SEPA CARDS STANDARDISATION (SCS) "VOLUME"

STANDARDS' REQUIREMENTS

BOOK 6

IMPLEMENTATION GUIDELINES

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

Abstract	This document contains the work on SEPA Cards standardisation to date
Document Reference	ECSG001-17
Issue	Book 6 - v8.6.00
Date of Version	1 March 2017
Reason for Issue	Publication
Reviewed by	Approved for publication by the ECSG Board of 9 February 2017
Produced by	ECSG Secretariat
Owned by	ECSG
Circulation	Public

Change History of Book 6		
6.6.0.x	2012-2013	Working version of Book 6
7.6.1.0	12.12.2013 (published 07.01.2014)	EPC Published version - Volume v7.0
7.6.1.0x	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

Table of Contents

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 Cards 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.

Book 6 also provides migration paths and timelines to assist with the aim of maintaining interoperability in the migration to full Volume conformance. Another objective of Book 6 is to phase out some implementations which create risks to SEPA for Cards implementations.

This document will provide:

- General Implementation Guidelines and options applicable to the Payment Contexts;

- Specific implementation Guidelines and Options for each Payment Context;

- Use cases for contactless as well as e and m commerce transaction scenarios;

- Time lines for all newly approved solutions to be conformant to the Volume;

- Sunset dates for the removal of non-Volume conforming functions and options.

The requirements per payment context are necessary because several implementations of the same service have evolved in the European markets. Consequently it has been agreed that all Card stakeholders shall harmonise on the Volume requirements. If several implementation options are possible 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 Payment Service:

- Local with:

  o Chip with Contact;

- o Chip and Mobile Contactless.

- Remote with:

    - o E and m-Commerce

    - o Mail Order Telephone Order

Deferred Payment Service:

- Local with:

    - o Chip with Contact;

Pre-Authorisation Service:

- Local with:

    - o Chip with Contact;

Additional contexts and use cases will be described in future versions of this document, including (for example) ATMs.

The creation and maintenance of implementation specifications are out of scope of this book.

1.1.2. Migration Roadmap

In addition to the 3 year conformance process after publication of the Volume as described in Book 1, Book 6 may allow or require alternative timelines for the implementation of a particular function, service or option. These timelines may also be applicable to Issuers, Acquirers and Schemes.

1.1.3. Structure of this book

The General implementation guidelines and options are defined in chapter 2 and specific payment contexts implementation guidelines are set out in chapter 3. Both sections include Volume conformant requirements and implementation options with selected roadmaps for implementing the options by a given date. Chapter 4 contains the description of a number of use cases to illustrate mobile contactless transactions.

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

1.2   Description of changes since the last version of Book 6

The following major changes have been made since the last version of Book 6:

- All descriptions of 'current implementation' information have been removed.

- Chapter 2: New implementation guidance on the Interchange Fee Regulation (as defined in articles 8.6 and 10.5) on priority selection and Choice of Application for local and Remote transactions and visual product identification of the product type have been added.

- Part of previous guidance have been integrated in Book 2 as requirements.

- Chapter 3: A new structure of chapter has been defined per Cardholder's environments and the payment contexts guidance are now presented in tables. Specific guidance is kept for completeness.

- Chapter4: A new chapter with five use cases for contactless, e and m-commerce transactions has been introduced.

2. GENERAL IMPLEMENTATION GUIDELINES

2.1. Introduction

This section describes implementation guidelines common to all contexts described in section 3.

2.2. Implementation guidance on 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:

Environ-ment	Acceptance Technology	Type Choice of Application with override		
		Choice by Cardholder without Acceptor 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	**Example 1:** Cardholder choice Text based interface (2.2.1.1.1) **Example 2:** Cardholder choice Graphical interface (2.2.1.1.2)	**Example 3:** Upfront Acceptor preferred Brand preselection with override after Card insertion (2.2.1.1.3)	**Example 4:** Acceptor preferred selection with override during the EMV process (2.2.1.1.4) **Example 5:** Acceptor preferred selection with override on the same screen using arrows during EMV process (2.2.1.1.5) **Example 6:** 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		**Example 7:** Acceptor Pre-selection with override up front (2.2.1.2.1)	
Local - Physical POI 2.2.1	Mobile Contactless (wallet) 2.2.1.3	**Example 8:** Cardholder choice prior to presenting the Mobile Device (2.2.1.3.1)	**Example 9:** Choice of Application with a Mobile Device supporting multiple Applications (2.2.1.3.2)	
Remote - Virtual POI 2.2.2	Manual Entry by Cardholder	**Example 10:** Cardholder selection using brand logos (2.2.2.1)		**Example 11:** 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

2.2.1. Local Transactions - Physical POI

2.2.1.1. *Contact - Choice by Cardholder without Acceptor Preference*

2.2.1.1.1. *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
```
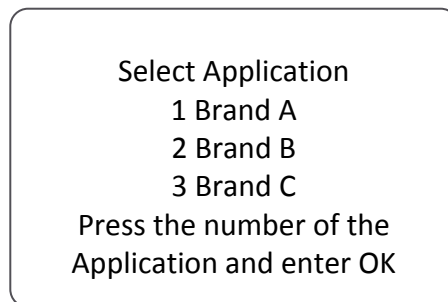
Figure 2: EXAMPLE 1 (STEP 1): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE

- Step 2:

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

```
Application      Brand B
EUR              100.00
Enter PIN          ****
          + OK
```
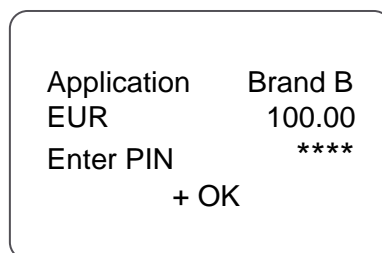
Figure 3: EXAMPLE 1 (STEP 2): CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - TEXT BASED INTERFACE, INCLUDING THE SELECTED APPLICATION, TOTAL AMOUNT AND PIN ENTRY

2.2.1.1.2. *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 to provide visual assistance to the Cardholder (see Figure 4).
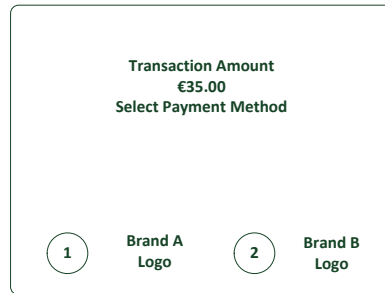
Figure 4: EXAMPLE 2: CONTACT - CHOICE BY CARDHOLDER WITHOUT ACCEPTOR PREFERENCE - GRAPHICAL INTERFACE

The Cardholder is then asked to enter their PIN and validate the transaction (see step 2 of example 1)

2.2.1.1.3. 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).

Brand A
Sale
€35.00
Insert Card
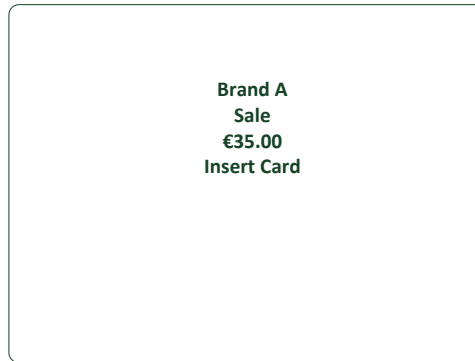
Figure 5: EXAMPLE 3 (STEP 1): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE

- Step 2:

On inserttion 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).

Brand A
Sale
€35.00
Enter PIN

○ **Press for other payment options**   **Display Brand Logos**
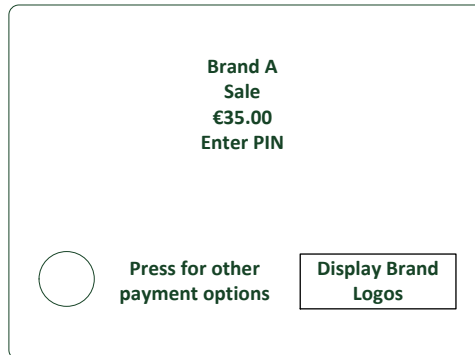
Figure 6: EXAMPLE 3 (STEP 2): CONTACT - UPFRONT ACCEPTOR PREFERRED BRAND PRESELECTION WITH OVERRIDE AFTER CARD INSERTION

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.

2.2.1.1.4. *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, which may include, if applicable;

- transaction amount,

- PIN entry.

```
      Pre-selected
       application
    Press 'Change Choice'
   button for different choice


        Enter OK
```
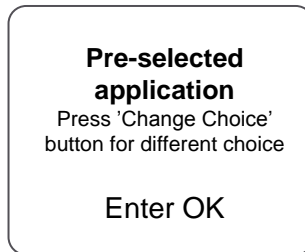
FIGURE 7: EXAMPLE 4: CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE DURING THE EMV PROCESS - WITH SIGNATURE AS CVM AND WITHOUT DISPLAYING THE FINAL AMOUNT[1]

```
      Pre-selected
       application
    Press 'Change Choice'
   button for different choice


