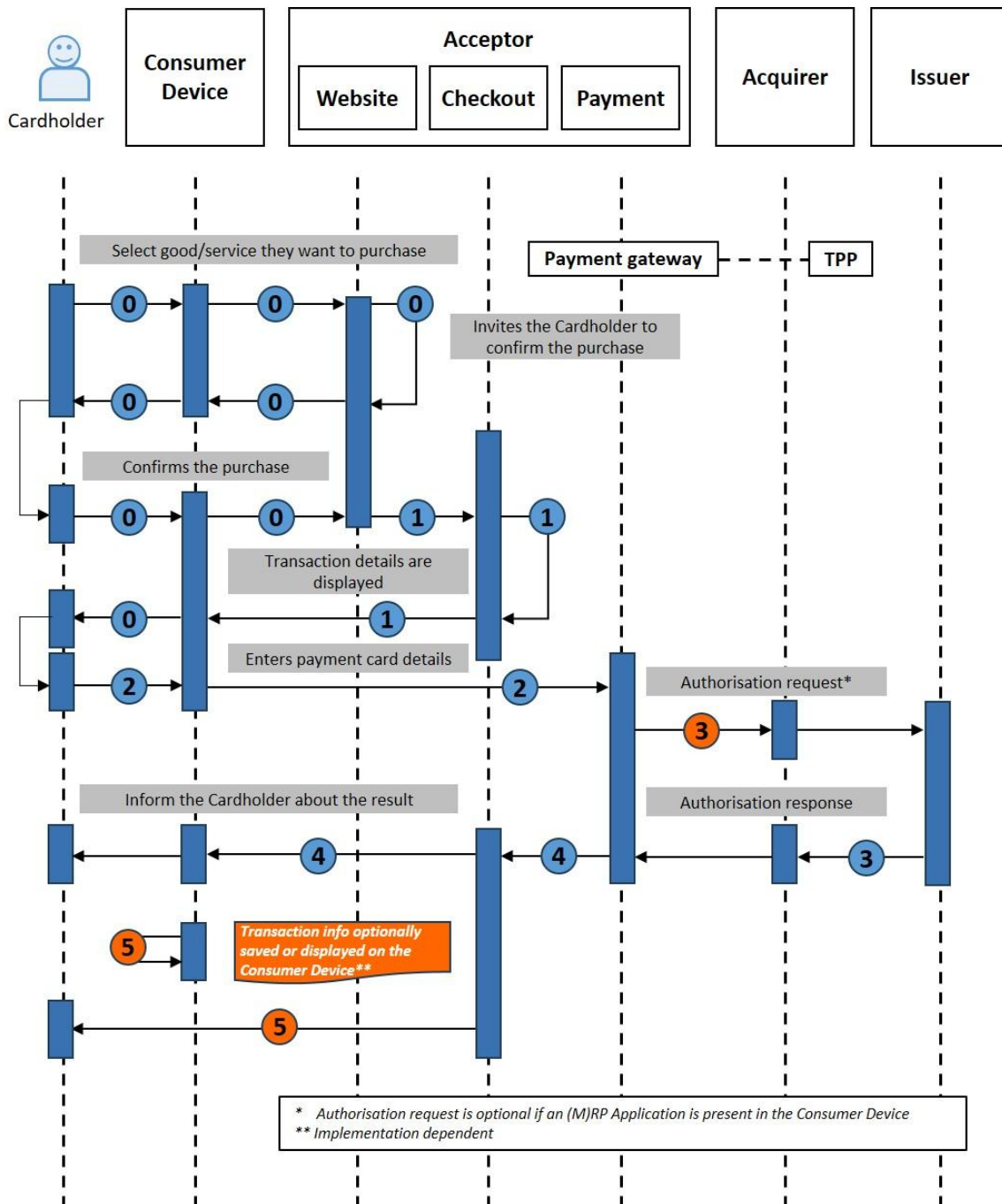


Figure 63: e- & m-commerce with Static Authentication- No CVM

In the figure above, the following steps are illustrated:

### Step 0 (Pre-requisite)

- The Cardholder navigates using their Consumer Device to an acceptor website via internet and selects the goods / service they wants to purchase.
- After having accepted the general purchase conditions, they are invited to confirm the purchase.

