EPC020-08 26.05.2016

(Vol Ref. 7.6.2.50)

SEPA CARDS STANDARDISATION (SCS) "VOLUME"

BOOK 6

IMPLEMENTATION GUIDELINES

Payments and Cash Withdrawals with Cards in SEPA

Applicable Standards and Conformance Processes

© European Payments Council/Conseil Européen des Paiements AISBL.
Any and all rights are the exclusive property of
EUROPEAN PAYMENTS COUNCIL - CONSEIL EUROPEEN DES PAIEMENTS AISBL.

DRAFT

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.6.2.50
Date of Version	26 May 2016
Reason for Issue	Consultation
Reviewed by	CSG
Produced by	CSG Secretariat
Owned by	EPC
Circulation	Public

Conseil Européen des Paiements AISBL – Cours Saint-Michel 30 – B 1040 Brussels
Tel: +32 2 733 35 33 Fax: +32 2 736 49 88
Enterprise N° 0873.268.927 www.epc-cep.eu secretariat@epc-cep.eu

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
7.6.2.11-7.6.2.5	16.12.2015-	Working Version 2015-2016

DRAFT

Table of Contents

1. GENERAL 5

1.1 Book 6 - Executive summary 5
1.1.1. Objectives 5
1.1.2. Migration Roadmap 6
1.1.3. Structure of this book 6

1.2 Description of changes since the last version of Book 6 7

2. GENERAL IMPLEMENTATION GUIDELINES 8

2.1. Introduction 8

2.2. Implementation guidance on Priority Selection and Choice of Application 8
2.2.1. Local Transactions 8
2.2.1.1. Override option during the EMV Chip with Contact payment process 8
2.2.1.2. Override option from an upfront screen before the EMV payment process starts with Chip Contact and Chip and Mobile Contactless 9
2.2.2.1.1 Example of an override option using an upfront selection screen 10
2.2.1.3. Example of choice of application by the sole cardholder during the EMV payment process 11
2.2.2. Remote Transactions 12
2.2.2.1 Example of Cardholder selection using brand logos 12
2.2.2.2 Example Acceptor's priority selection using BIN / IIN tables with a cardholder's overriding mechanism 13

2.3. Implementation guidance on Visual Product Identification 15

2.4. PIN based Cardholder Verification Methods 15
2.4.1. PIN Based Cardholder Verification Methods (Acceptance) 15
2.4.1.1. Volume Conformant Implementation 15

2.5. Data Capture 16
2.5.1. Current Implementations 16
2.5.2. Volume Conformant Implementation 16
2.5.3. Volume Conformant Implementation – Examples 16

3. IMPLEMENTATION GUIDELINES PER PAYMENT CONTEXT 20

3.1. Local Transaction 20
3.1.1. Chip with Contact 20
3.1.1.1. Payment 20
3.1.1.1.1. Definition of the payment context 20
3.1.1.1.2. Card Services 21

DRAFT

3.1.1.1.3. Example of Message Flows 22
3.1.1.1.3.1. Example of Message Flow - Attended with PIN 22
3.1.1.1.3.2. Example of Message Flow - Unattended with PIN 24
3.1.1.1.3.3. Example of Message Flow - Unattended with "No CVM Required" 25
3.1.1.2. Deferred Payment 27
3.1.1.2.1. Definition of the payment context 27
3.1.1.2.2. Card Services 28
3.1.1.2.3. Example of Message Flows 29
3.1.1.3. Pre-Authorisation Services 30
3.1.1.3.1. Definition of the payment context 30
3.1.1.3.2. Example of Message Flows 35
3.1.2. Chip and Mobile Contactless Payment 37
3.1.2.1. Definition of the payment context 37
3.1.2.2. Card services 38
3.1.2.2.1. Example of Message Flows 39

3.2. Remote Transactions 41
3.2.1. e-and m-Commerce Payment 41
3.2.1.1. Definition of the payment context 41
3.2.1.2. Card services 43

4. USE CASES 44

4.1. Contactless 45
4.1.1. Use case 1: Mobile Contactless - Single Tap - Off-line transaction - offline CVM 45
4.1.2. Use case 2: Mobile Contactless - Double Tap - Off-line transaction - Offline CVM 48
4.1.3. Use case 3: Mobile contactless - Single Tap - On-line transaction - no CVM 51
4.1.4. Use case 4: Mobile contactless - Single Tap - On-line transaction - On-line CVM 54
4.1.5. Use case 5: Mobile Contactless - Single Tap - Off-line transaction - no CVM 57

4.2. E and m commerce 59
4.2.1. Basic e- and m-commerce - No CVM 59
4.2.2. Secured e- and m-commerce - Strong dynamic authentication 62

5. FIGURES AND TABLES 65

DRAFT

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.

The objective of Book 6 is to describe how stakeholders shall implement some or all of the Volume requirements, as appropriate for their business needs. 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.

As not all requirements and Services described in Book 2 of the Volume are offered and supported by all acceptors, 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.

This document will provide:

- General Implementation Requirements and options applicable to the Payment Contexts;
- Specific implementation Requirements 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:
  - Chip with Contact;
  - Chip and Mobile Contactless.
- Remote with:
  - E and m-Commerce

DRAFT

- Mail Order Telephone Order

Deferred Payment Service:

- Local with:
  - Chip with Contact;

Pre-Authorisation Service:

- Local with:
  - 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

The long term vision is that all approved card payment products and solutions for transactions initiated in the SEPA area will in future be conformant with the requirements described in the Volume. A migration roadmap is therefore required to move from the current implementations to the future vision mindful of a desire to maintain interoperability with non SEPA general purpose cards.

All newly approved products and solutions shall conform to the requirements of the latest published Volume release within a maximum of 3 years after publication.

In addition, 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 requirements and options are defined in chapter 2 and specific payment contexts implementation requirements are in chapter 3. Both sections include Volume conformant requirements and implementation options with selected roadmaps for implementing the options by a given date.

DRAFT

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 guidance on the Interchange Fee Regulation (as defined in articles 8.6 and 10.5) on 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 book2 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 are kept for completeness.
- Chapter4: A new chapter with five use cases for contactless, e and m-commerce transactions has been introduced.

DRAFT

2. General Implementation Guidelines

2.1. Introduction

This section describes common 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 Acceptors' priority selection and cardholder's override mechanism for local contact and contactless card transactions for cards issued in EEA 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 sole cardholder during the EMV payment process

Please note that these are just three examples of priority selection implementation with a cardholder override mechanism. They are provided for illustration purposes and may or may not be integrated in the final release v8.0 of the Volume, to be published in December 2016. The CSG are welcoming any comment to improve these examples as well as submissions of other examples of implementations.

2.2.1. Local Transactions

2.2.1.1. Override option during the EMV Chip with Contact payment process

If the Cardholder is presented with the Acceptor's preferred application on the POI using an automatic mechanism, the following rules apply:

The POI shall display all the required information of the pre-selected application on the POI first screen in the following order:

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

DRAFT

Example of Choice of Application in the case of Acceptor pre-selection with signature as CVM and without displaying the final amount

FIGURE 1: EXAMPLE: CHOICE OF APPLICATION IN THE CASE OF ACCEPTOR PRE-SELECTION WITH SIGNATURE AS CVM AND WITHOUT DISPLAYING THE FINAL AMOUNT

Example of Choice of Application in the case of Acceptor pre-selection that includes the total amount and PIN entry.

Figure 2: Example: Choice of Application in the case of Acceptor pre-selection that includes THE TOTAL amount and PIN entry.

2.2.1.2. Override option from an upfront screen before the EMV payment process starts with Chip Contact and Chip and Mobile Contactless

Where technically feasible by the POI, e.g. a keyboard or touchscreen are present, the cardholder may perform a selection of a 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 willingness to have displayed upfront the card applications they wish to use to pay by choosing the Corr / Yellow button (additional keys or virtual button may be provided).