     Total 100.00 EUR
     Enter PIN + OK
```
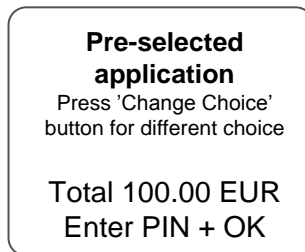
Figure 8: EXAMPLE 4: CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE DURING THE EMV PROCESS - WITH THE TOTAL AMOUNT AND PIN ENTRY AS CVM[2]

[1] 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] 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.

2.2.1.1.5. *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 9.

Brand A
Sale
€35.00
Enter PIN

Press arrows for more payment Brands.

Figure 9: 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, (see FIGURE 10) Once the Cardholder has confirmed the Application to be used for that transaction, normal EMV processing resumes.

Brand B
Sale
€35.00
Enter PIN

Press arrows for more payment Brands.

Figure 10: EXAMPLE 5 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING ARROWS

2.2.1.1.6. *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 11). At the same time it is made clear to the Cardholder other payment options are available, and how to access the other options. If the Cardholder accepts the Acceptor choice normal EMV processing resumes.
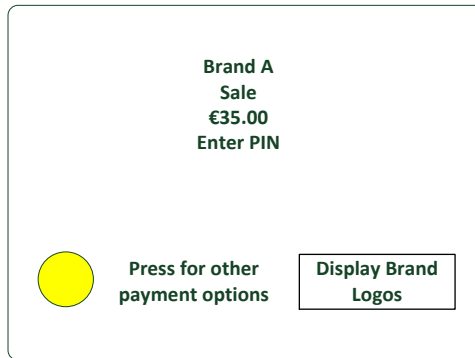
Figure 11: EXAMPLE 6 (STEP 1): CONTACT - ACCEPTOR PREFERRED SELECTION WITH OVERRIDE ON THE SAME SCREEN USING GRAPHICAL INTERFACE

If the Cardholder selects 'other payment options', all available Applications are listed (see Figure 12). The Acceptor may present their preferred Application first. On selection of the Cardholders preferred Application normal EMV processing resumes.
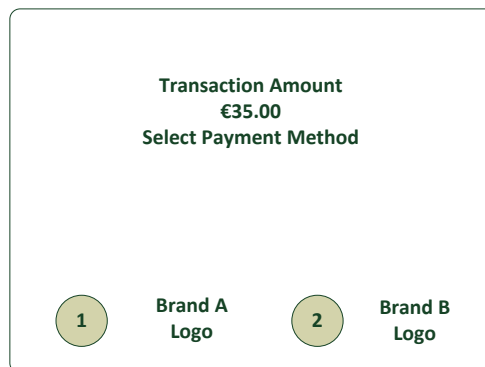
Figure 12: EXAMPLE 6 (STEP 2): CONTACT - CARDHOLDER SELECTION AFTER OVERRIDE USING GRAPHICAL INTERFACE

2.2.1.2.   *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

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

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

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

   b. After the Card has been read by the POI, either by presenting or inserting the Card, the POI will display to the Cardholder all Card Applications mutually supported by the Card and the POI.

      • 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 to start the payment process.

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

   a. They present or insert the Card

   b. After the Card has been read by the POI, the Acceptor's preferred Application is automatically selected

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

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

An example of the POI message using the yellow function keys button providing a Choice of Application to the Cardholder with an upfront selection screen is displayed in FIGURE 13.

> **Purchase**
> **Amount xxx.xx EUR**
> **Insert or Present**
> **card**
> Press 'Change Choice'
> button for Choice of
> Application
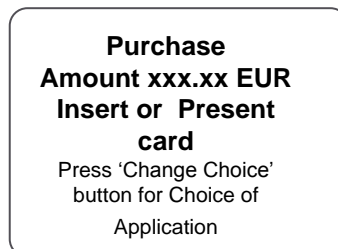
Figure 13: EXAMPLE 7: CONTACT & CONTACTLESS - ACCEPTOR PRE-SELECTION WITH OVERRIDE UP FRONT

If the Cardholder wishes to choose their preferred method of payment and selects the 'change choice' button then the Cardholder may:

- Insert the Card in the POI

All Card Applications mutually supported by the Card and the POI are presented to the Cardholder for them to select. The Acceptor's preferred Application may be the first Application in the list presented and/or may be highlighted.

After selection by the Cardholder, standard EMV payment process applies.

- Present the Card to the POI

All Card Applications mutually supported by the Card and the POI are presented to the Cardholder for them to select. The Acceptor's preferred Application may be the first Application in the list presented and/or may be highlighted.

An additional tap for the Choice of Application may be required, though the process is not described in the current release of the Volume.

After selection by the Cardholder, standard EMV payment process applies.

If the Cardholder does not wish to choose and therefore does not press the 'change choice' button, then the Cardholder may:

- Insert the Card in the POI

The Acceptor preferred Application is selected. The Cardholder may be asked to enter the PIN and confirm (PIN verification).

Standard EMV contact payment applies.

- Present the Card or Mobile Device to the POI

The Cardholder wants to "tap & go" (tap a Card, a mobile…). The Acceptor preferred Application is selected. The Cardholder may be asked to enter the PIN and confirm if the amount is above the CVM limit (online PIN verification).

Standard EMV contactless payment applies.

2.2.1.3. Local Mobile Contactless (wallet)

2.2.1.3.1. Example 8: Mobile Contactless - Cardholder choice prior to presenting the Mobile Device

To simplify the transaction process whilst using a mobile device, the Cardholder may choose their preferred co-badged Application prior to presenting their device for payment (see Figure 14), note that a Cardholder may have several wallets on the same payment device. Should the Cardholder choose their preferred Application in this way, the Acceptor's POI will be only be presented with a single Application and may automatically select it.
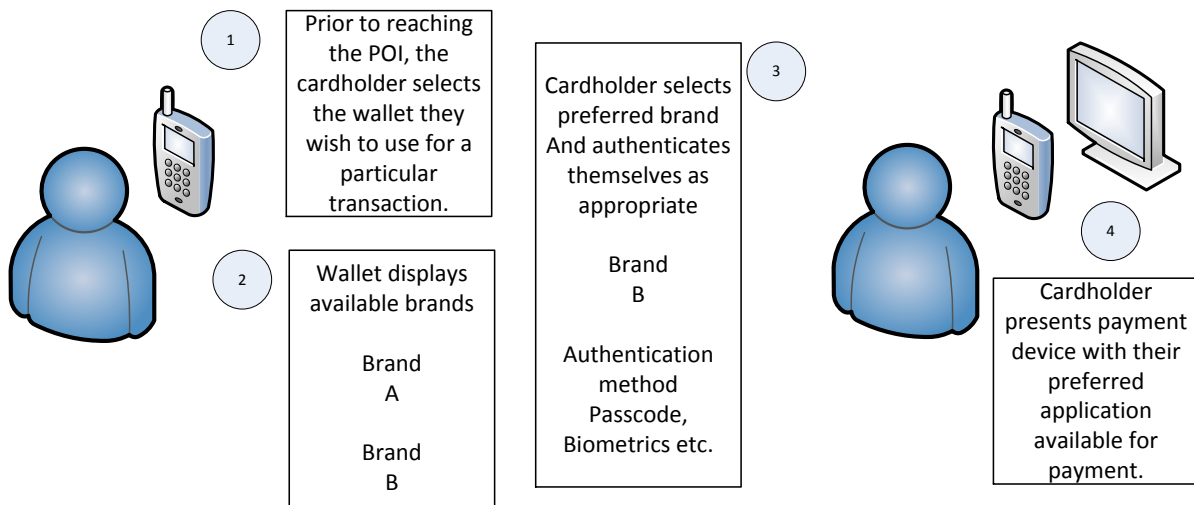

Figure 14: EXAMPLE 8: MOBILE CONTACTLESS - CARDHOLDER CHOICE PRIOR TO PRESENTING THE MOBILE DEVICE

2.2.1.3.2. Example 9: Mobile Contactless - Choice of Application with a Mobile Device supporting multiple Applications

A mobile device may return several co-badged Applications in the PPSE in which case, Choice of Application by the Acceptor and Cardholder is performed on the POI. The method of doing so is determined by the routine that the Acceptor has implemented, which may be one of the contactless implementation examples described above.
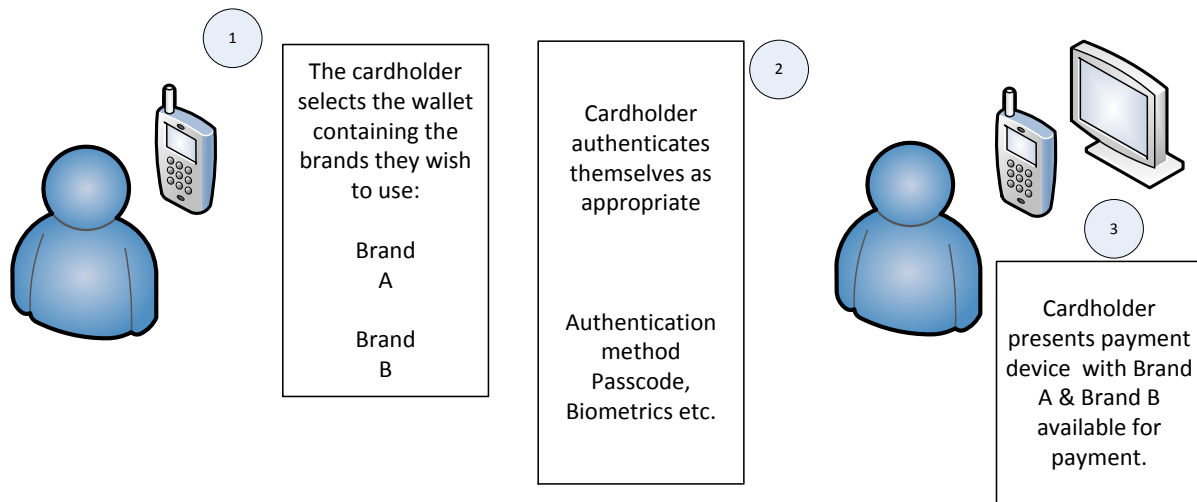