1364 **Step 1 (Transaction details displayed)**

- 1365       • The checkout section of the Acceptor website displays the transaction details including  
1366       the amount and the payment options, via the Consumer Device to the Cardholder.

1367 **Step 2 (Card payment selection)**

- 1368       • The Cardholder selects the "payment by Card" option via internet and is subsequently  
1369       redirected to the payment section under the control of a payment gateway to proceed  
1370       with the transaction under a secure http connection (https). The Cardholder is invited  
1371       to enter their Payment Card details (e.g., PAN, expiry date and CSC).
- 1372       • As an alternative to the entry of the Payment Card details by the Cardholder, there may  
1373       be an Application stored in, or accessed through, the Consumer Device. The Cardholder  
1374       is then redirected to the user interface of this Application to select the Payment Card to  
1375       be used and the Card details are automatically transferred to the payment section.
- 1376       • The transaction summary is displayed on the Consumer Device, typically including the  
1377       date, the Acceptor reference, the amount and the selected Payment Card whereby the  
1378       Cardholder is invited to confirm the transaction.

1379 **Step 3 (Payment process)**

- 1380       • The payment is processed as a Remote Card Transaction. This typically<sup>17</sup> involves an  
1381       online authorisation request by the Acceptor to the Issuer, at which time static  
1382       authentication occurs.

1383 **Step 4 (Transaction finalisation)**

1384 Once the payment is authorised,

- 1385       • The Cardholder is automatically redirected to the Acceptor website and receives a  
1386       confirmation of the transaction;
- 1387       • The acceptor releases the good / service to the Cardholder.

1388 **Step 5 (Transaction information)**

- 1389       • Transaction information (such as the transaction amount) may be saved in an (M)RP  
1390       Application log file and / or optionally displayed on the Consumer Device.
- 1391       • An electronic receipt may be made available by the Acceptor to the Cardholder.

---

<sup>17</sup> In particular cases, if an (M)RP Application is present in the Consumer Device, the authorisation request could be optional, depending on the type of Payment Card and the Acceptor's decision. But, in any case, the capability to do an authorisation request must be there.

### 5.1.3.2. e- and m-commerce with dynamic authentication

In this scenario, illustrated in the figure below, the Cardholder uses their Consumer Device to conduct a payment to an Acceptor, which is providing goods or services (e.g., mobile content). This scenario uses a "dynamic authentication method", i.e. a combination of Card authentication with a CVM.