DRAFT

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 for interacting with the POI using:

- Chip contactless card and Mobile technology
- Chip with contact technology (an override option described in the next section may be included).

b. Following with the Acceptor's POI preferred application that 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 can be 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).

2.2.1.2.1. Example of an override option using an upfront selection screen

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 3.

Example: Override option using an upfront selection screen on the POI

Figure 3: EXAMPLE: OVERRIDE OPTION USING AN UPFRONT SELECTION SCREEN ON THE POI

DRAFT

If the cardholder **wishes** to choose their preferred method of payment and selects upfront the **yellow** button "CORR" then the cardholder may:

- Insert the card in the POI

At which point only Contact card payment is offered. All card applications mutually supported by the card and the POI are presented to the cardholder for them to select. The merchants preferred payment may be pre-selected (e.g. at the top of the list to be first item and/or highlighted (pre-selected)). After final selection by the cardholder, standard EMV payment process applies.

- Present the card to the POI

At which point only contactless card payment is offered. All card applications mutually supported by the card and the POI are presented to the cardholder for them to select. The merchants preferred payment is being pre-selected (e.g. at the top of the list to be first item and/or highlighted (pre-selected)). When this is supported by the POI, multiple taps (one additional for the choice of application for contactless card payment) may be offered, 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, the cardholder may:

- Present the card (tap a card, a mobile, …) **without** pressing the selection yellow button "CORR"

The cardholder wants to "tap & go". He 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.

- Insert the card **without** pressing the selection yellow button "CORR"

The Merchant preferred application is selected. He may be asked to enter the PIN and confirm (PIN verification). Standard EMV payment applies.

2.2.1.3. Example of choice of application by the sole cardholder during the EMV payment process

In this particular example the acceptor has not implemented a priority selection and the POI allows for cardholder choice. The POI shall present all mutually supported application to enable Cardholder choice.

When presented to the cardholder, the Application name, and if available the category of card, should be accompanied by a number. It allows the cardholder to choose the application by use of a key on the numeric keypad corresponding to the number assigned to each application mutually supported.

DRAFT

Example choice of Application by the sole Cardholder

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

Figure 4: EXAMPLE: CHOICE OF APPLICATION BY THE SOLE CARDHOLDER AMONG ALL MUTUALLY SUPPORTED APPLICATIONS

The cardholder is then asked to enter his PIN and validate the transaction.

Example of Choice of Application by the sole Cardholder including the selected application, total amount and PIN entry

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

Figure 5: EXAMPLE: CHOICE OF APPLICATION BY THE SOLE CARDHOLDER AFTER HAVING SELECTED THEIR PREFERABLE APPLICATION

2.2.2. Remote Transactions

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

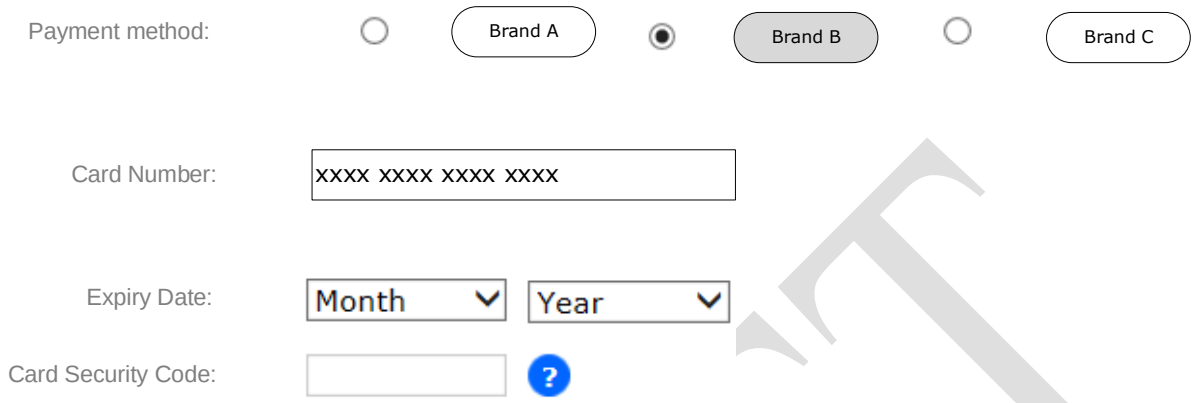
2.2.2.1 Example of Cardholder selection using brand logos

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

DRAFT

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.



2.2.2.2 *Example Acceptor's priority selection using BIN / IIN tables with a cardholder's overriding mechanism*

When choosing to pay by card, the Cardholder is asked to input the PAN of the card he wishes to pay with. If the cardholder uses a co-badged card, the Acceptor sets a priority selection and presents his preferred card application to the cardholder. An overriding option is provided to the cardholder.

The Acceptor's Virtual POI is extracting the BIN range from the PAN and uses IIN/BIN tables for the identification of the card Product and brand and to determinate its preferred card application presented to the cardholder.

DRAFT

Step 1: Acceptor's selection

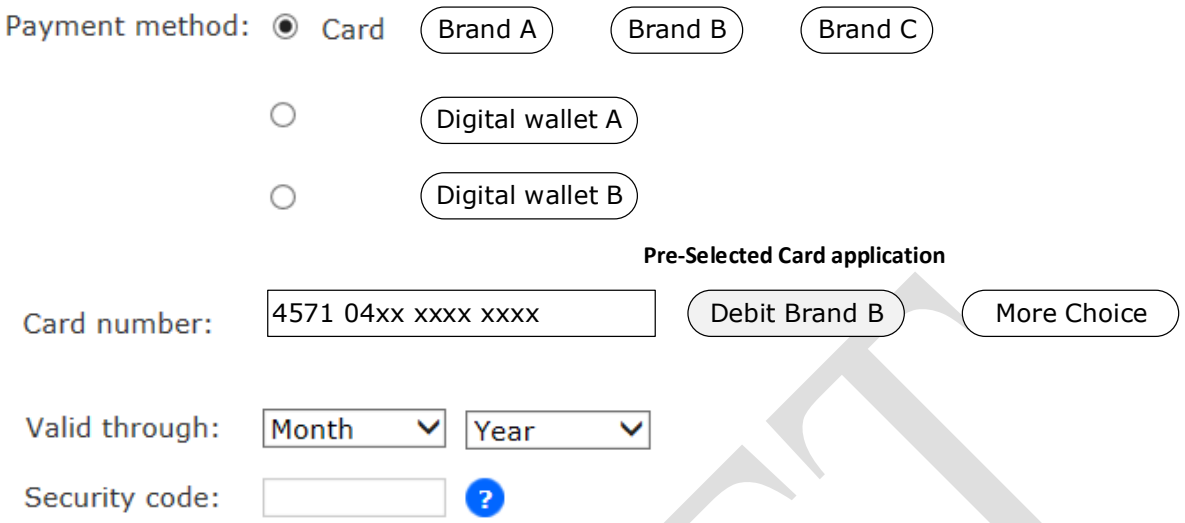


FIGURE 4: EXAMPLE: REMOTE TRANSACTION WITH ACCEPTOR'S PRE-SELECTION CHOICE OF APPLICATION FROM PAN INPUT

The Cardholder may override the Acceptor's Selection by choosing the "more choice" option. The Acceptor will display all card applications and may put their preferred card application on top of the list.