Figure 15: EXAMPLE 9: CONTACTLESS - CHOICE OF APPLICATION WITH A MOBILE DEVICE SUPPORTING MULTIPLE APPLICATIONS

2.2.2. 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

2.2.2.1 *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.

Payment method: ○ (Brand A)   ◉ (Brand B)   ○ (Brand C)

Card Number: [xxxx xxxx xxxx xxxx]

Expiry Date: [Month ∨] [Year ∨]

Card Security Code: [   ] ❓

Figure 16: EXAMPLE 10: REMOTE - CARDHOLDER SELECTION USING BRAND LOGOS

2.2.2.2 *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 (Brand A) (Brand B) (Brand C)

○ (Digital wallet A)

○ (Digital wallet B)

Card Number: [   ]

Expiry Date: [Month ∨] [Year ∨]

Card Security Code: [   ] ❓

Figure 17: 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.

Figure 18: EXAMPLE 11 (STEP 2): REMOTE - ACCEPTOR PRODUCT IDENTIFICATION

Step 3: the Cardholder exercises their override right

An option to change the Acceptor'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.

Figure 19: EXAMPLE 11 (STEP 3): REMOTE - THE CARDHOLDER EXERCISES THEIR OVERRIDE RIGHT

2.3. Implementation guidance on 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.

2.4. Implementation guidance on 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

- Debit

- Credit

- Commercial

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

2.5. Data Capture

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.

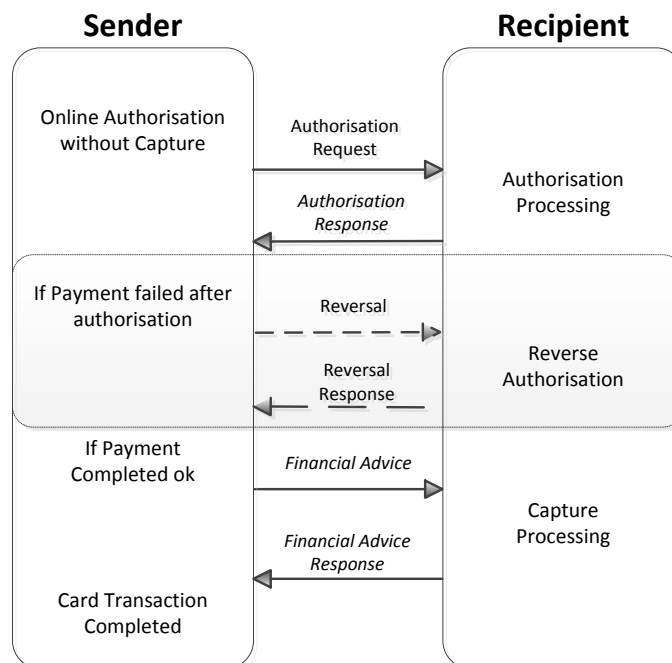# Mode 1: Online Authorisation, Capture immediately after Transaction Completion

FIGURE 20: MODE 1
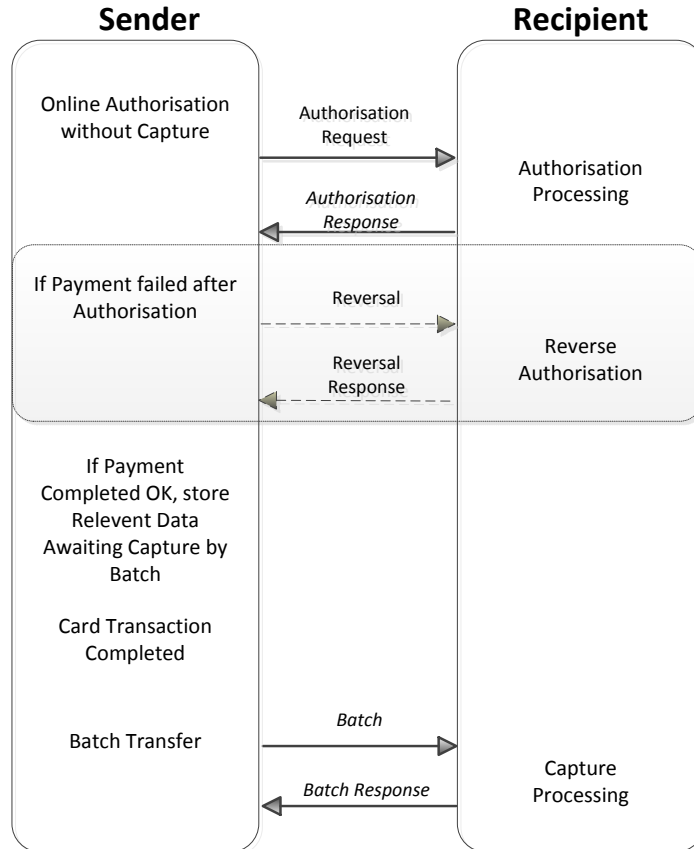
Mode 2: Online Authorisation, Capture by Batch

Sender		Recipient

Sender

Online Authorisation without Capture

Authorisation Request →

Authorisation Response ←

Recipient

Authorisation Processing

If Payment failed after Authorisation

Reversal ⇢

Reversal Response ⇠

Reverse Authorisation

If Payment Completed OK, store Relevent Data Awaiting Capture by Batch

Card Transaction Completed

Batch Transfer

Batch →

Batch Response ←

Capture Processing

FIGURE 21: MODE 2

Mode 3: Online Authorisation with Capture

Sender   **Recipient**

Online Authorisation with Capture	*Authorisation Request* →
	Authorisation and Capture Processing
	← *Authorisation Response*
If Payment failed after Authorisation	Reversal →
	Reverse Authorisation and Capture
	← Reversal Response
If Payment Completion OK, no further message exchange	
Card Transaction Completed	
Offine Authorised, Payment Completed ok	Financial Advice →
	Capture Processing
	← *Financial Advice Response*
Card Transaction Completed	

FIGURE 22: MODE 3

3. IMPLEMENTATION GUIDELINES PER PAYMENT CONTEXT

3.1. Local Transaction

3.1.1. Chip with Contact

3.1.1.1. *Payment*

3.1.1.1.1. *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.

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 The Physical POI shall either be offline with online capability or online only		
Data Capture	All 3 modes defined in section 2.5 are applicable		
Attendant Present	Y	N	
EMV Online Card Authentication.	Required		
EMV Offline Card Authentication	SDA optional from 2020[3] 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 23: Local Transaction Contact Payment - Acceptance Characteristics

---

[3] SDA is still required by some non SEPA general purpose Card schemes.

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	SDA not permitted for all newly issued and replacement Cards DDA and CDA required for all newly issued and replacement Cards	
Cardholder Verification Method	PIN mandatory	"No CVM Required" mandatory[4]

Table 24: Local Transaction Contact Payment - Issuance Characteristics

3.1.1.1.2. Card Services

For attended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required
Cancellation	Required	Required	Required	Optional
Refund	Required	Required	Required	Optional

Table 25: Card Services - Volume Conformant IMPLEMENTATIONS FOR ATTENDED

---

[4] 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.

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

<div align="center">Table 26: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR UNATTENDED</div>

3.1.1.1.3. *Example of Message Flows*

3.1.1.1.3.1. *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.
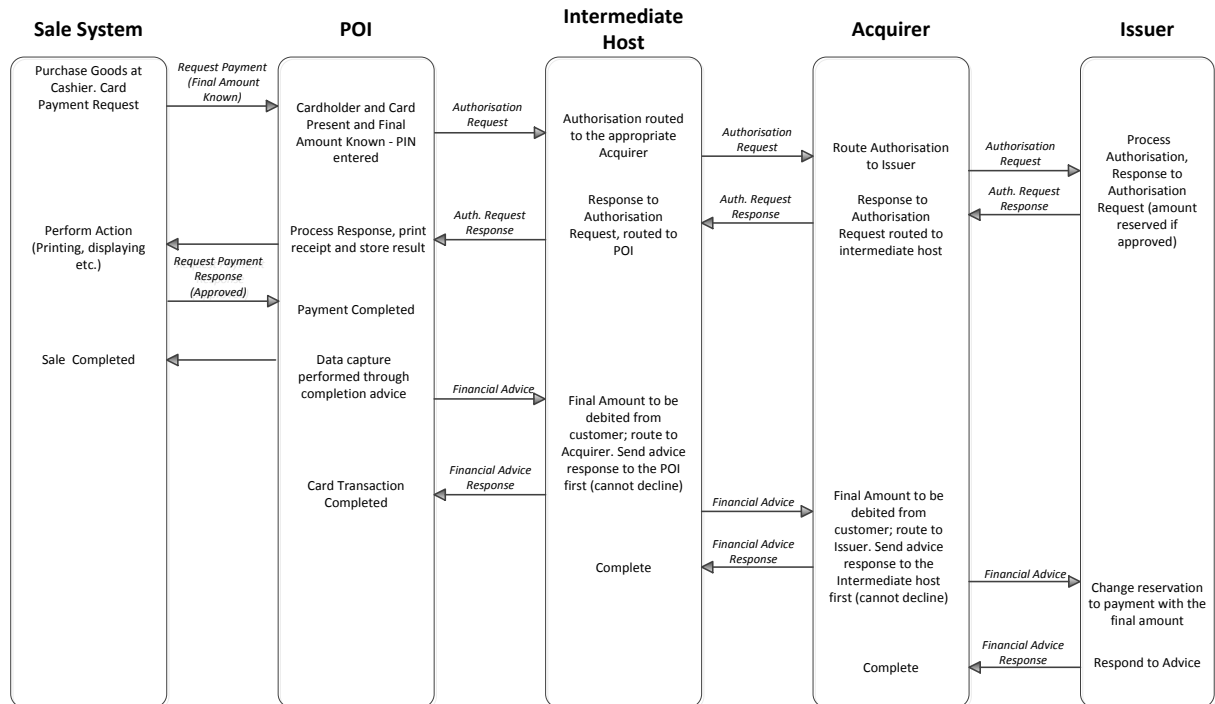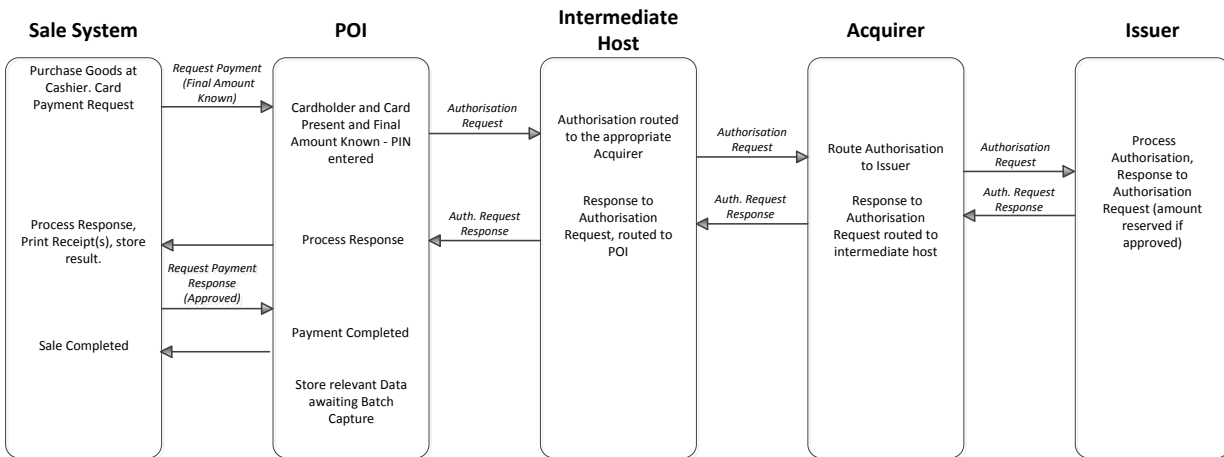

FIGURE 27: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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

FIGURE 28: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

3.1.1.1.3.2.   *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.
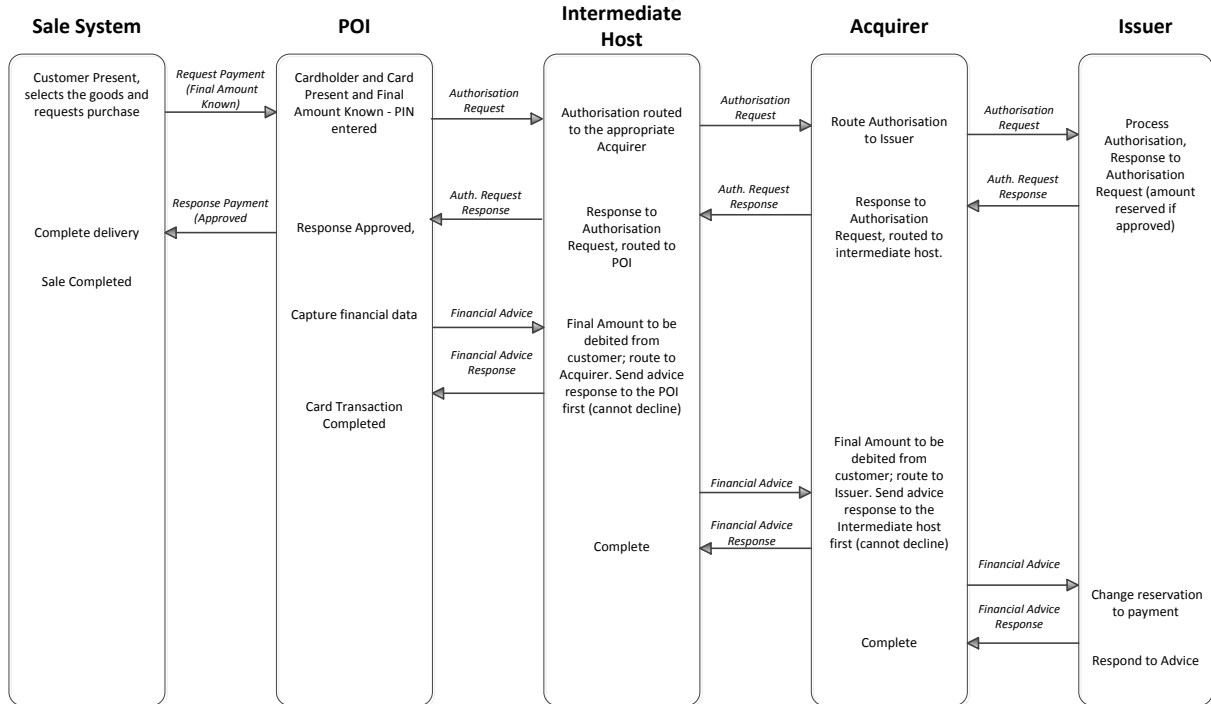
Payment in unattended environment, Cardholder is present, Cardholder Verification performed and final amount known, Capture by Batch
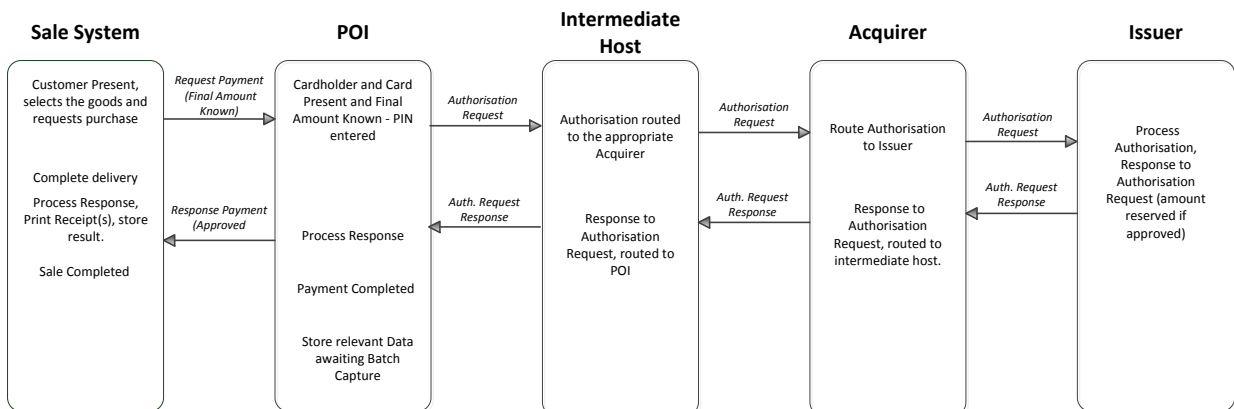

Figure 30: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN, CAPTURE BY BATCH

3.1.1.1.3.3. *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
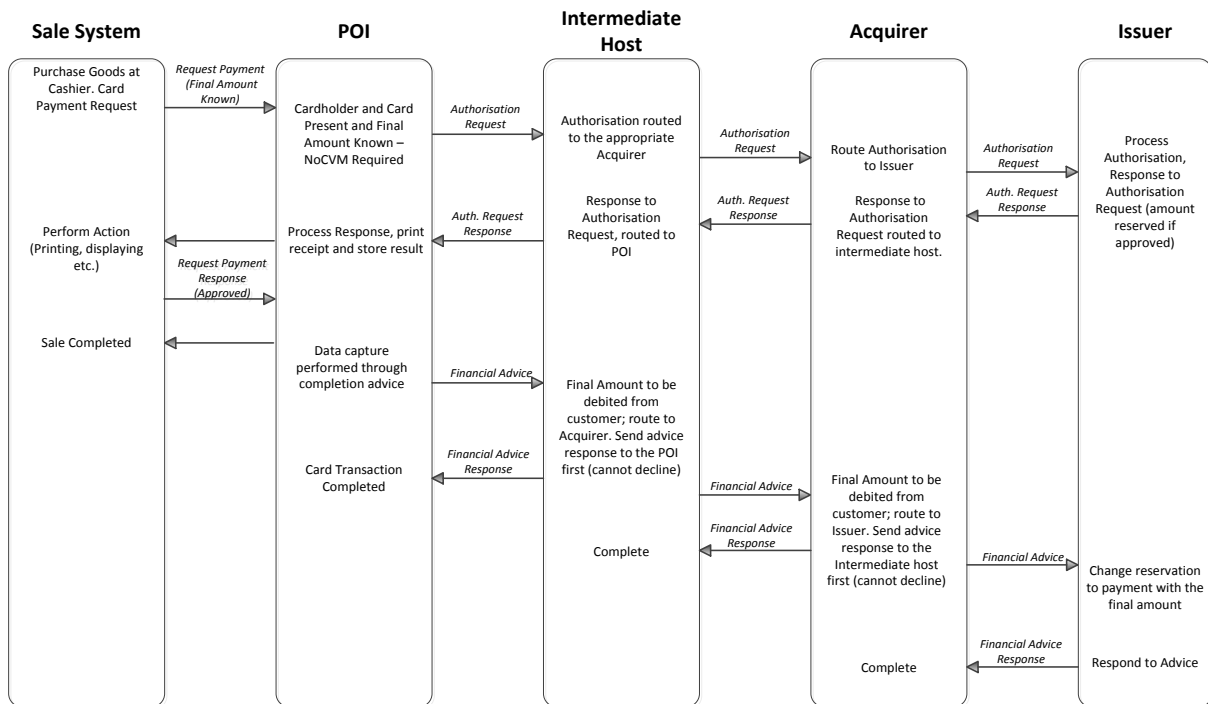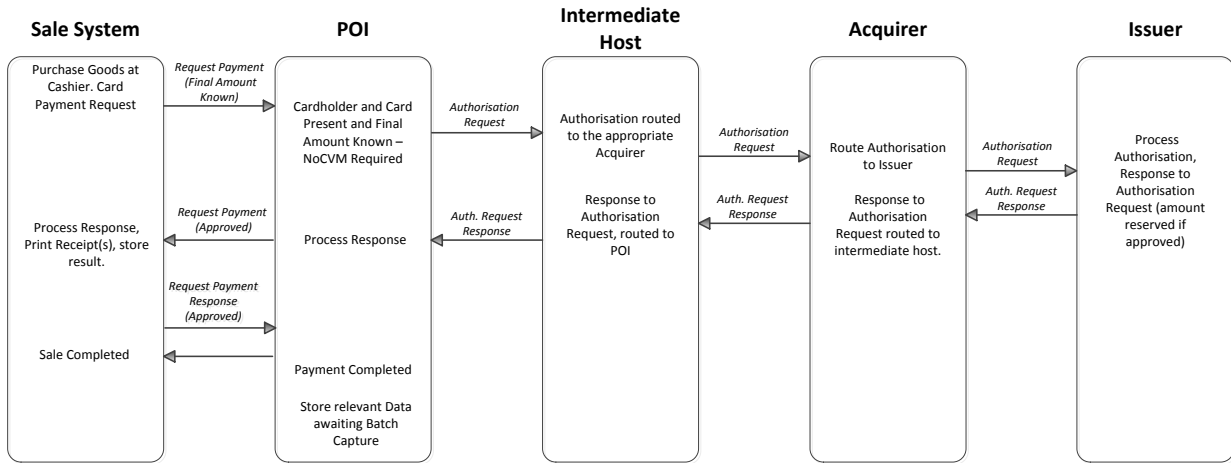

Figure 31: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION.

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

Figure 32: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

3.1.1.2. Deferred Payment

3.1.1.2.1. Definition of the payment context

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

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.

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 2.5 are applicable[5]		
Attendant Present	Y	N	
EMV Online Authentication.	Required		
EMV Offline Card Authentication	SDA optional from 2020[6] 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

Table 33: Local Transaction Deferred Payment - Acceptance Characteristics

---

[5] Mode 3 is not applicable as, at the time of Authorisation, the final amount is not known.