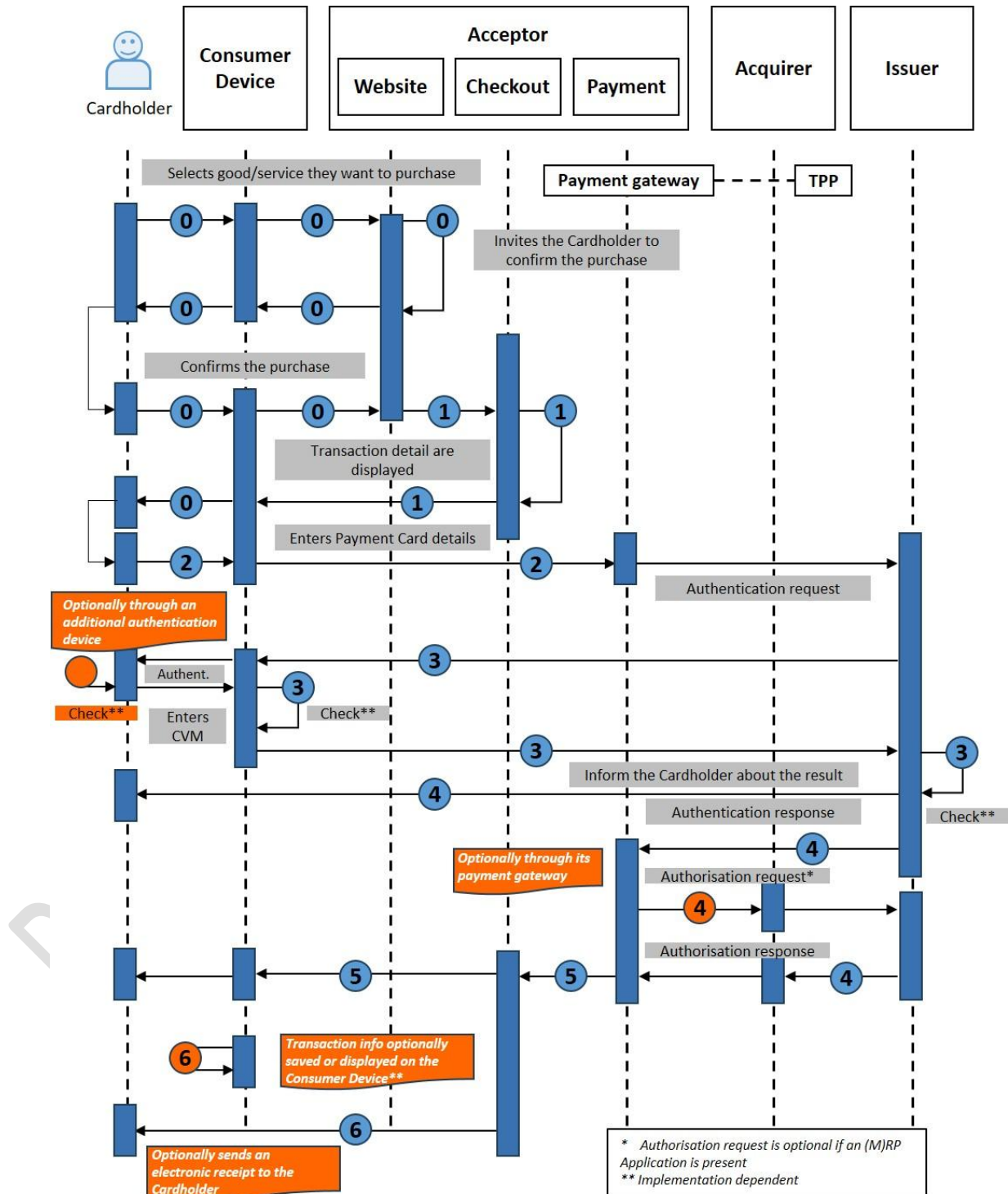


Figure 64: e- & m-commerce with dynamic authentication

1398 In the figure above, the following steps are illustrated:

1399 **Step 0 (Pre-requisite)**

- 1400 • The Cardholder navigates using their Consumer Device to an Acceptor website via  
1401 internet and selects the goods / service they wants to purchase.
- 1402 • After having accepted the general purchase conditions, the Cardholder is invited to  
1403 confirm the purchase.

1404 **Step 1 (Transaction details displayed)**

- 1405 • The checkout section of the Acceptor website displays the transaction details including  
1406 the amount and the payment options, via the Consumer Device to the Cardholder.

1407 **Step 2 (Card payment selection)**

- 1408 • The Cardholder selects the "payment by Card" option via internet and is subsequently  
1409 redirected to the payment section under the control of a payment gateway to proceed  
1410 with the transaction under a secure http connection (https). The Cardholder is invited  
1411 to enter their payment Card details (e.g., PAN, expiry date and CSC).
- 1412 • As an alternative to the entry of the Payment Card details by the Cardholder, there may  
1413 be an Application stored in, or accessed through, the Consumer Device. The Cardholder  
1414 is then redirected to the user interface of this Application to select the Payment Card to  
1415 be used and the Card details are automatically transferred to the payment section.
- 1416 • The transaction summary is displayed on the Consumer Device, typically including the  
1417 date, the Acceptor reference, the amount and the selected Payment Card whereby the  
1418 Cardholder is invited to confirm the transaction.