Step 2: the Cardholder exercises their override right

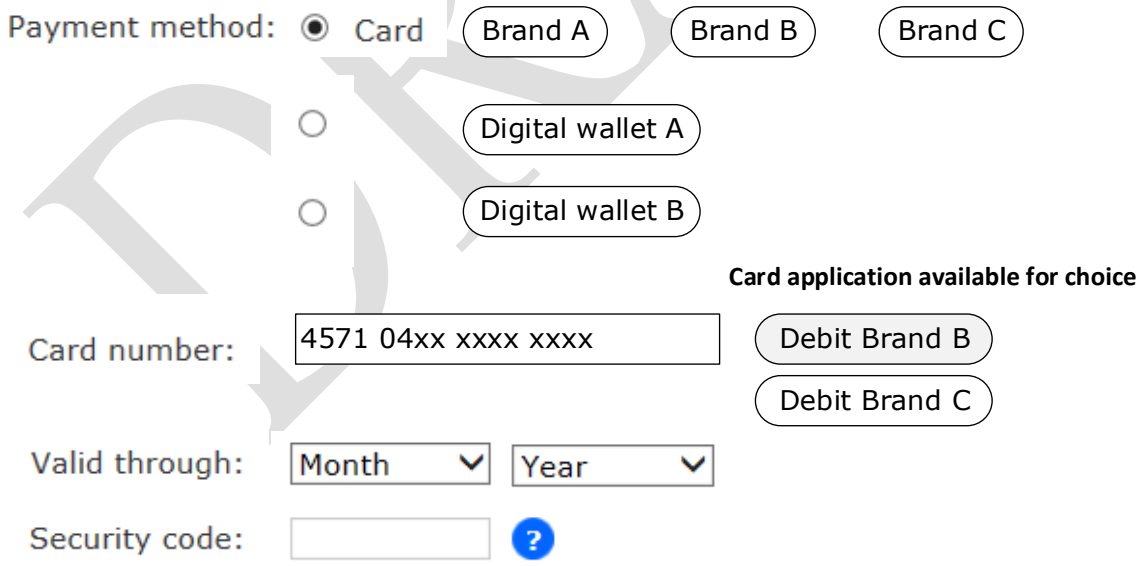


FIGURE 5: EXAMPLE: REMOTE TRANSACTION CHOICE OF APPLICATION FROM PAN INPUT WITH OVERRIDING

DRAFT

2.3. Implementation guidance on Visual Product Identification

The appropriate card category for Visual Product Identification shall be displayed on the card in English, as follows;

- Prepaid
- Debit
- Credit
- Commercial

If required by local regulation, the card category may also be displayed in the local language.

2.4. PIN based Cardholder Verification Methods

Plaintext PIN is no longer deemed to be a sufficiently secure cardholder verification method to be supported by the POI. The objective is to remove its support from the POI.

2.4.1. PIN Based Cardholder Verification Methods (Acceptance)[1]

This section only applies to POIs with PIN pads providing payment services excluding ATMs.

2.4.1.1. Volume Conformant Implementation

	Offline Plaintext PIN	Offline enciphered PIN	Online PIN
Online only terminals	Not used for SEPA Cards and shall not be mandatory on the POI from 2020	Conditional[2]	Conditional[4]
Offline with online capability terminals	Not used for SEPA Cards and shall not be mandatory on the POI from 2020	Required	Optional[3]

TABLE 6: VOLUME CONFORMANT CARDHOLDER VERIFICATION METHOD (ACCEPTANCE)

[1] Whether or not this section will be integrated in to Book 2 version 8.0 will be reviewed post consultation.

[2] Either

- Offline Plaintext PIN and Offline enciphered PIN;
- Online PIN;
- all 3 must be supported.

[3] Currently only required for some debit brands.

DRAFT

2.5. Data Capture

2.5.1. Current Implementations

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.

2.5.2. Volume Conformant Implementation

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.