[6] SDA is still required by some non SEPA general purpose Card schemes

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

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

This service enables the acceptor to:

- Request an authorisation from the issuer to get a maximum amount available for the transaction where the amount requested may be chosen by the acceptor or Cardholder;

- Obtain a full approval, or a partial approval when the Cardholder has insufficient funds for the amount requested;

- Complete the delivery of goods or use of service to be paid up to the approved amount within a limited time frame (e.g., 20 minutes for petrol);

- Inform the issuer of the payment of these goods or services with the final amount that is less than or equal to the authorised amount in real time.

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

1) The amount that is requested to be authorised online is the maximum amount that may be required;

2) In order to avoid transactions being unnecessarily declined, Issuers shall support partial approval in responses when the "Cardholder Available Funds" is lower than the amount requested;

3) All parties in the protocol chain shall forward and/or act on on-line advice messages (or reversal), including zero amounts, so that the Cardholder Available Funds shall be adjusted in real time. If additional messages (e.g., batch clearing messages) are received, they shall be correctly handled".

3.1.1.2.2. *Card Services*

For attended and unattended environments:

Service	Issuers	Schemes	Acquirers	Acceptors
Deferred Payment	Required			
Deferred Payment with Partial Approval	Required	Required	Required	Required

Table 34: PAYMENT SERVICES - VOLUME CONFORMANT IMPLEMENTATION

3.1.1.2.3. *Example of Message Flows*

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.

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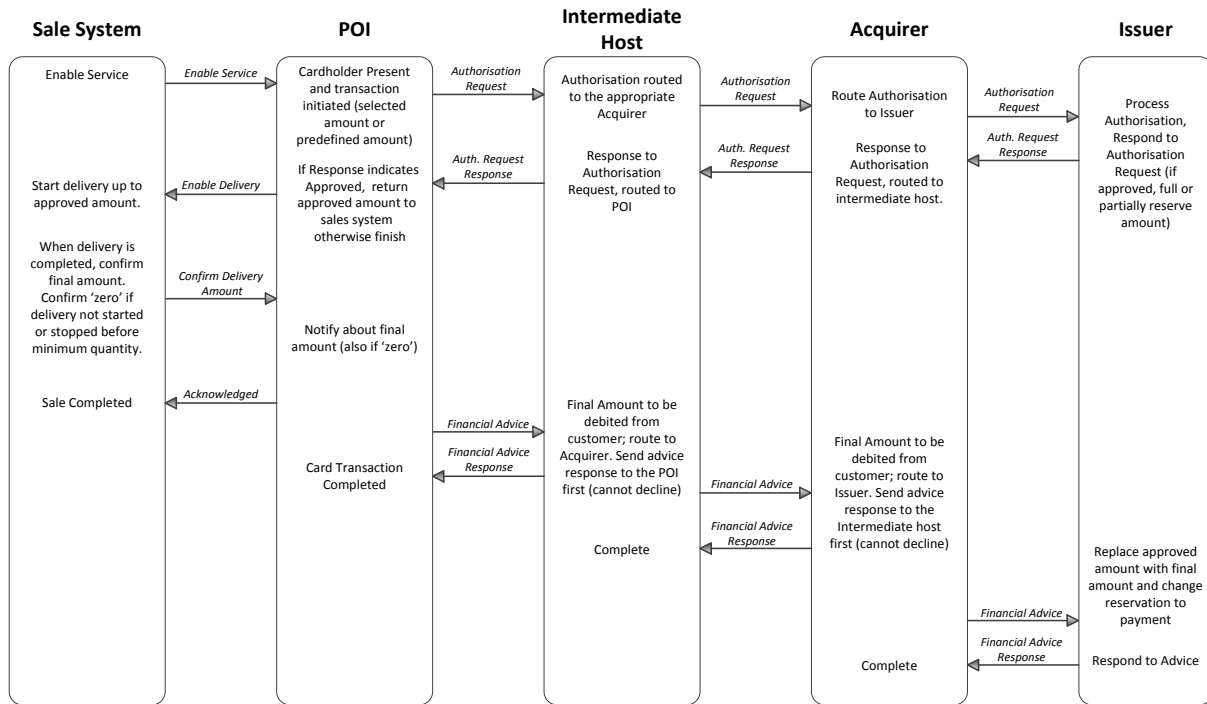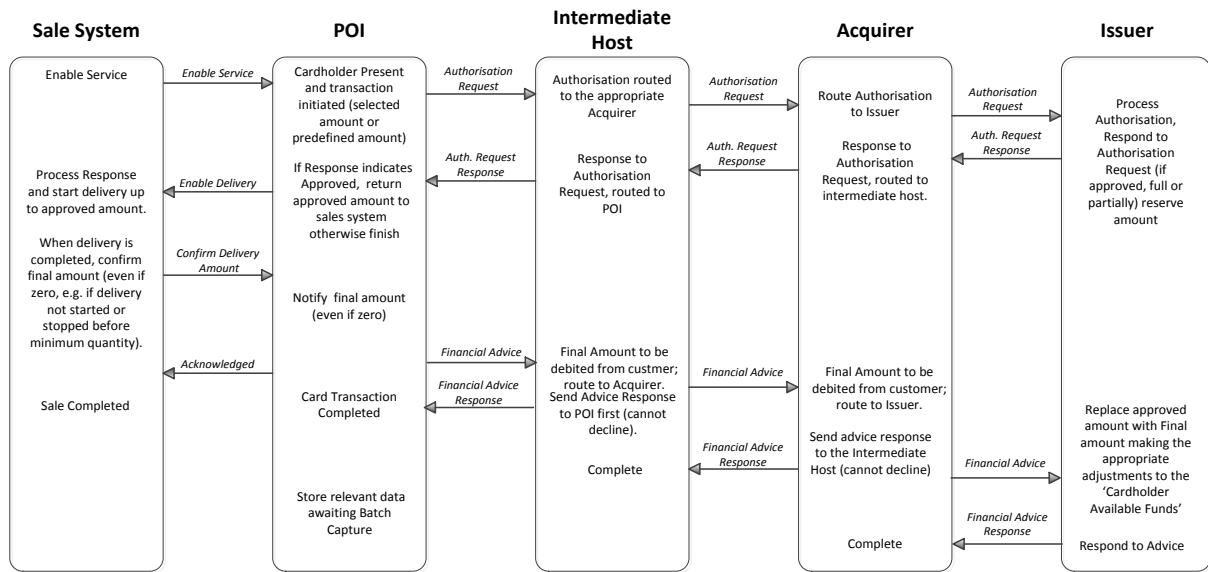

FIGURE 35: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

Deferred Payment Card Message Flow, Capture by Batch.

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

FIGURE 36: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE BY BATCH

3.1.1.3.   Pre-Authorisation Services

3.1.1.3.1.   Definition of the payment context

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

- The Acceptor to reserve an estimated amount until the final amount is known.

- The Issuer to more efficiently manage the Cardholder Available Funds in real-time, by either reserving or releasing funds.

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

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

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

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

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

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

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	
Attendant Present	Y	N
EMV Online Card Authentication.	Required	
EMV Offline Card Authentication	SDA optional from 2020[7] Offline with Online capability POI: DDA and CDA required Online only POI: DDA and CDA optional (recommended)	
Cardholder Verification Method	PIN Mandatory	PIN Mandatory

Table 37: Local Transaction Pre-Authorisation and Update Pre-Authorisation Service - Acceptance Characteristics

---

[7] 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 2.5 are applicable[8]	
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 38: 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)[9] to increase or decrease the pre-authorised amount if, prior to completion, the pre-authorised amount;

  o Is insufficient to cover the estimated final amount.

  o Is more than that required to cover the estimated final amount, to reduce the reserved amount(s) including, if necessary, to zero.

  o Exceeds the configured overspend percentage amount allowed by some scheme rules.

- Payment completion for an equal or lesser amount than the amount previously Authorised when the final amount is known or for a greater amount provided it is within the configured overspend percentage amount allowed by the appropriate scheme rules

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). The accumulated authorised amount(s) can only be exceeded by a configurable overspend percentage, if allowed by scheme rules.

---

[8] If Authorisation is used for Payment Completion, Mode 3 may also be used for Data Capture.

[9] Multiple update Pre-Authorisation(s) may be used in this scenario.

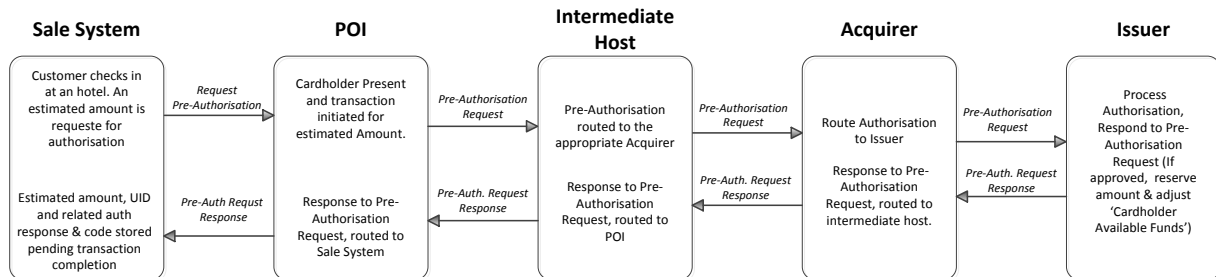The following Card services are supported for this context:

Service	Issuers	Schemes	Acquirers	Acceptors
Pre-Authorisation	Required 01/2021	Required 01/2021	Required 01/2021	Required 01/2021
Update Pre-Authorisation	Required 01/2021	Required 01/2021	Required 01/2021	Optional
Cancellation	Required 01/2021	Required 01/2021	Required 01/2021	Optional
Payment Completion	Required 01/2021	Required 01/2021	Required 01/2021	Required 01/2021

Table 39: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

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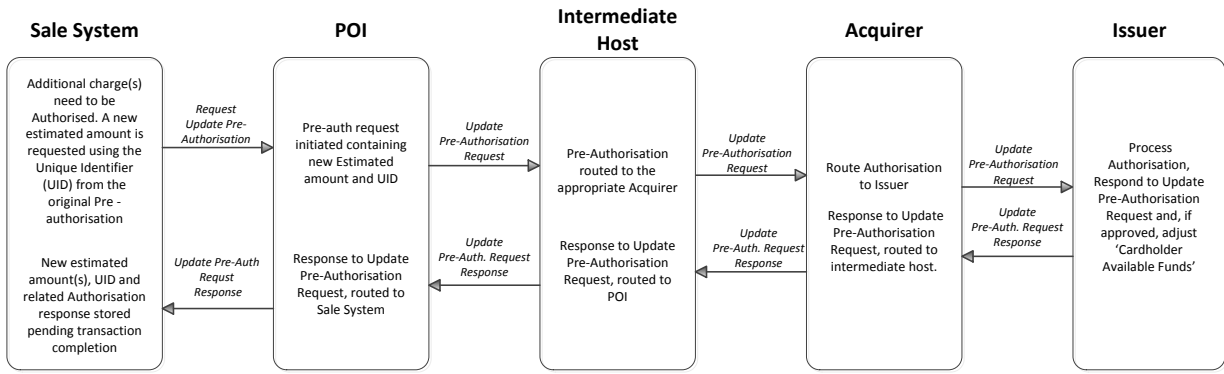
Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount, cardholder present: Pre-Authorisation

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

Figure 40: 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
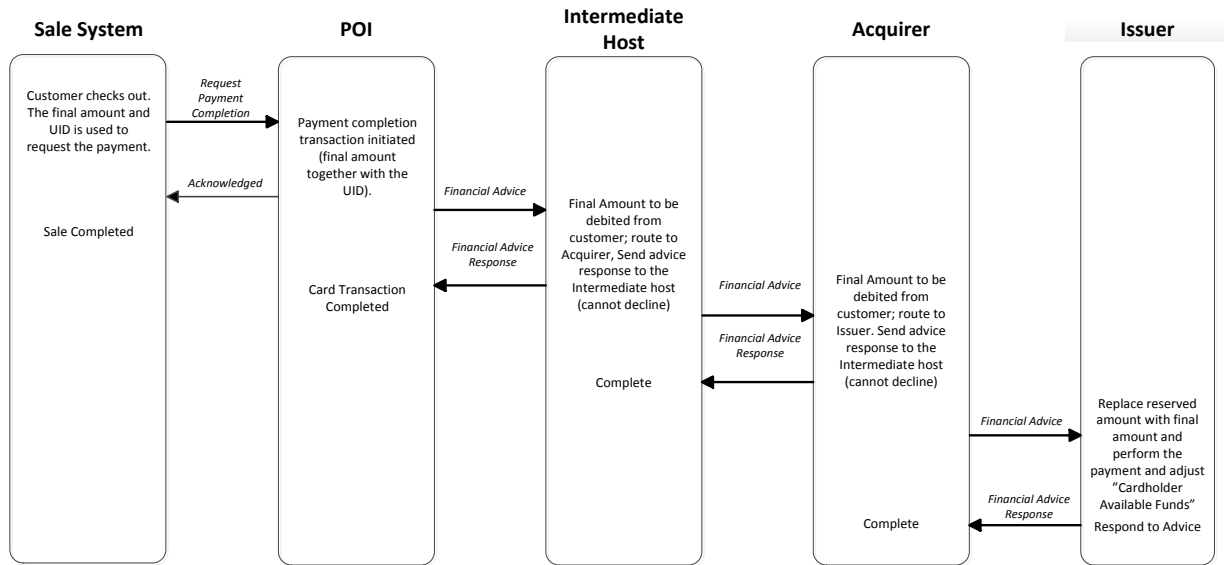
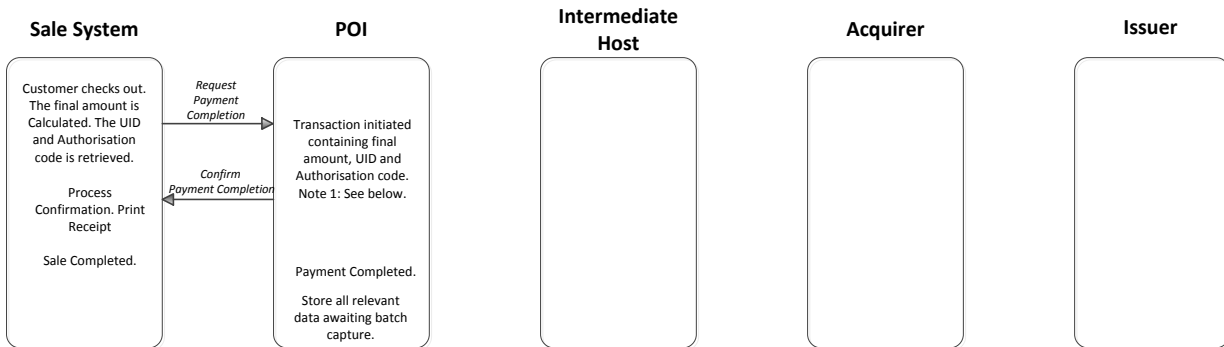| Sale System	POI	Intermediate Host	Acquirer	Issuer
Additional charge(s) need to be Authorised. A new estimated amount is requested using the Unique Identifier (UID) from the original Pre-authorisation	Pre-auth request initiated containing new Estimated amount and UID	Pre-Authorisation routed to the appropriate Acquirer	Route Authorisation to Issuer	Process Authorisation, Respond to Update Pre-Authorisation Request and, if approved, adjust 'Cardholder Available Funds'