1419 **Step 3 (Authentication)**<sup>18</sup>

1420 The Cardholder and the relevant data are subsequently authenticated<sup>19</sup> by the Issuer<sup>20</sup> or their  
1421 agent according to one of the following typical processes:

- 1422 • In case an Authentication or (M)RP Application is present on the Consumer Device, a  
1423 dynamic authentication method (e.g., challenge/response method) is initiated by the  
1424 Issuer and is handled automatically by the authentication Application in a secure  
1425 environment. The Cardholder is also requested to enter their personal/mobile code  
1426 during the transaction process. The personal/mobile code is checked either locally by  
1427 the Authentication or (M)RP Application (CDCVM), or online by the Issuer.

---

<sup>18</sup> The usage of a CVM in combination with the dynamic authentication results into a Strong Customer Authentication.

<sup>19</sup> This authentication may involve transaction details.

<sup>20</sup> Or a TPP in the issuer domain.

- In case none of these applications is present on the Consumer Device, another Authentication Method (e.g., OTP and Online Personal Code) compliant to regulatory requirements is initiated by the Issuer or the Transaction is declined.

#### **Step 4 (Payment process)**

- The Cardholder is informed by their Issuer about the result of the authentication.
- The payment gateway is informed of the authentication result through the authentication response.
- The Acceptor is informed of the authentication result via the payment gateway .
- Subject to successful authentication by the Issuer, the payment is further processed as a Remote Card Transaction. This typically<sup>21</sup> involves an online authorisation request by the Acceptor to the Issuer.

#### **Step 5 (Transaction finalisation)**

Once the payment is authorised,

- The Cardholder is automatically redirected to the Acceptor website and receives a confirmation of the transaction;
- The Acceptor releases the good / service to the Cardholder.

#### **Step 6 (Transaction information)**

- Transaction information (such as the transaction amount) may be saved in an (M)RP Application log file and / or optionally displayed on the Consumer Device.
- An electronic receipt may be sent by the Acceptor to the Cardholder.

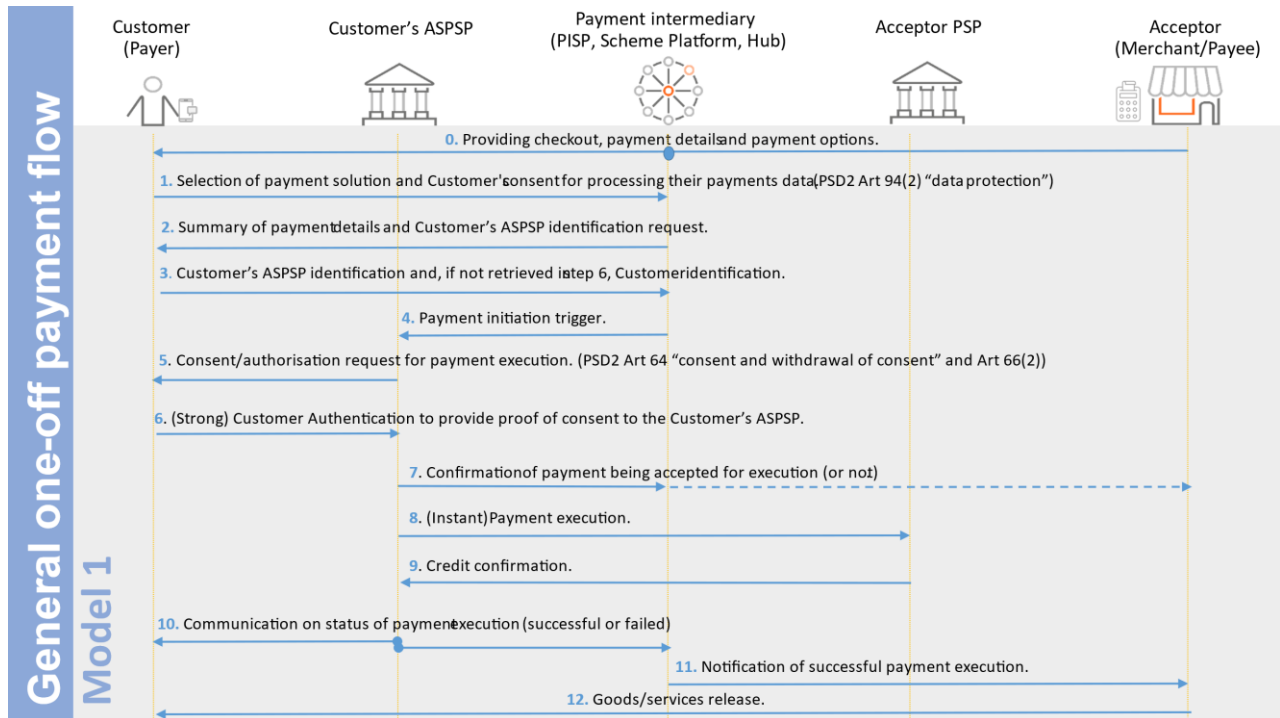
### **5.2. Instant Credit Transfer Transactions**