2.5.3. Volume Conformant Implementation – 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.

DRAFT

Mode 1: Online Authorisation, Capture immediately after Transaction Completion

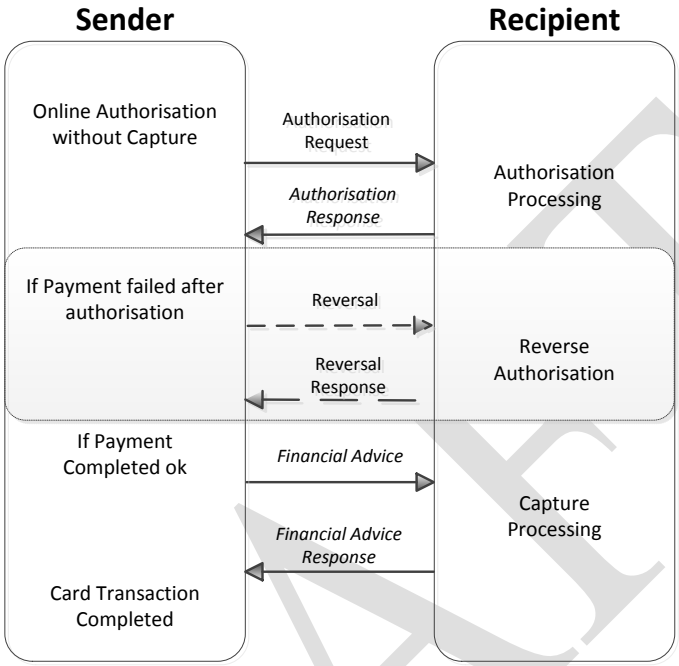


FIGURE 7: MODE 1

DRAFT

Mode 2: Online Authorisation, Capture by Batch

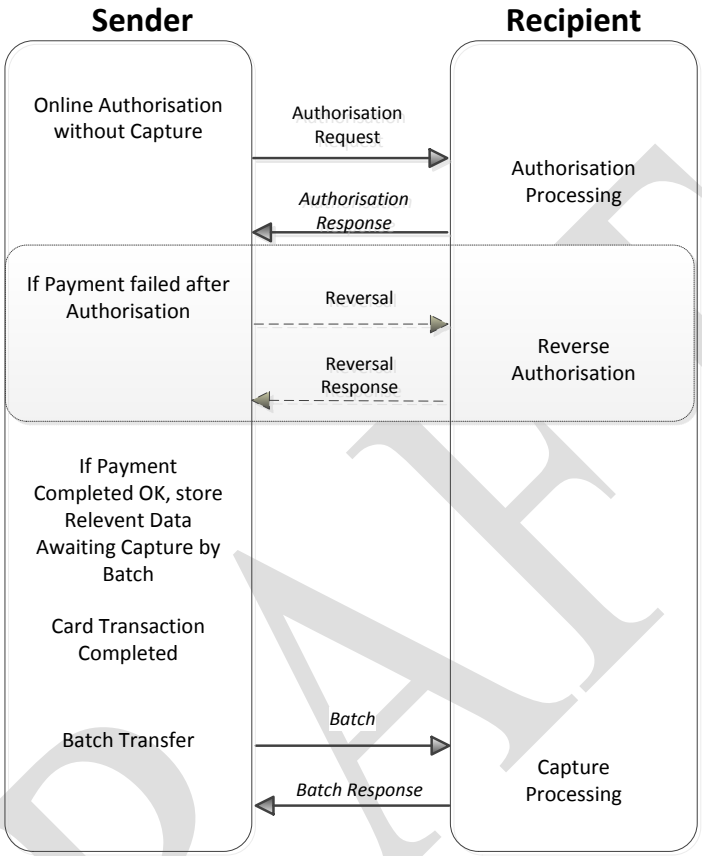


FIGURE 8: MODE 2

DRAFT

Mode 3: Online Authorisation with Capture

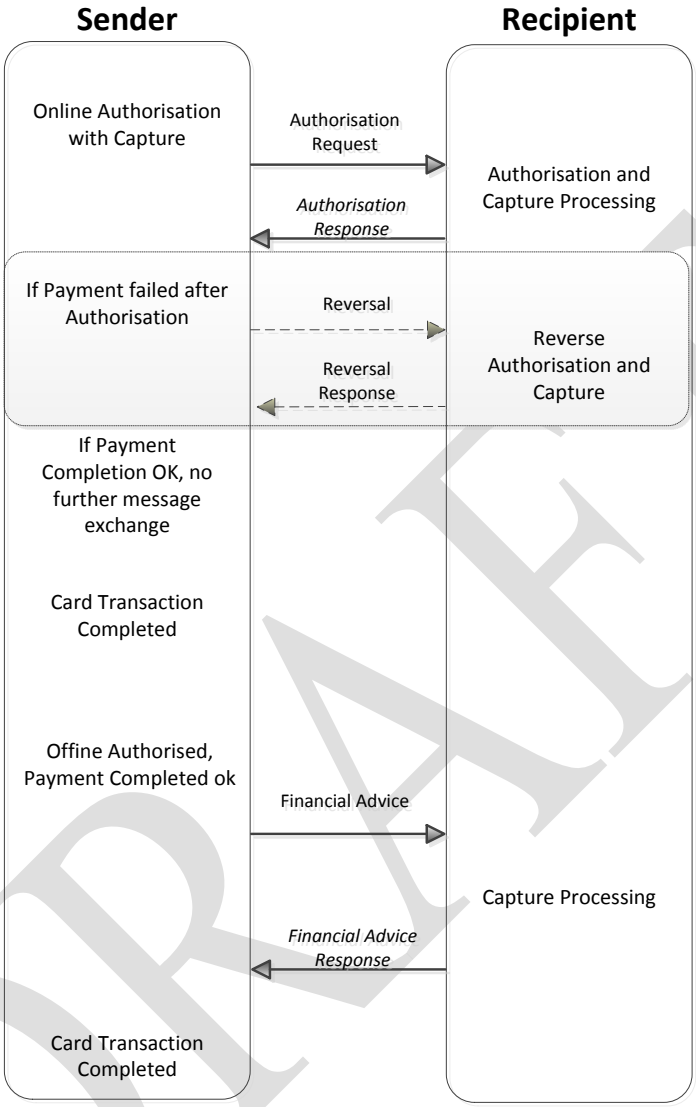


FIGURE 9: MODE 3

DRAFT

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 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	SDA optional from 2020[4] 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 10: Local Transaction Contact Payment - Acceptance Characteristics

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

DRAFT

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 Offline with Online capability Card: DDA and CDA required for all newly issued and replacement cards Online only Card: DDA and CDA required for all newly issued and replacement cards, if the card supports Offline PIN	
Cardholder Verification Method	PIN mandatory	"No CVM Required" mandatory[5]

Table 11: 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 12: Card Services - Volume Conformant Implementations for attended

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

Table 13: Card Services - Volume Conformant Implementations for unattended

[5] 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.

DRAFT

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.

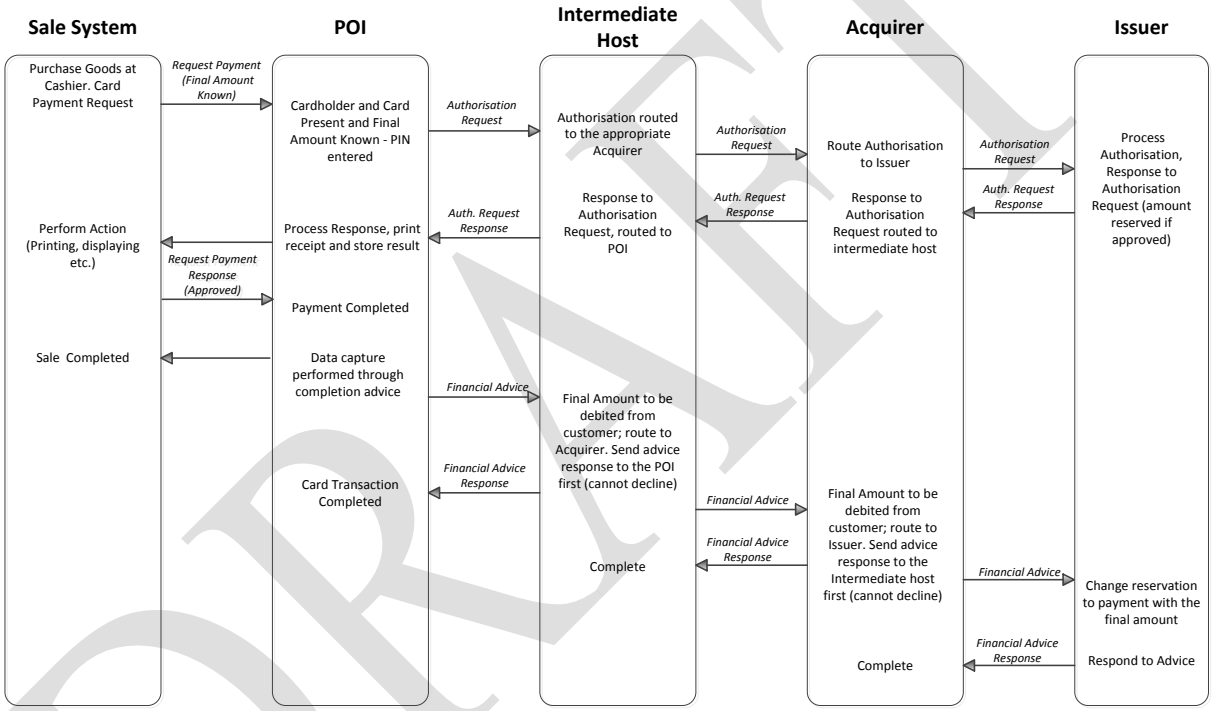


FIGURE 14: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

DRAFT

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

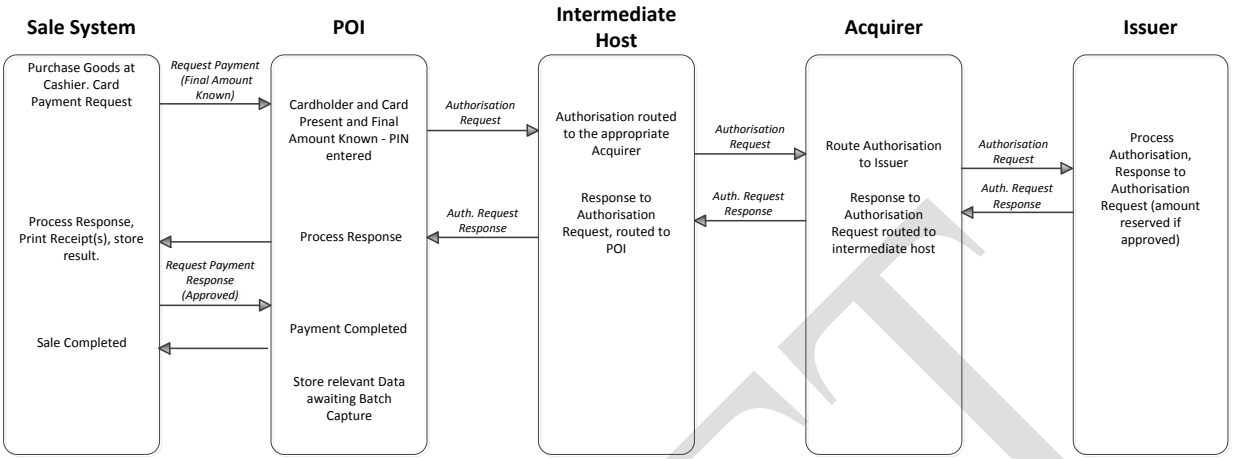


FIGURE 15: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

DRAFT

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 is PIN and final amount known. Capture immediately after transaction completion.