New estimated amount(s), UID and related Authorisation response stored pending transaction completion	Response to Update Pre-Authorisation Request, routed to Sale System	Response to Update Pre-Authorisation Request, routed to POI	Response to Update Pre-Authorisation Request, routed to intermediate host.	

Request Update Pre-Authorisation / *Update Pre-Authorisation Request* / *Update Pre-Authorisation Request* / *Update Pre-Authorisation Request*

Update Pre-Auth Requst Response / *Update Pre-Auth. Request Response* / *Update Pre-Auth. Request Response* / *Update Pre-Auth. Request Response*

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

No Data Capture

Figure 41: 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.

Sale System	POI	Intermediate Host	Acquirer	Issuer
Customer checks out. The final amount and UID is used to request the payment.	Payment completion transaction initiated (final amount together with the UID).	Final Amount to be debited from customer; route to Acquirer, Send advice response to the Intermediate host (cannot decline)	Final Amount to be debited from customer; route to Issuer. Send advice response to the Intermediate host (cannot decline)	Replace reserved amount with final amount and perform the payment and adjust "Cardholder Available Funds"
Sale Completed	Card Transaction Completed	Complete	Complete	Respond to Advice

Request Payment Completion / *Acknowledged* / *Financial Advice* / *Financial Advice Response* / *Financial Advice* / *Financial Advice Response* / *Financial Advice* / *Financial Advice Response*

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

Figure 42: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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

| Sale System | POI | Intermediate Host | Acquirer | Issuer |

Customer checks out. The final amount is Calculated. The UID and Authorisation code is retrieved.

Request Payment Completion

Transaction initiated containing final amount, UID and Authorisation code. Note 1: See below.

Confirm Payment Completion

Process Confirmation. Print Receipt

Sale Completed.

Payment Completed.

Store all relevant data awaiting batch capture.

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'

Figure 43: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE BY BATCH

3.1.2. Chip and Mobile Contactless Payment

3.1.2.1. Definition of the payment context

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

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.

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 2.5 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 Offline Mobile Code No CVM Required Signature [10]	Online PIN Offline Mobile Code No CVM Required

Table 44: Local Transaction Contactless Payment - Acceptance Characteristics

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	Offline with Online capability POI: CDA and fDDA required Online only POI: CDA and fDDA required
Cardholder Verification Method	Online PIN Offline Mobile Code No CVM Required Signature

Table 45: Local Transaction Contactless Payment - Issuance Characteristics

3.1.2.2. _Card services_

For attended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required
Cancellation	Optional	Optional	Optional	Optional
Refund	Optional	Optional	Optional	Optional

Table 46: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

Table 47: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR UNATTENDED

---

[10] for acceptance of Cards which do not support online PIN.

3.1.2.2.1. 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
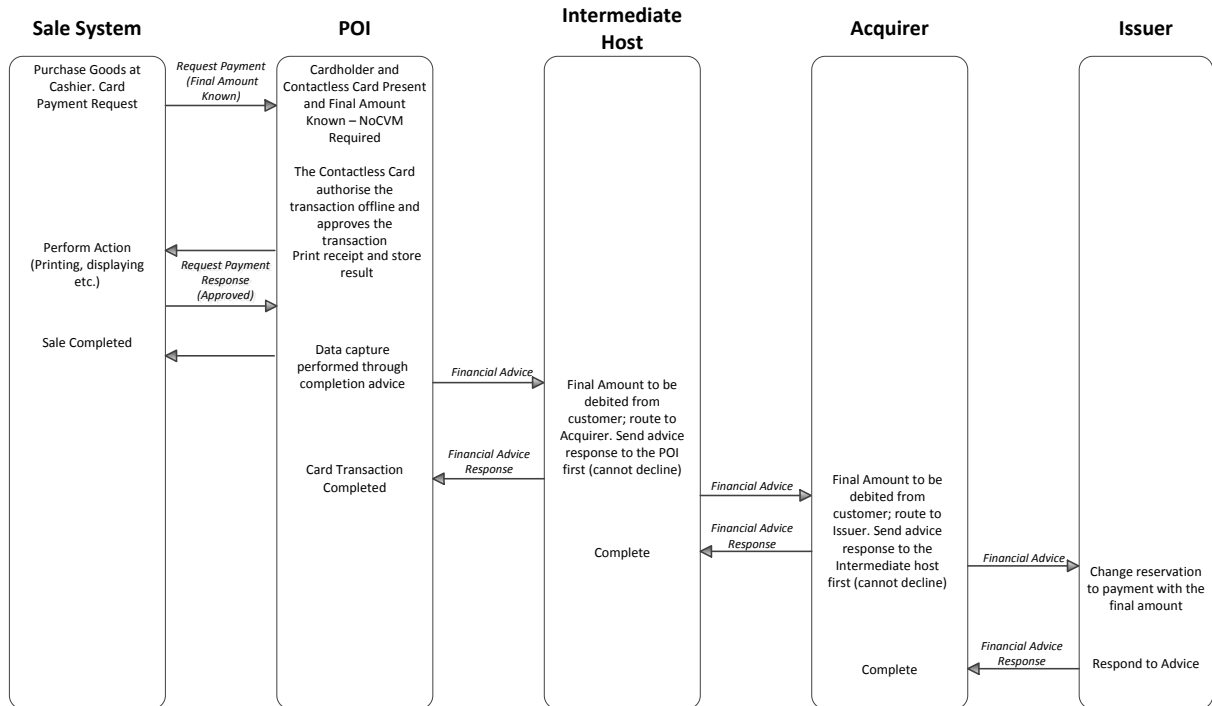
Figure 48: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION)WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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
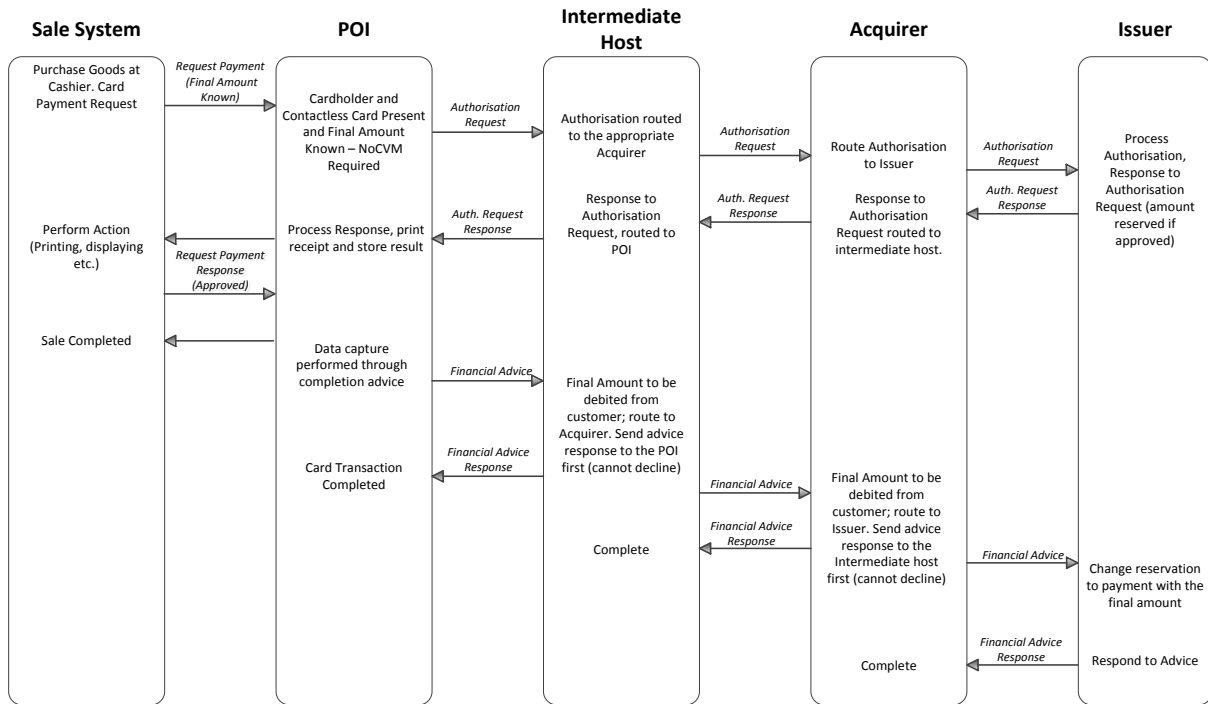
Figure 49: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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
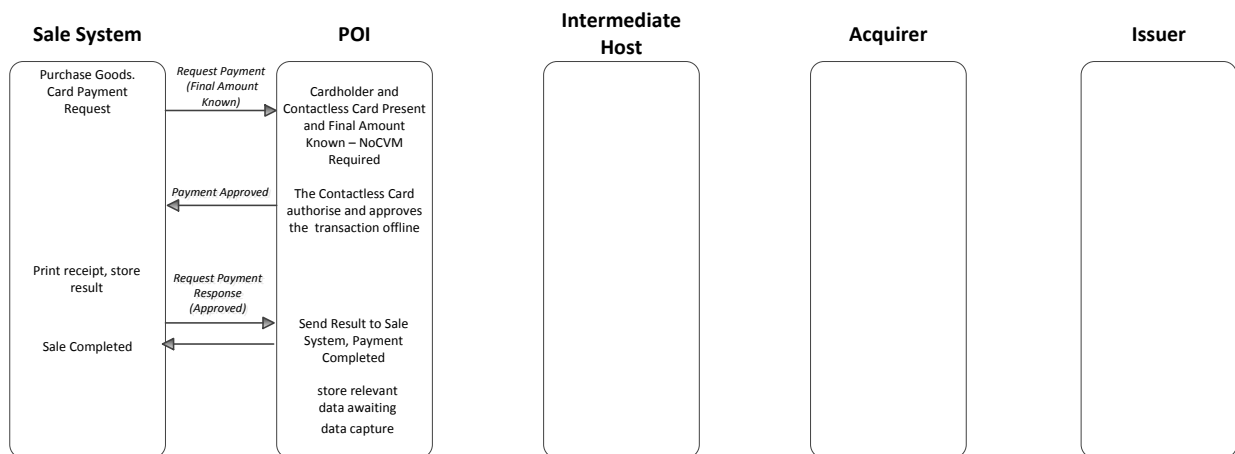
Figure 50: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH

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
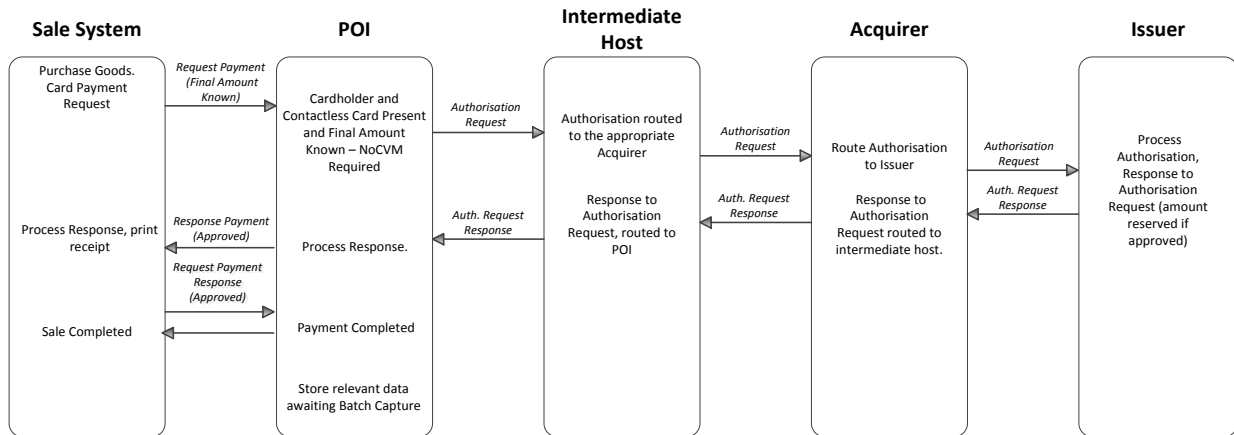
Figure 51: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH

3.2. Remote Transactions

3.2.1. e-and m-Commerce Payment

3.2.1.1. 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 payments related data is transferred from the payment page via the payment gateway to the Acquirer. The Virtual POI may also facilitate redirection services to support "direct" remote authentication of the Cardholder by the issuer via an authentication server.

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

Characteristics of the context	Virtual POI	
	with Cardholder Verification	without Cardholder Verification
Acceptance Technology	Manual Entry by Cardholder Stored Card Data Payment Credentials on Consumer Device Payment Credentials on Consumer Device with Authentication Application (M)RP Application on Consumer Device	
Physical Card or Consumer device present	Remotely	
Final amount known	Y	
Authorisation	Authorisation may either be online or offline (if an (M)RP Application is present in the consumer device) The Virtual POI shall be online	
Data Capture	All 3 modes defined in section 2.5 are applicable	
Card Authentication	Static Authentication for low risk payments (see [EBA]) Dynamic authentication [11], Redirection to the Card issuer domain may occur	
Passive Authentication	Optional, but requires redirection to the Card issuer domain	
Cardholder Verification Method	At least one of the following CVM shall be supported • Mobile Code (m-commerce) or Personal Code (e-commerce) • PIN on additional authentication device (does not involve virtual POI)	No CVM required