In this scenario, illustrated in the figure below, the Customer uses his/her Consumer Device with Instant Payment functionality to conduct a payment to an Acceptor, which is providing goods or services (e.g., mobile content) locally or remote.

---

<sup>21</sup> In particular cases, if an (M)RP Application is present in the Consumer Device, the authorisation request could be optional, depending on the type of Payment Card and the Acceptor's decision. But, in any case, the capability to do an authorisation request must be there.





In the figure above, the following steps are illustrated:

### **Step 0 (Checkout)**

- The Customer has selected the goods/service he/she wants to purchase in advance to this step
- The Acceptor provides a checkout option with payment details and options for the purchase of those goods/services to the Customer on a Physical or Virtual POI\* and, at the same time, to the Payment Intermediary.

*\*For Virtual POI, the information for the Customer may be provided through the Payment Intermediary.*

### **Step 1 (Selection of payment solution)**

- The Customer makes a selection of payment solution and provides consent for processing their payment data (In accordance with PSD2 art. 94(2) "data protection")

### **Step 2 (Payment details and identification request)**

- The Payment Intermediary provides the Customer with a payment details summary and sends a ASPSP customer identification request

### **Step 3 (Identification)**

- The Customer provides ASPSP identification and if relevant, customer identification, to the Payment Intermediary



1472 **Step 4 (Payment initiation)**

- 1473
  - A payment initiation trigger is sent to the Customer's ASPSP

1474 **Step 5 (Authorisation request)**

- 1475
  - The Customer's ASPSP provides the Customer with a consent/authorisation request for
- 1476 payment execution (In accordance with PSD2 art. 64 "consent and withdrawal of
- 1477 consent" and art. 66(2))

1478 **Step 6 (Proof of consent)**

- 1479
  - The Customer provides (Strong) Customer Authentication to the Customer's ASPSP to
- 1480 proof consent with the payment execution

1481 **Step 7 (Confirmation of payment execution approval)**

- 1482
  - The Customer's ASPSP provides the Payment Intermediary with confirmation of
- 1483 whether or not payment execution is accepted by the Customer. (If not, the payment is
- 1484 cancelled)
- 1485
  - Information of the result of the payment execution request is forwarded to the
- 1486 Acceptor

1487 **Step 8 (Payment execution)**

- 1488
  - Instant payment execution notification is sent from the Customer's ASPSP to the
- 1489 Acceptor PSP

1490 **Step 9 (Credit information)**

- 1491
  - The Customers credit information is provided by the Acceptor PSP to the Customer's
- 1492 ASPSP