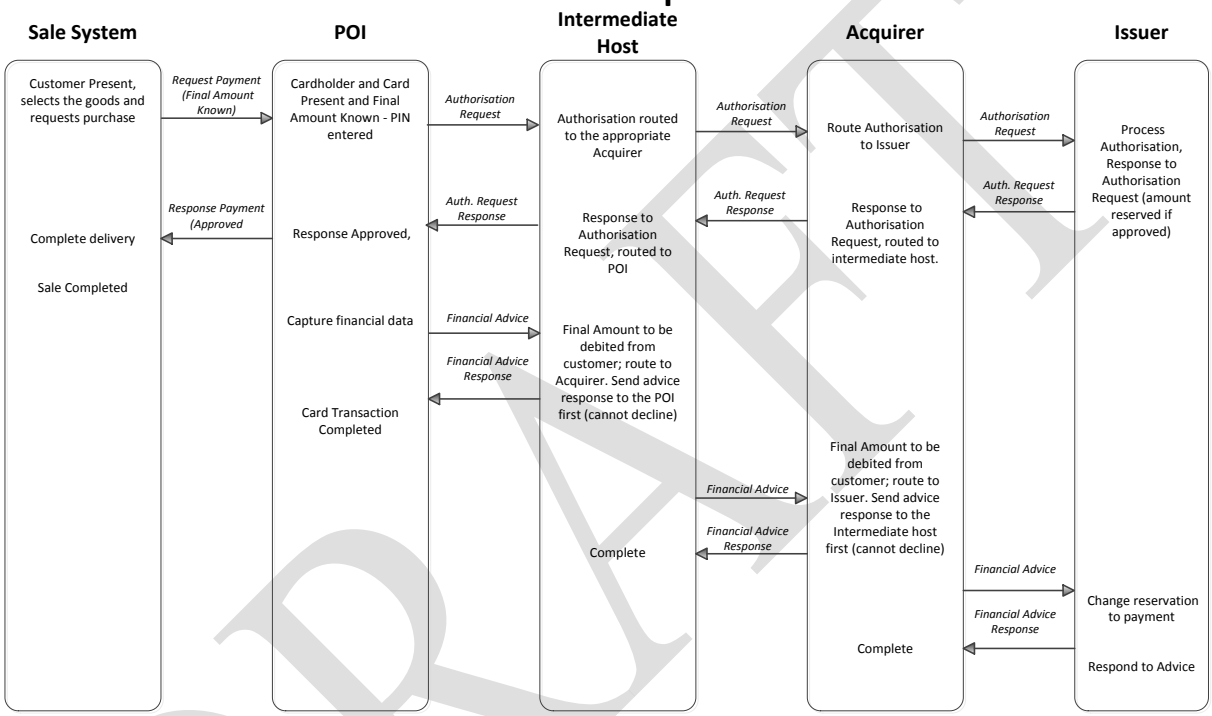


Figure 16: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION IS PIN AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

DRAFT

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

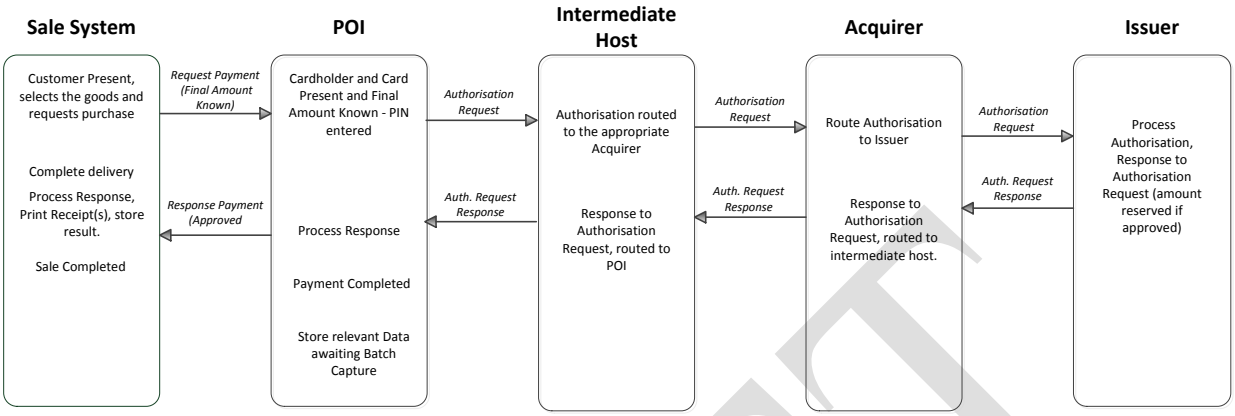


Figure 17: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION IS PIN AND FINAL AMOUNT KNOWN, CAPTURE BY BATCH

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.

DRAFT

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

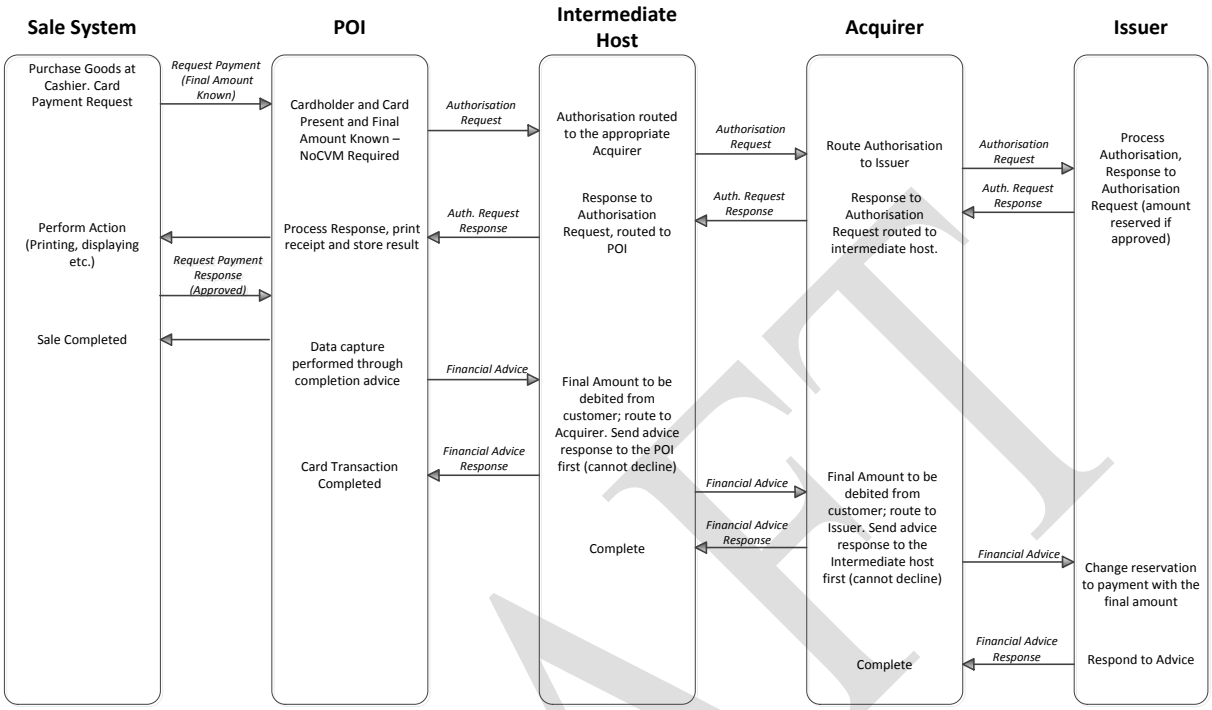


Figure 18: Example Flow: Payment with 'No CVM Required' in unattended environment, Cardholder present and final amount known. Capture immediately after Transaction Completion.