CVM entry on consumer device or on additional authentication device	Mandatory	Optional

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

Characteristics of the context	Virtual POI	
	with Cardholder Verification	without Cardholder Verification
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[12]	
Passive Authentication	Optional, but requires redirection to the Card issuer domain	
Cardholder Verification Method	At least one of the following CVM shall be supported • Mobile Code (m-commerce) or Personal Code (e-commerce) • PIN on additional authentication device (does not involve virtual POI)	No CVM required

3.2.1.2. *Card services*

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required
Cancellation	Optional	Optional	Optional	Optional
Refund	Optional	Optional	Optional	Optional

Table 52: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

---

[11] Note that some of the methods used for dynamic authentication also facilitate Cardholder authentication (e.g., OTP in some implementations).

[12] 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].

4. USE CASES

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	**On-line PIN**	**Mobile Code**
On-line transaction	Card and Mobile Contactless	Card and Mobile Contactless	Mobile Contactless Single tap/Double Tap
Off-line transaction	Card and Mobile Contactless[13]		Mobile Contactless Single tap/Double Tap

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	**On-line PIN**	**Mobile Code**
On-line transaction	Use case 3	Use case 4	
Off-line transaction	Use case 5		Use case 1 (single tap) Use case 2 (double tap)

A use case for an On-line transaction with mobile code is not described in this release of Book 6.

---

[13] With appropriate risk management in the MCP Application.

4.1. Contactless

4.1.1. Use case 1: Mobile Contactless - Single Tap - Off-line transaction - Off-line CVM

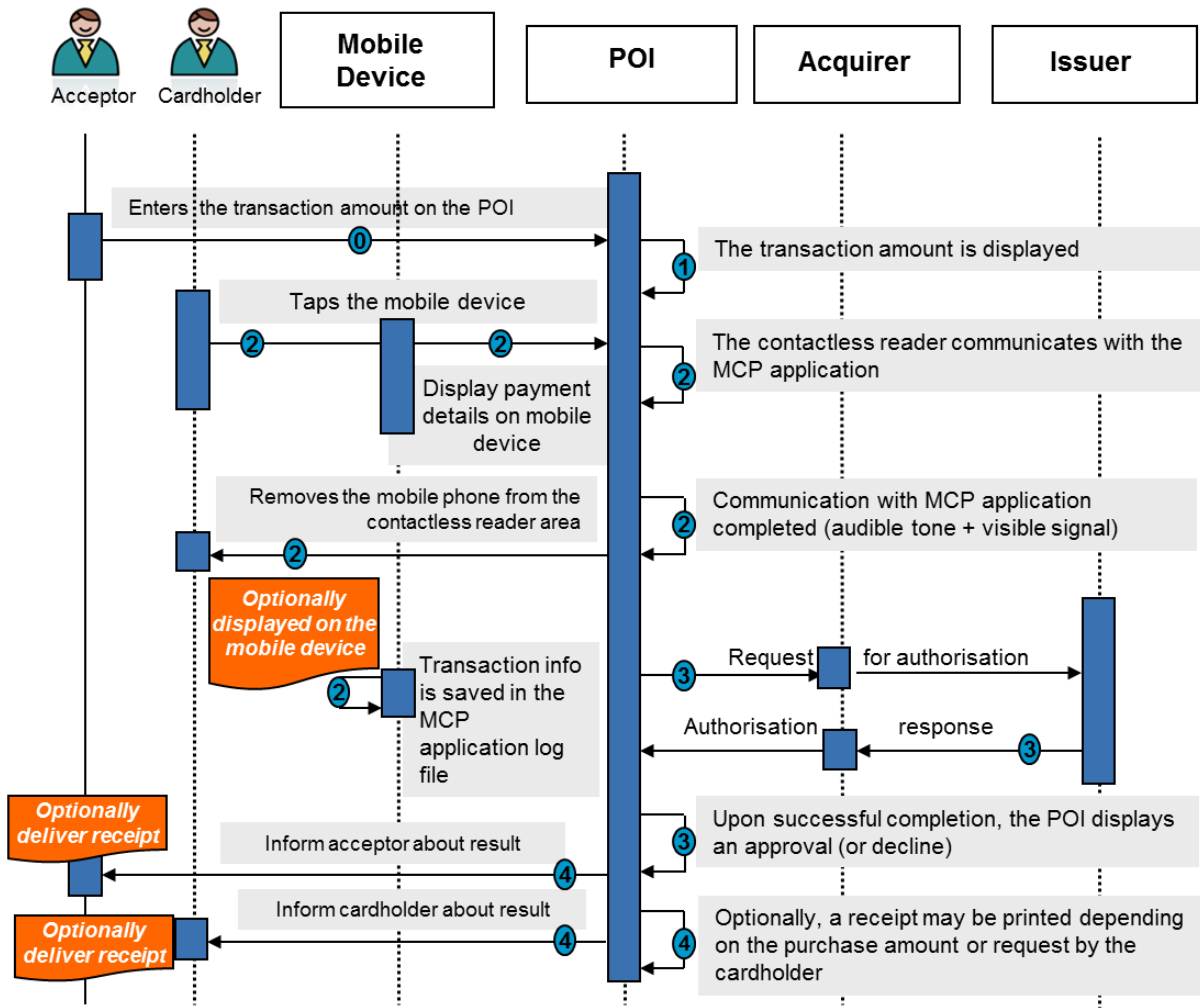# Off-line transaction – single Tap - off-line CVM
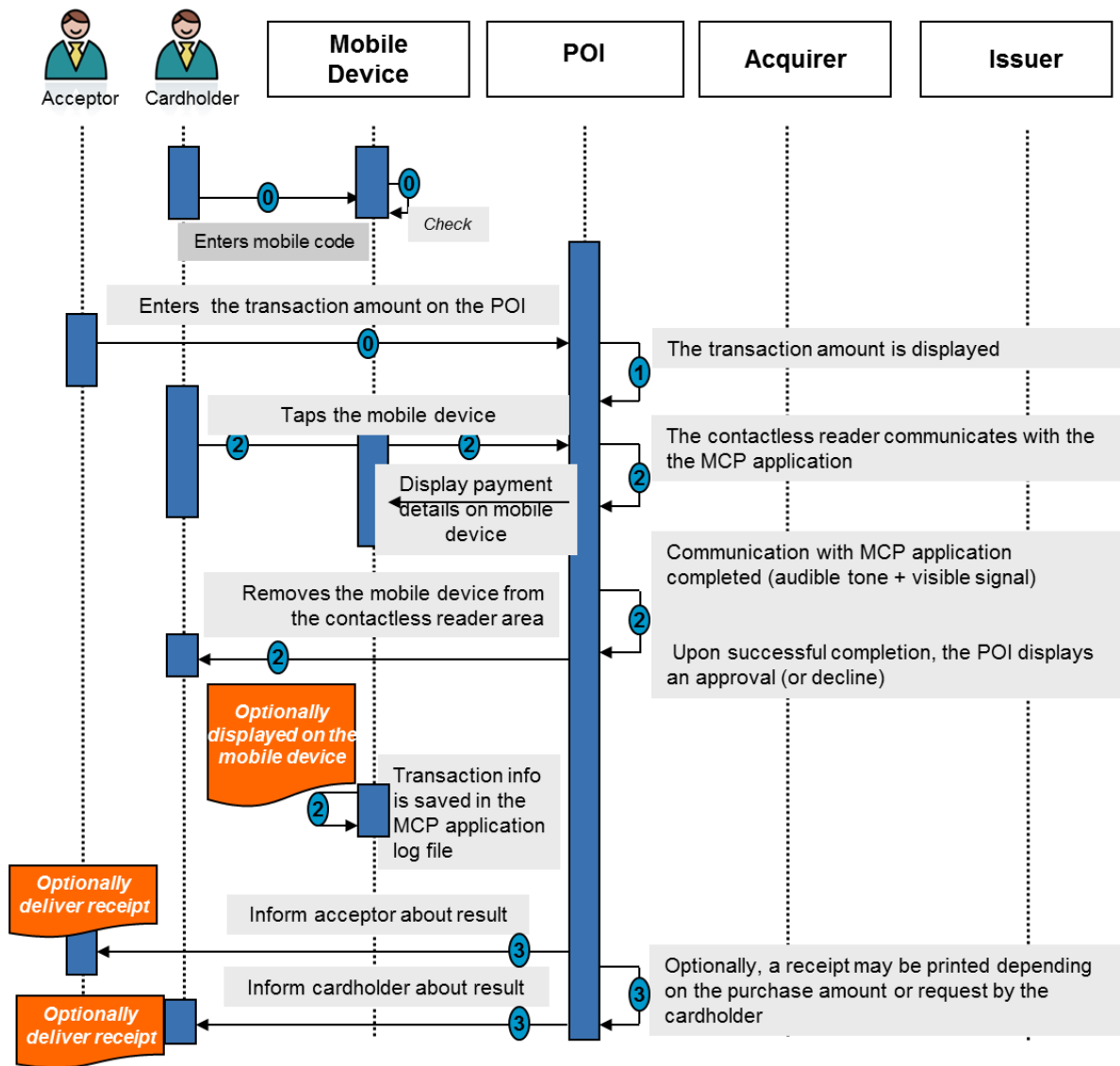
Figure 53: Single Tap - off-line transaction - off-line CVM

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.

- The Cardholder enters their mobile code which is verified by the MCP Application.

- The acceptor enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the acceptor's POI.

- The POI requests for a Card payment.

Step 2

- The Cardholder taps his/her mobile phone on the contactless reader area. (The Cardholder holds his/her mobile phone 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 through 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 phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.

- An off-line Card authentication/ transaction authorisation is performed by the POI.

- After processing the off-line authorisation, the acceptor's POI displays an approval or decline.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

Step 3

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

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

- Depending on the purchase amount, the acceptor's POI features and Cardholder choice, a transaction receipt may be printed.

4.1.2. Use case 2: Mobile Contactless - Double Tap - Off-line transaction - Off-line CVM
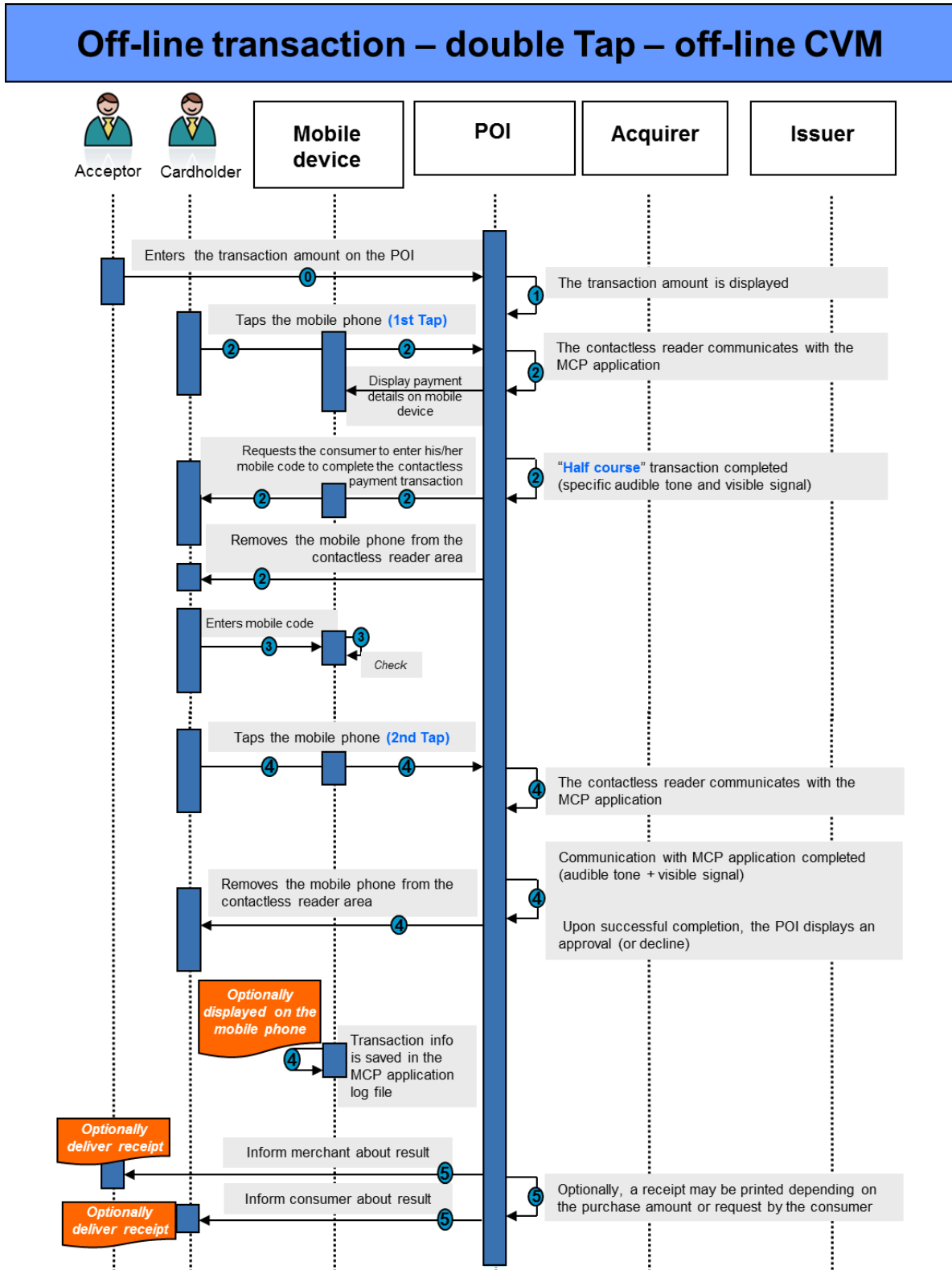
Figure 54: Double Tap - Off-line transaction - Offline CVM

Step 0 (Pre-requisite)

- The acceptor enters the transaction amount on the POI Terminal.

Step 1

- The transaction amount is displayed on the acceptor's POI Terminal.

- The POI requests for a Card payment.

Step 2

- The Cardholder taps (1st Tap) his/her mobile phone on the contactless reader area. (The Cardholder holds his/her mobile phone close to the contactless reader area until audible tone and/or visible signal take place).

- The POI uses the contactless technology and selects the appropriate MCP Application through 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 that an off-line CVM (mobile code) is required.

- A specific audible tone and/or visible signal indicate that the first step of the transaction is completed and that the Cardholder is requested to enter their mobile code to complete the contactless payment transaction.

- The Cardholder then removes his/her mobile phone from the contactless reader area.

Step 3

- The Cardholder checks the purchase amount and enters his/her mobile code on the mobile phone.

- Upon successful verification of the mobile code, a message is displayed on the mobile phone requiring the Cardholder to tap again his/her mobile phone on the contactless reader area.

Step 4

- The Cardholder taps again (2nd Tap) his/her mobile phone on the contactless reader area.

- An audible tone and/or visible signal then indicate that the mobile phone - contactless reader interaction is completed. After this the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.

- An off-line MCP Application authentication/authorisation is performed by the POI.

- After processing the off-line authorisation, the Acceptor's POI Terminal displays an approval or decline message.

- Information about the current transaction (e.g., transaction amount) is saved in the MCP Application log file and optionally displayed on the mobile phone.

Step 5

- The Acceptor is informed about result of the transaction.

- The Cardholder is informed about result of the transaction.

- Depending on the purchase amount, the Acceptor's POI Terminal features and Cardholder choice, a transaction receipt may be printed.

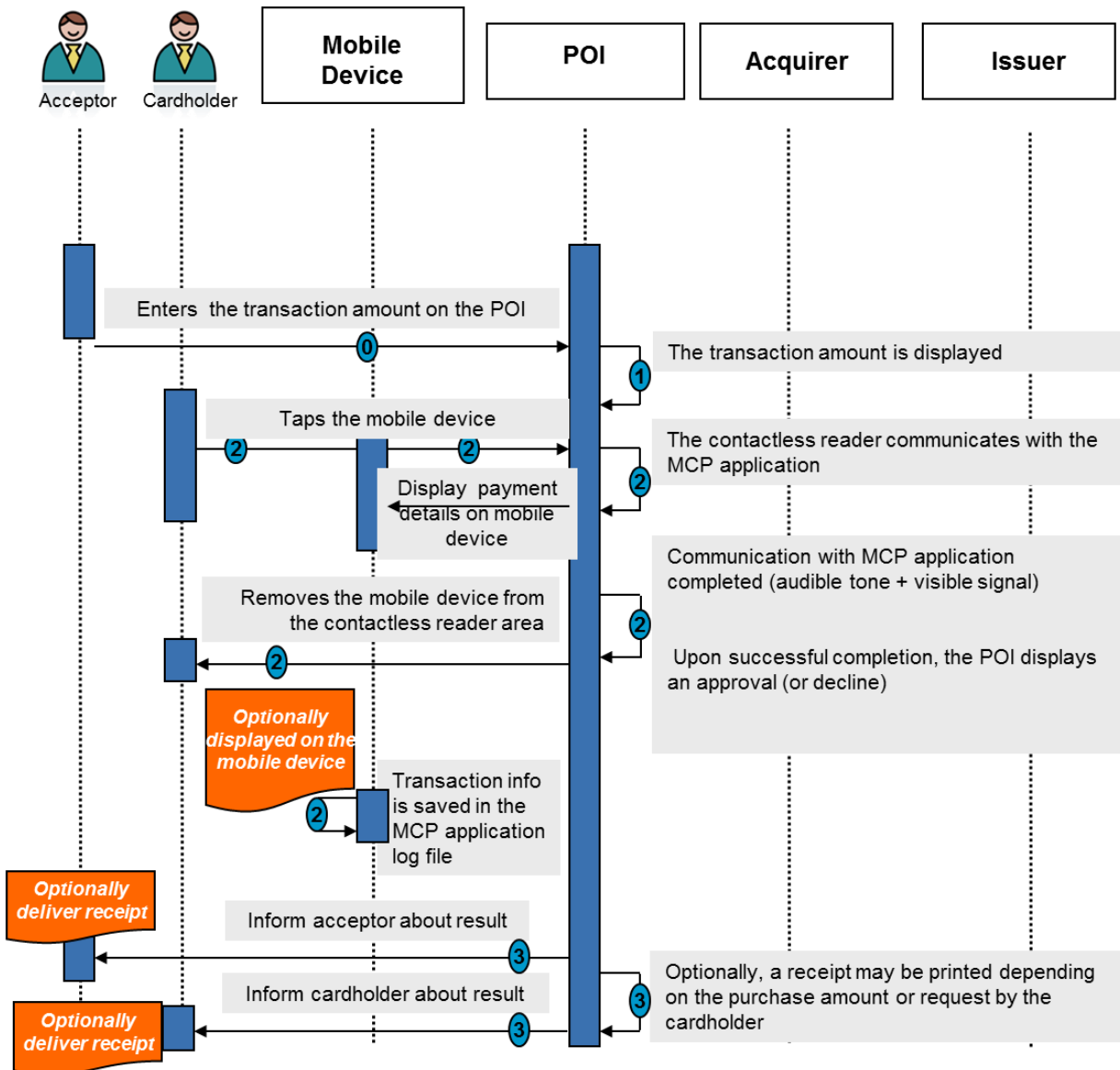### 4.1.3. Use case 3: Mobile contactless - Single Tap - On-line transaction - no CVM

Figure 55: Single Tap - On-line 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 acceptor enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the acceptor's POI.