1493 **Step 10 (Payment result)**

- 1494
  - The Customer's ASPSP communicates the payment execution result to both the
- 1495 Customer and the Payment Intermediary

1496 **Step 11 (Result notification)**

- 1497
  - The Payment Intermediary notifies the Acceptor of the payment execution result

1498 **Step 12 (Goods/Service release)**

- 1499
  - The Acceptor releases/hands over the goods/services to the Customer

## 6. FIGURES AND TABLES

FIGURE 1: SUMMARY OF EXAMPLE IMPLEMENTATIONS OF CHOICE OF THE APPLICATION WITHIN BOOK 6.....	9
FIGURE 2: EXAMPLE 1 (STEP 1): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE.....	10
FIGURE 3: EXAMPLE 1 (STEP 2): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE, INCLUDING THE SELECTED APPLICATION, TOTAL AMOUNT AND PIN ENTRY .....	10
FIGURE 4: EXAMPLE 2: CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - GRAPHICAL INTERFACE.....	11
FIGURE 5: EXAMPLE 3 (STEP 1): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE.....	12
FIGURE 6: EXAMPLE 3 (STEP 2): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE AFTER CARD INSERTION .....	12
FIGURE 7: EXAMPLE 4: CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE DURING THE EMV PROCESS - WITH THE TOTAL AMOUNT AND PIN ENTRY AS CVM .....	13
FIGURE 8: EXAMPLE 5 (STEP 1): CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE ON THE SAME SCREEN USING ARROWS .....	14
FIGURE 9: EXAMPLE 5 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING ARROWS .....	14
FIGURE 10: EXAMPLE 6 (STEP 1): CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE ON THE SAME SCREEN USING GRAPHICAL INTERFACE .....	15
FIGURE 11: EXAMPLE 6 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING GRAPHICAL INTERFACE.....	15
FIGURE 12: EXAMPLE 7: CONTACT & CONTACTLESS - ACCEPTOR PRE-SELECTION WITH OVERRIDE UP FRONT .....	17
FIGURE 13: EXAMPLE 10: REMOTE - CARDHOLDER SELECTION USING BRAND LOGOS.....	17
FIGURE 14: EXAMPLE 11 (STEP 1): REMOTE - CARD HOLDER ENTERS THEIR CARD DETAIL .....	18
FIGURE 15: EXAMPLE 11 (STEP 2): REMOTE - ACCEPTOR PRODUCT IDENTIFICATION.....	18
FIGURE 16: EXAMPLE 11 (STEP 3): REMOTE - THE CARDHOLDER EXERCISES THEIR OVERRIDE RIGHT .	19
FIGURE 17: EXAMPLE OF ACCESSIBLE PIN PAD DESIGNED FOR ENHANCED READABILITY .....	26
FIGURE 18: MODE 1.....	34
FIGURE 19: MODE 2.....	35
FIGURE 20: MODE 3.....	36
FIGURE 21: THE REDIRECT PROCESS.....	37
FIGURE 22: THE IFRAME .....	38
FIGURE 23: THE DIRECT POST .....	39