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

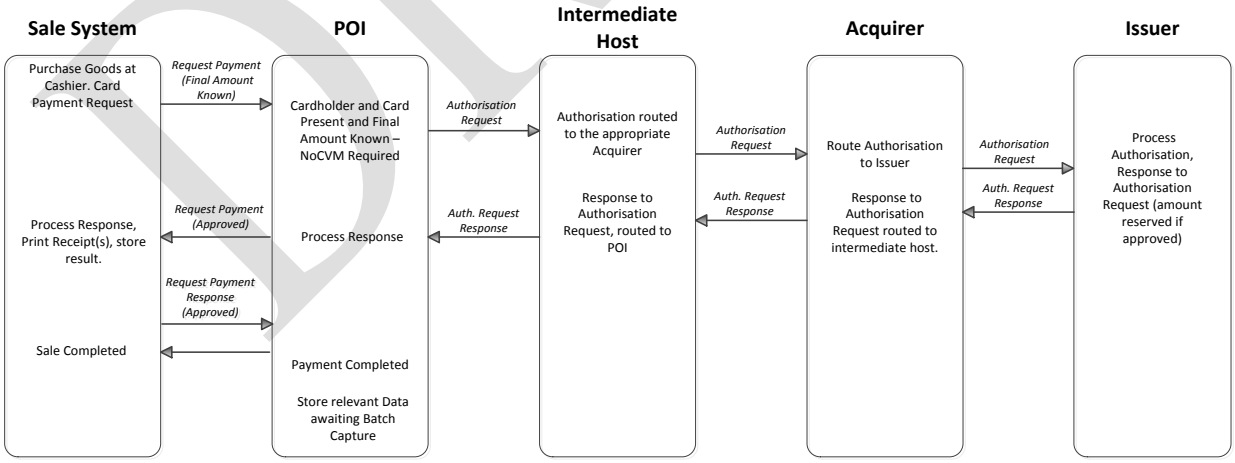


Figure 19: Example Flow: Payment with 'No CVM Required' in attended or unattended environment, Cardholder present and final amount known. Capture by Batch.

DRAFT

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	Low value 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[6]		
Attendant Present	Y	N	
EMV Online Authentication.	Required		
EMV Offline Card Authentication	SDA optional from 2020[7] 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 20: Local Transaction Deferred Payment - Acceptance Characteristics

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

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

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

DRAFT

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 or partial approval when the cardholder has insufficient balance 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, as described in Book 2 T185, to cater for 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 not erroneously impact the "Cardholder Available Funds".

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

DRAFT

Table 21: 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.

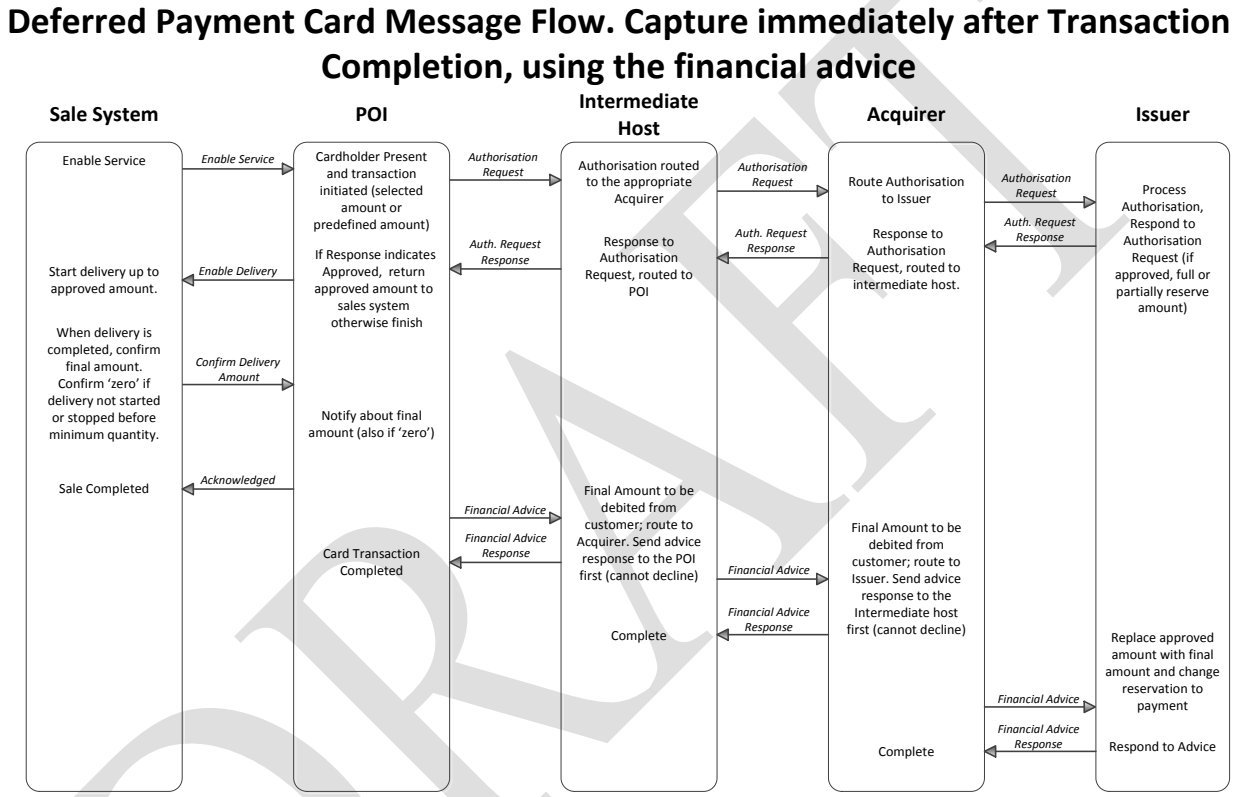
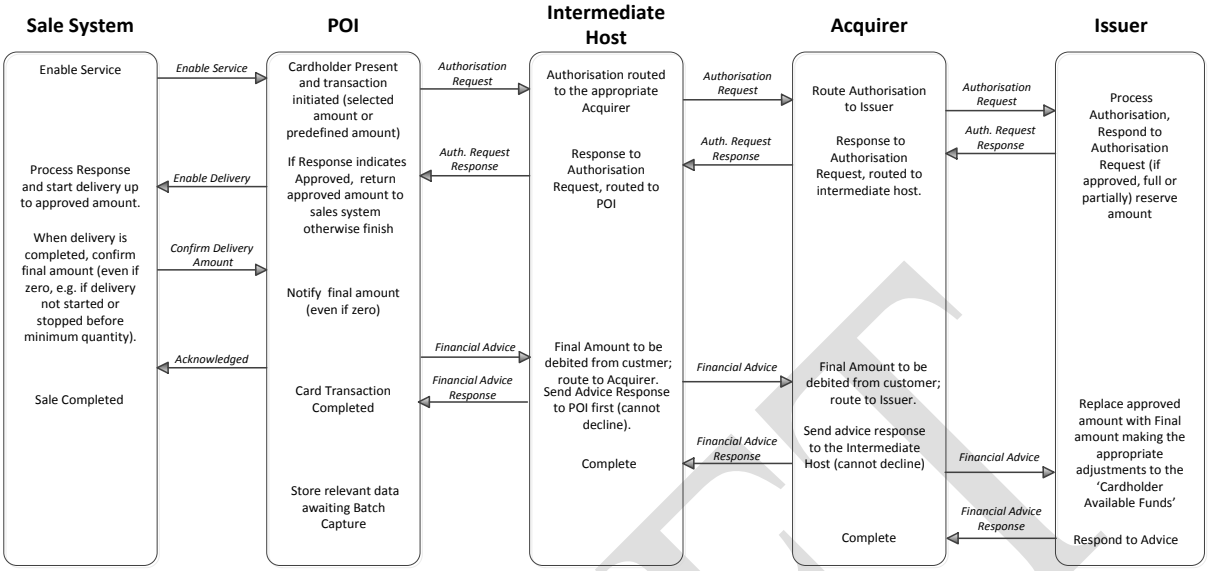


FIGURE 22: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

DRAFT

Deferred Payment Card Message Flow, Capture by Batch.