- The POI requests a Card payment.

Step 2

- The Cardholder taps his/her mobile phone on the contactless reader area. (The Cardholder holds his/her mobile phone close to the contactless reader area until audible tone and/or visible signal take place).

- The POI selects the appropriate MCP Application through 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 that no CVM is required.

- An audible tone and/or visible signal then indicate that the mobile phone - contactless reader interaction is completed. After this, subsequently, the mobile phone can be removed from the contactless reader area. Note however that the transaction processing at the POI might still continue.

- An off-line Card authentication is optionally performed by the POI.

- An on-line Card authentication / transaction authorisation is performed by the POI.

- The Cardholder then removes his/her mobile phone from the contactless reader area.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

Step 3

- After processing the on-line authorisation, the acceptor's 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.

- Depending on the purchase amount, the acceptor's POI features and Cardholder choice, a transaction receipt may be printed.

Note: A similar use case can be described for an online contactless Card transaction (single brand) with no CVM.

4.1.4. Use case 4: Mobile contactless - Single Tap - On-line transaction - On-line CVM
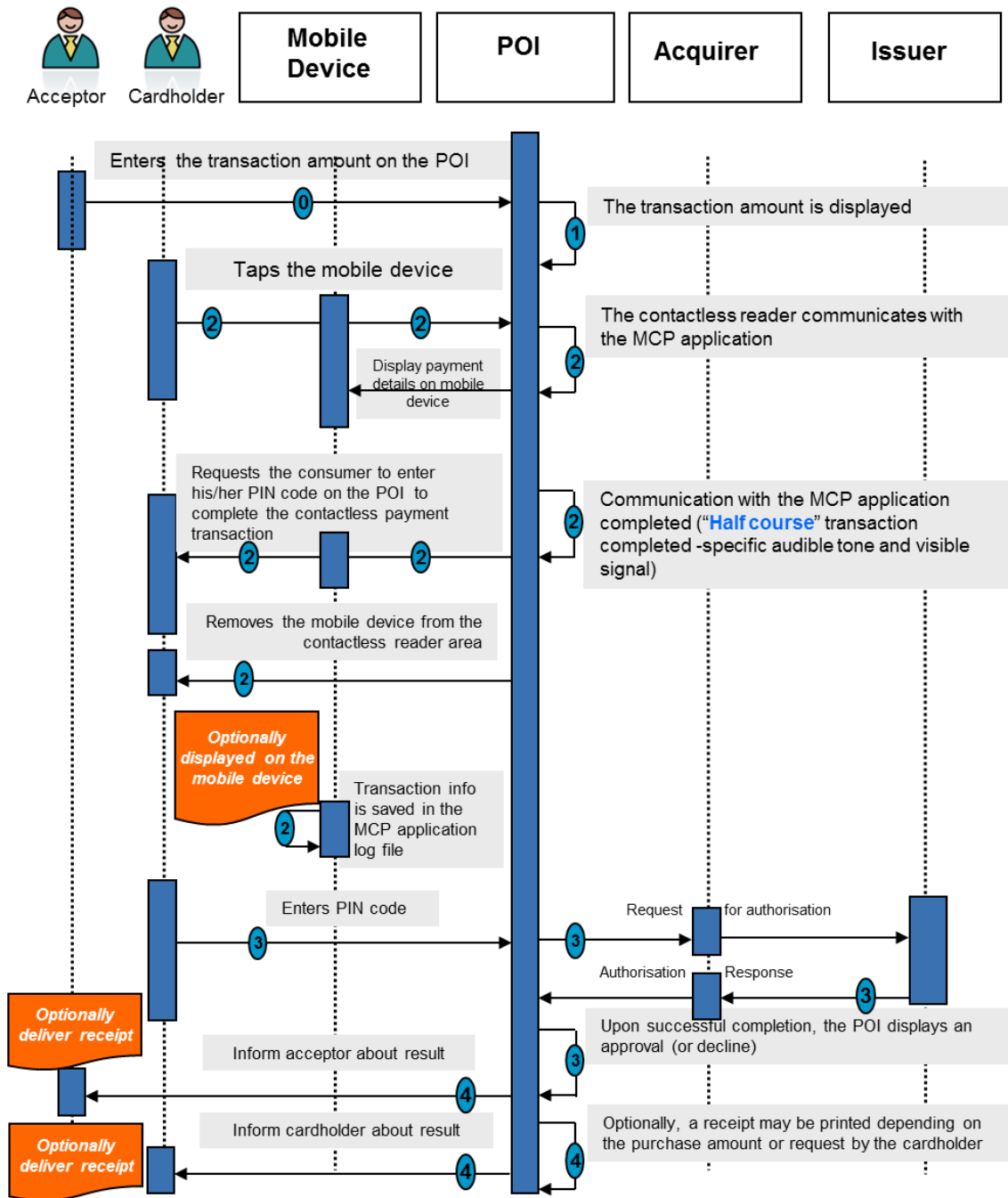
Figure 56: Single Tap - On-line transaction - On-line CVM

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 acceptor enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the acceptor's POI.

- The POI requests for a Card payment.

Step 2

- The Cardholder taps his/her mobile phone on the contactless reader area. (The Cardholder holds his/her mobile phone close to the contactless reader area until an audible tone and/or visible signal occur).

- The POI selects the appropriate MCP Application through 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 that an on-line CVM (PIN code on the POI) is required.

- A specific audible tone and/or visible signal indicate that "half-course" transaction is completed and that the Cardholder is requested to enter his/her PIN code on the POI to complete the contactless payment transaction.

- The Cardholder can remove his/her mobile phone from the contactless reader area.

- An off-line Card authentication is optionally performed by the POI.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

Step 3

- The Cardholder checks the purchase amount and enters his/her PIN code on the acceptor's POI.

- An on-line Card authentication / transaction authorisation is performed by the POI.

- After processing the on-line authorisation, the acceptor's POI Terminal displays an approval or decline.

Step 4

- The acceptor is informed about result of the transaction.

- The Cardholder is informed about result of the transaction.

- Depending on the purchase amount, the acceptor's POI features and Cardholder choice, a transaction receipt may be printed.

Note: A similar use case can be described for an online contactless Card transaction (single brand) with online CVM.

4.1.5. Use case 5: Mobile Contactless - Single Tap - Off-line transaction - no CVM

Figure 57: Single Tap - Off-line 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 acceptor enters the transaction amount on the POI.

Step 1

- The transaction amount is displayed on the acceptor's POI.

- The POI requests for a Card payment.

Step 2

- The Cardholder taps his/her mobile phone on the contactless reader area. (The Cardholder holds his/her mobile phone close to the contactless reader area until an audible tone and/or a visible signal takes place).

- The POI selects the contactless technology.

- The POI checks the available Applications and selects the appropriate MCP Application through the PPSE.

- The contactless reader and MCP Application[14] mutually determine appropriate processing of the transaction, including analysing and applying relevant risk management parameters.

- An audible tone and/or visible signal then indicate that the mobile phone - contactless reader interaction is completed. After this, the mobile phone can be removed from the contactless reader area. Note, however, that the transaction processing at the POI might still continue.

- An off-line Card authentication/ transaction authorisation is performed by the POI.

- After processing the off-line authorisation, the acceptor's POI displays an approval or decline.

- Information about the current transaction is saved in the MCP Application log file and optionally displayed on the mobile phone.

Step 3

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

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

- Depending on the purchase amount, the acceptor's POI features and Cardholder choice, a transaction receipt may be printed.

---

[14] In this use case it is assumed that the MCP Application has appropriate risk management capabilities.

Note: A similar use case can be described for an offline contactless Card transaction (single brand) with "no CVM".

4.2. E and m commerce

4.2.1. e- & m-commerce with Static Authentication- No CVM

In this scenario, illustrated in the figure below, the Cardholder uses his/her consumer device to conduct a payment to an acceptor, which is providing goods or services (e.g., mobile content). In this scenario, no CVM method is used.
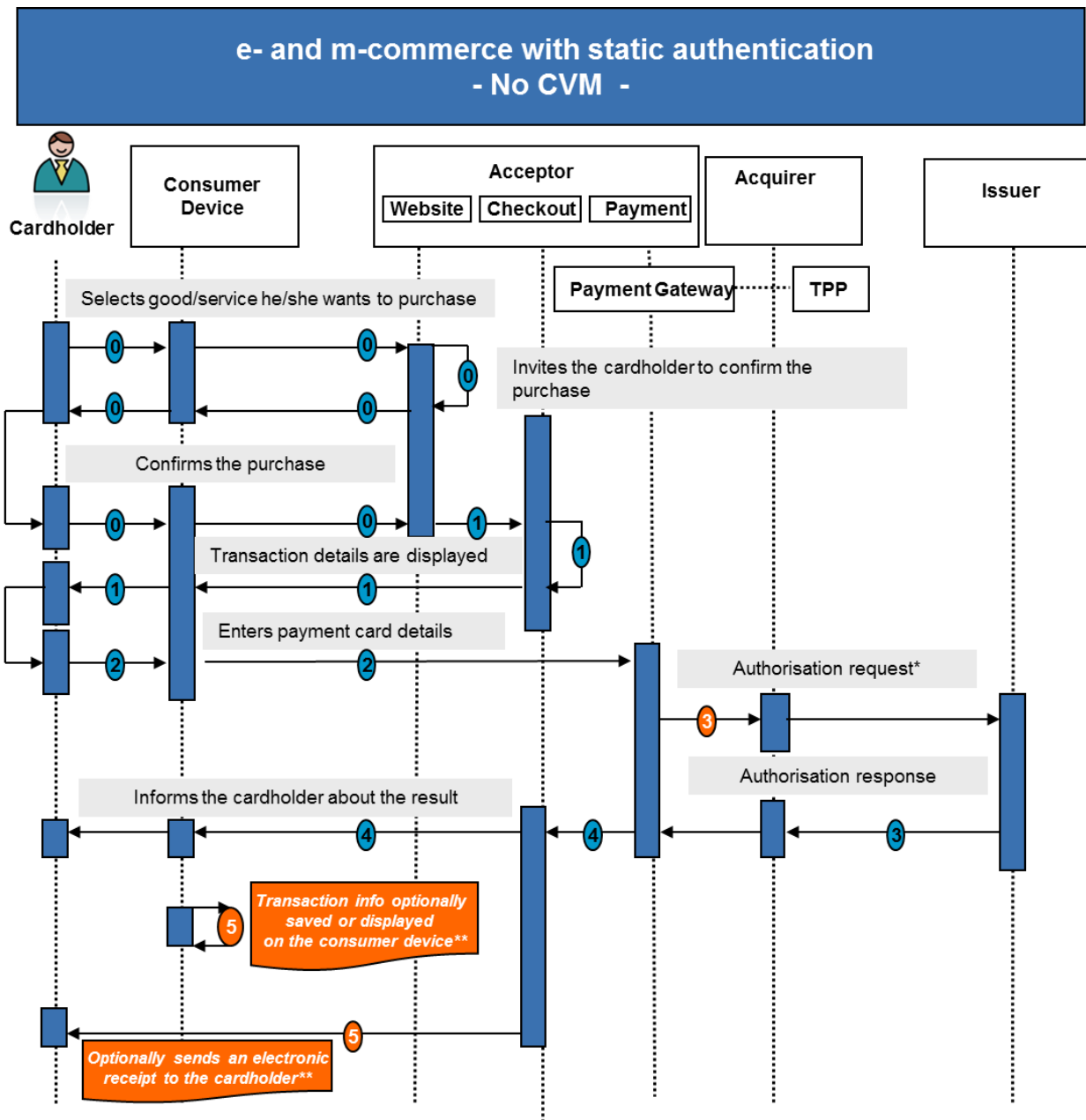
Figure 58: e- & m-commerce with Static Authentication- No CVM

In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)

- The Cardholder navigates using his/her consumer device to an acceptor website via internet and selects the goods / service he/she wants to purchase.