1537	FIGURE 24: JAVASCRIPT CREATED FORM.....	39
1538	FIGURE 25: THE API.....	40
1539	FIGURE 26: EXAMPLE OF ACCEPTOR STORAGE IN API INTEGRATION MODE.....	41
1540	FIGURE 27: EXAMPLE OF TPP STORAGE IN IFRAME INTEGRATION MODE.....	41
1541	FIGURE 28: EXAMPLE OF SHARED STORAGE IN DIRECT POST INTEGRATION MODE .....	42
1542	FIGURE 29: SRC CHECKOUT .....	43
1543	FIGURE 30: MERCHANT ORCHESTRATED CHECKOUT .....	44
1544	FIGURE 31: MERCHANT DIGITAL CARD-ON-FILE CHECKOUT .....	45
1545	TABLE 32: LOCAL TRANSACTION CONTACT PAYMENT - ACCEPTANCE CHARACTERISTICS.....	46
1546	TABLE 33: LOCAL TRANSACTION CONTACT PAYMENT - ISSUANCE CHARACTERISTICS .....	47
1547	FIGURE 34: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER	
1548	VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION	
1549	COMPLETION .....	48
1550	FIGURE 35: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER	
1551	VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.....	49
1552	FIGURE 36: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER	
1553	VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION	
1554	COMPLETION .....	50
1555	FIGURE 37: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER	
1556	VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN, CAPTURE BY BATCH .....	50
1557	FIGURE 38: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN UNATTENDED ENVIRONMENT, CARDHOLDER	
1558	PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION. ....	51
1559	FIGURE 39: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT,	
1560	CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.....	52
1561	TABLE 40: LOCAL TRANSACTION DEFERRED PAYMENT - ACCEPTANCE CHARACTERISTICS .....	53
1562	FIGURE 41: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE IMMEDIATELY AFTER TRANSACTION	
1563	COMPLETION .....	55
1564	FIGURE 42: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE BY BATCH.....	55
1565	TABLE 43: LOCAL TRANSACTION PRE-AUTHORISATION AND UPDATE PRE-AUTHORISATION SERVICE - ACCEPTANCE	
1566	CHARACTERISTICS.....	57
1567	TABLE 44: LOCAL TRANSACTION PAYMENT COMPLETION SERVICE - ACCEPTANCE CHARACTERISTICS.....	58
1568	FIGURE 45: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO	
1569	RESERVE AND SECURE AN AMOUNT, CARDHOLDER PRESENT: PRE-AUTHORISATION.....	60
1570	FIGURE 46: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO	
1571	RESERVE AN ESTIMATED AMOUNT: UPDATE PRE-AUTHORISATION.....	61
1572	FIGURE 47: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO	
1573	RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE IMMEDIATELY AFTER TRANSACTION	
1574	COMPLETION .....	61

1575	FIGURE 48: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO	
1576	RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE BY BATCH.....	62
1577	TABLE 49: LOCAL TRANSACTION CONTACTLESS PAYMENT - ACCEPTANCE CHARACTERISTICS .....	63
1578	TABLE 50: LOCAL TRANSACTION CONTACTLESS PAYMENT - ISSUANCE CHARACTERISTICS.....	63
1579	FIGURE 51: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION	
1580	METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL	
1581	AMOUNT KNOWN CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION .....	64
1582	FIGURE 52: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION	
1583	METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL	
1584	AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION .....	65
1585	FIGURE 53: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION	
1586	METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL	
1587	AMOUNT KNOWN. CAPTURE BY BATCH .....	65
1588	FIGURE 54: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION	
1589	METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL	
1590	AMOUNT KNOWN. CAPTURE BY BATCH .....	66
1591	TABLE 55: REMOTE TRANSACTION ONE-OFF PAYMENT - ACCEPTANCE CHARACTERISTICS .....	68
1592	TABLE 56: REMOTE TRANSACTION ONE-OFF PAYMENT - ISSUANCE CHARACTERISTICS .....	68
1593	TABLE 57: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS .....	68
1594	FIGURE 58: SINGLE TAP - OFFLINE TRANSACTION - OFFLINE CVM .....	70
1595	FIGURE 59: SINGLE TAP - ONLINE TRANSACTION - NO CVM.....	72
1596	FIGURE 60: SINGLE TAP - ONLINE TRANSACTION - ONLINE CVM.....	75
1597	FIGURE 61: SINGLE TAP - OFFLINE TRANSACTION - NO CVM .....	78
1598	FIGURE 62: SINGLE TAP - ONLINE TRANSACTION - CDCVM .....	80
1599	FIGURE 63: E- & M-COMMERCE WITH STATIC AUTHENTICATION- No CVM .....	83
1600	FIGURE 64: E- & M-COMMERCE WITH DYNAMIC AUTHENTICATION .....	85
1601		
1602		
1603		
1604		
1605		
1606		