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

FIGURE 23: 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.

DRAFT

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

DRAFT

Characteristics of the context	Attended	Unattended
Acceptance Technology for Pre-Authorisation	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[8] 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 24: Local Transaction Pre-Authorisation and Update Pre-Authorisation Service - Acceptance Characteristics

Characteristics of the context	Attended	Unattended
Acceptance Technology for Pre-Authorisation	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[9]	
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 25: Local Transaction Payment Completion Service - Acceptance Characteristics

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

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

DRAFT

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

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 or the Update Pre Authorisation service.

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)[10] 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.
    - Or 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 is within the configured overspend percentage amount allowed by some scheme rules.

  Or

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

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

DRAFT

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

Issuers may approve the full amount or a partial amount for both Pre-Authorisation and update Pre-Authorisation when the amount is being incremented.

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.

DRAFT

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 26: 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.

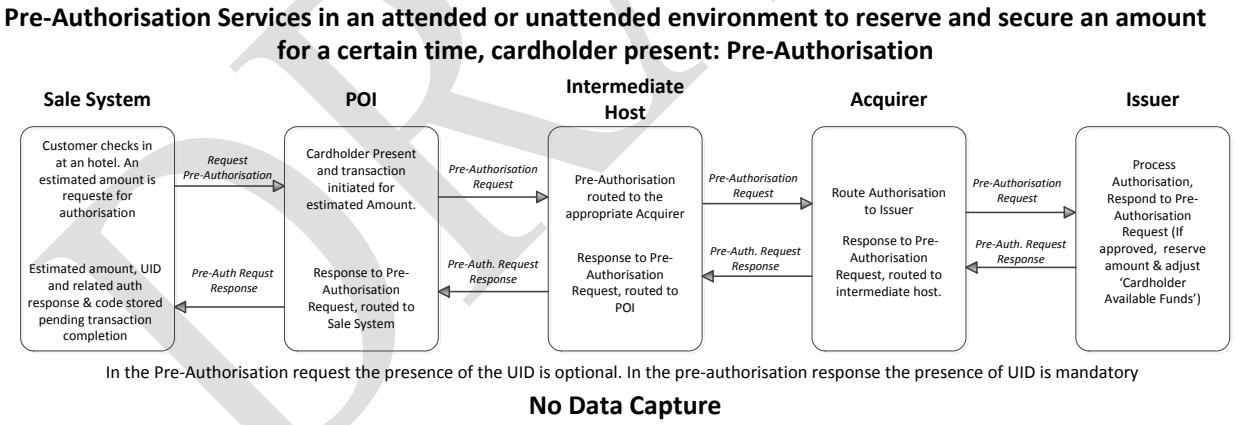
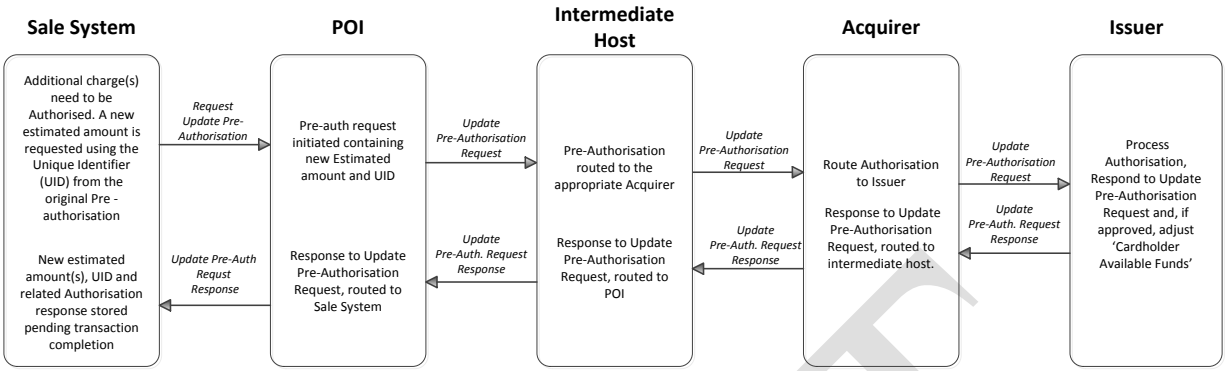


Figure 27: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT FOR A CERTAIN TIME, CARDHOLDER PRESENT: PRE-AUTHORISATION

DRAFT

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

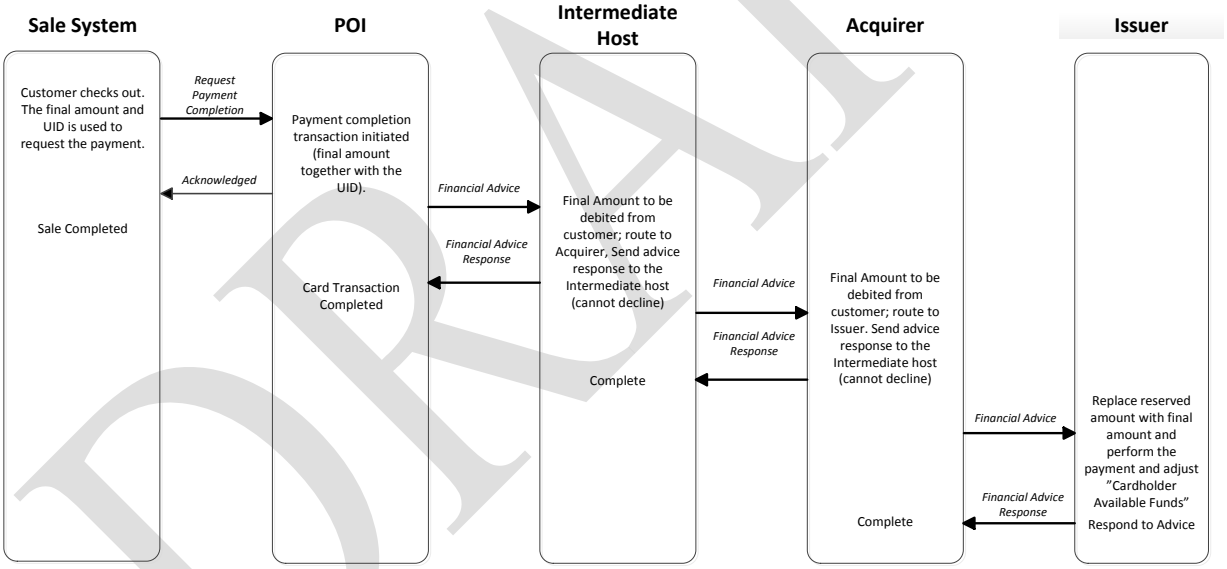


In the Update Pre-Authorisation request and response the presence of the UID is mandatory.