- After having accepted the general purchase conditions, he/she is invited to confirm the purchase.

Step 1 (Transaction details displayed)

- The checkout section of the acceptor website displays the transaction details including the amount and the payment options, via the consumer device to the Cardholder.

Step 2 (Card payment selection)

- The Cardholder selects the "payment by Card" option via internet and is subsequently redirected to the payment section under the control of a payment gateway to proceed with the transaction under a secure http connection (https). He/she is invited to enter his/her payment Card details (e.g., PAN, expiry date and CSC).

- As an alternative to the entry of the payment Card details by the Cardholder, there may be an Application stored in, or accessed through, the consumer device. The Cardholder is then redirected to the user interface of this Application to select the payment Card to be used and the Card details are automatically transferred to the payment section.

- The transaction summary is displayed on the consumer device, typically including the date, the acceptor reference, the amount and the selected payment Card whereby the Cardholder is invited to confirm the transaction.

Step 3 (Payment process)

- The payment is processed as a Remote Card transaction. This typically[15] involves an on-line authorisation request by the acceptor to the issuer, at which time authentication occurs.

Step 4 (Transaction finalisation)

Once the payment is authorised,

- The Cardholder is automatically redirected to the acceptor website and receives a confirmation of the transaction;

---

[15] 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.

- The acceptor releases the good / service to the Cardholder.

Step 5 (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 made available by the acceptor to the Cardholder.

4.2.2. e- and m-commerce with dynamic authentication

In this scenario, illustrated in the figure below, the Cardholder uses his/her 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.
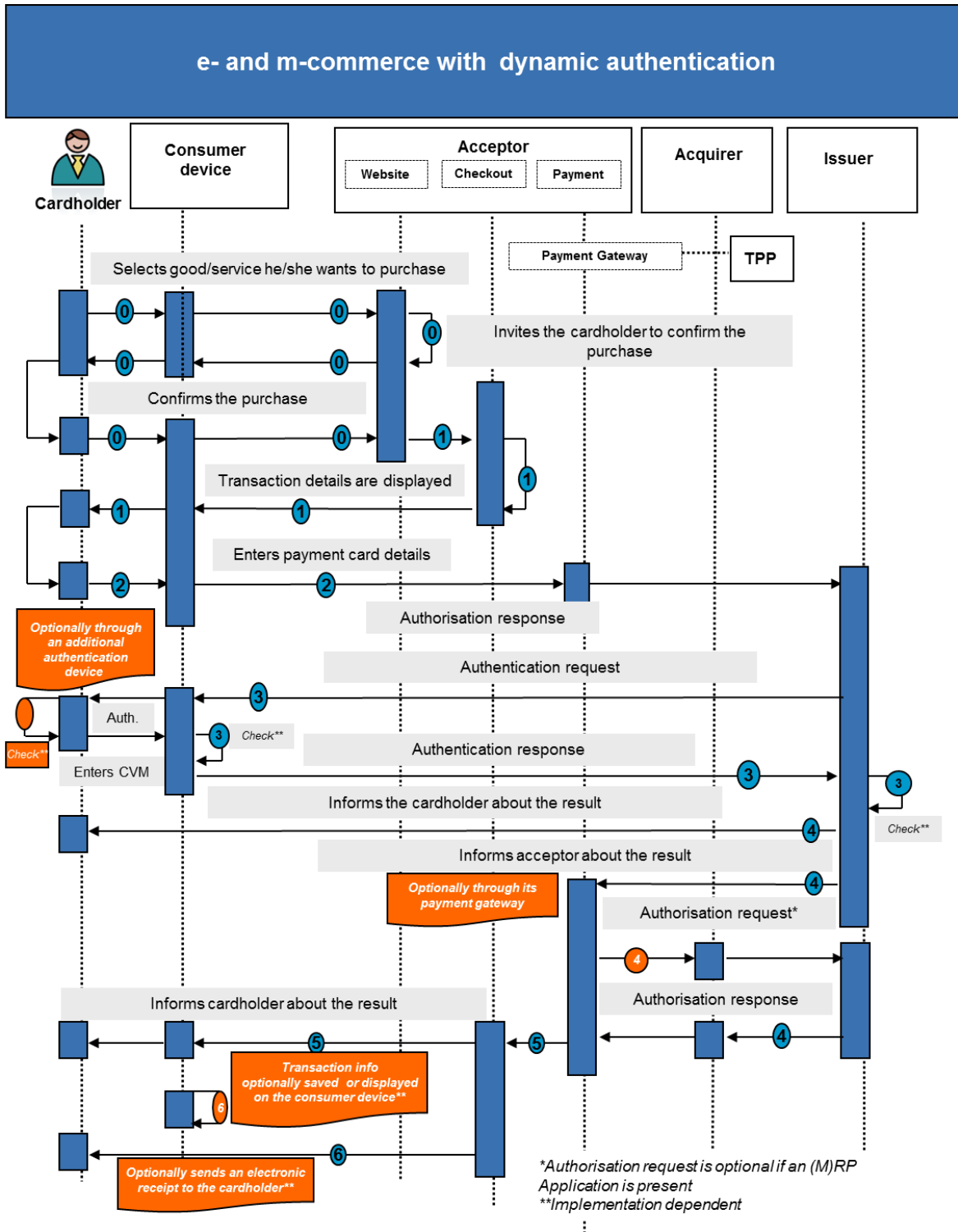
Figure 59: e- & m-commerce with dynamic authentication

In the figure above, the following steps are illustrated:

Step 0 (Pre-requisite)

- The Cardholder navigates using his/her consumer device to an acceptor website via internet and selects the goods / service he/she wants to purchase.

- After having accepted the general purchase conditions, he/she is invited to confirm the purchase.

Step 1 (Transaction details displayed)

- The checkout section of the acceptor website displays the transaction details including the amount and the payment options, via the consumer device to the Cardholder.

Step 2 (Card payment selection)

- The Cardholder selects the "payment by Card" option via internet and is subsequently redirected to the payment section under the control of a payment gateway to proceed with the transaction under a secure http connection (https). He/she is invited to enter his/her payment Card details (e.g., PAN, expiry date and CSC).

- As an alternative to the entry of the payment Card details by the Cardholder, there may be an Application stored in, or accessed through, the consumer device. The Cardholder is then redirected to the user interface of this Application to select the payment Card to be used and the Card details are automatically transferred to the payment section.

- The transaction summary is displayed on the consumer device, typically including the date, the acceptor reference, the amount and the selected payment Card whereby the Cardholder is invited to confirm the transaction.

Step 3 (Authentication) [16]

The Cardholder and the relevant data are subsequently authenticated[17] by the issuer[18] or their agent according to one of the following typical processes:

- In case of a payment Card via internet, the Cardholder and the relevant data are authenticated by their issuer via a dynamic authentication method. Various methods may exist. If an additional authentication device is used, the Cardholder inserts his/her payment Card into the additional device; the issuer provides the Cardholder with a "challenge" to be entered / transmitted (on)to the additional device, followed by the Cardholder's PIN entry. The authentication device then generates a "response" which the Cardholder is requested to enter at a given time during this process on their

[16] The usage of a CVM in combination with the dynamic authentication results into a strong customer authentication.

[17] This authentication may involve transaction details.

[18] Or a TPP in the issuer domain.

consumer device. The response is subsequently transmitted to the issuer via the authentication response for verification.

- In case an Authentication or (M)RP Application is present on the consumer device, a dynamic authentication method (e.g., challenge/response method) is initiated by the issuer and is handled automatically by the authentication Application in a secure environment. The Cardholder is also requested to enter his/her personal/mobile code during the transaction process. The personal/mobile code is checked either locally by the Authentication or (M) RP Application, or on-line by the issuer.

Step 4 (Payment process)

- The Cardholder is informed by their issuer about the result of the authentication.

- The acceptor is informed (possibly involving its payment gateway) by the issuer about the result of the authentication of the Cardholder.

- Subject to successful authentication by the issuer, the payment is further processed as a Remote Card transaction. This typically[19] involves an on-line 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.

---

[19] 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. FIGURES AND TABLES

❧⁓❧