No Data Capture

Figure 28: 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 29: Example Flow: Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount: Payment Completion. Capture immediately after Transaction Completion

DRAFT

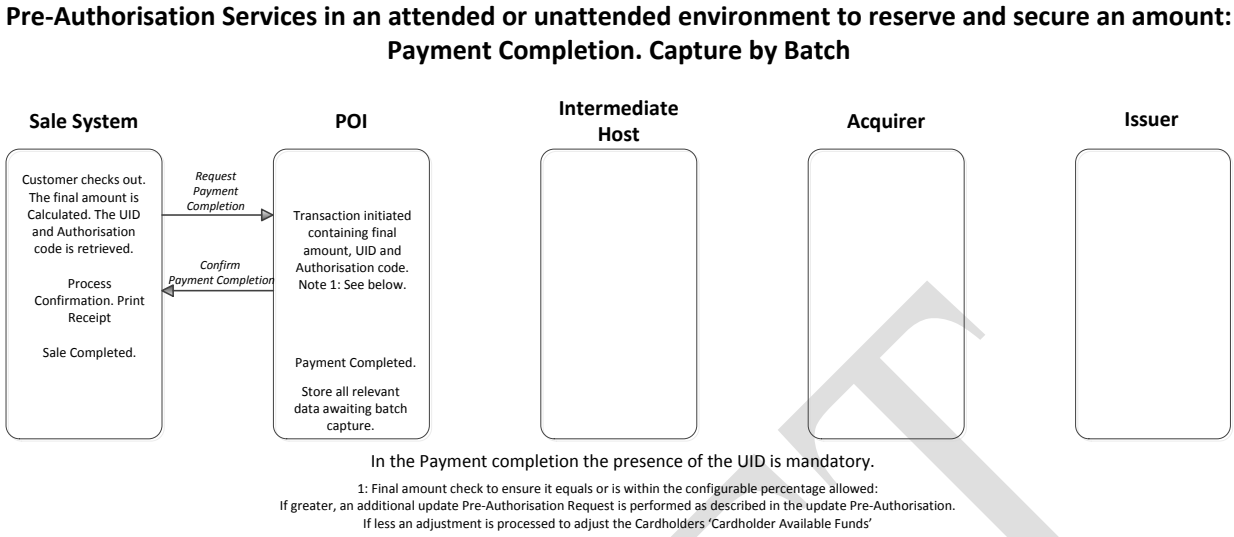


Figure 30: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE BY BATCH

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	

DRAFT

Characteristics of the context	Attended	Unattended
EMV Offline 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	Online PIN Offline Mobile Code No CVM Required

Table 31: 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 32: 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 33: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

DRAFT

Table 34: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR UNATTENDED

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

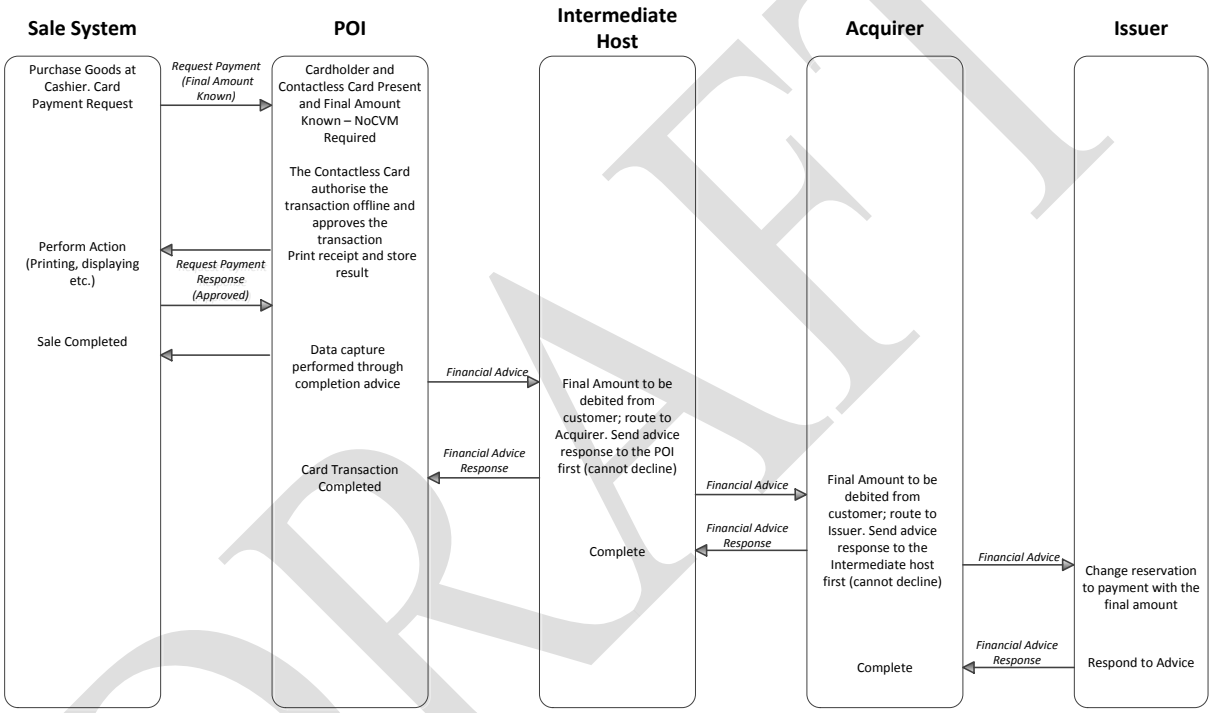


Figure 35: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION)WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

DRAFT

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

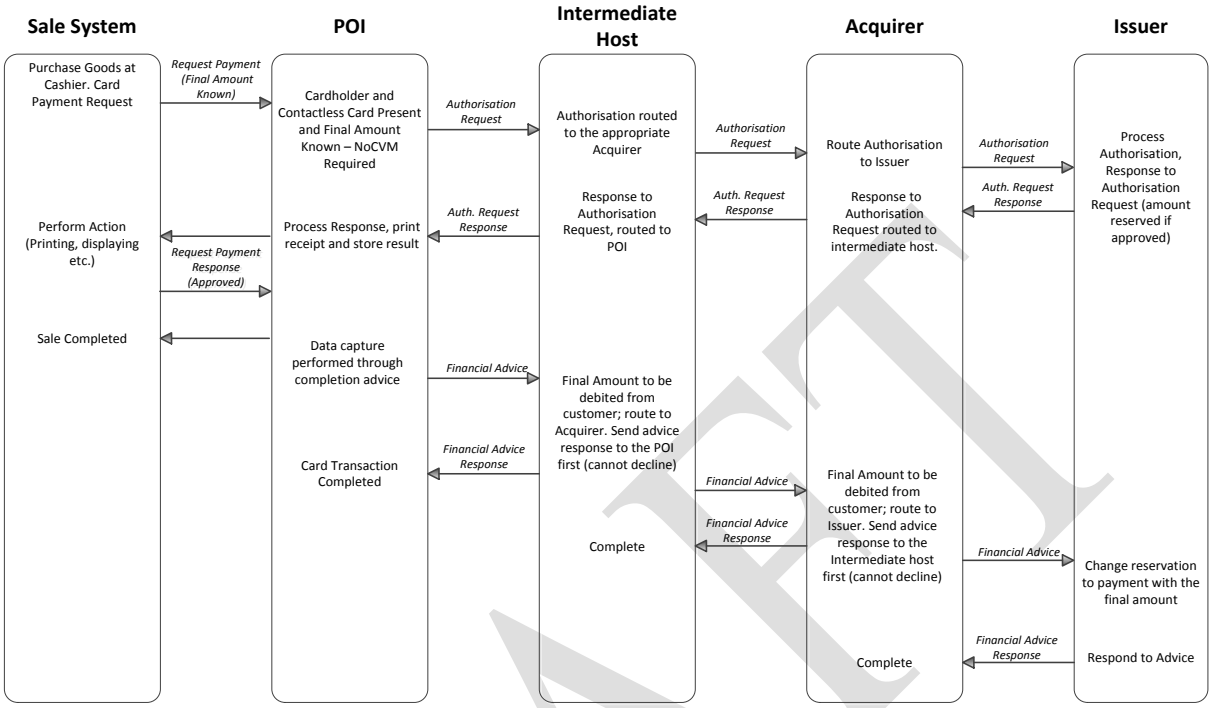


Figure 36: Example Flow: Contactless Payment (Online Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture immediately after Transaction Completion

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

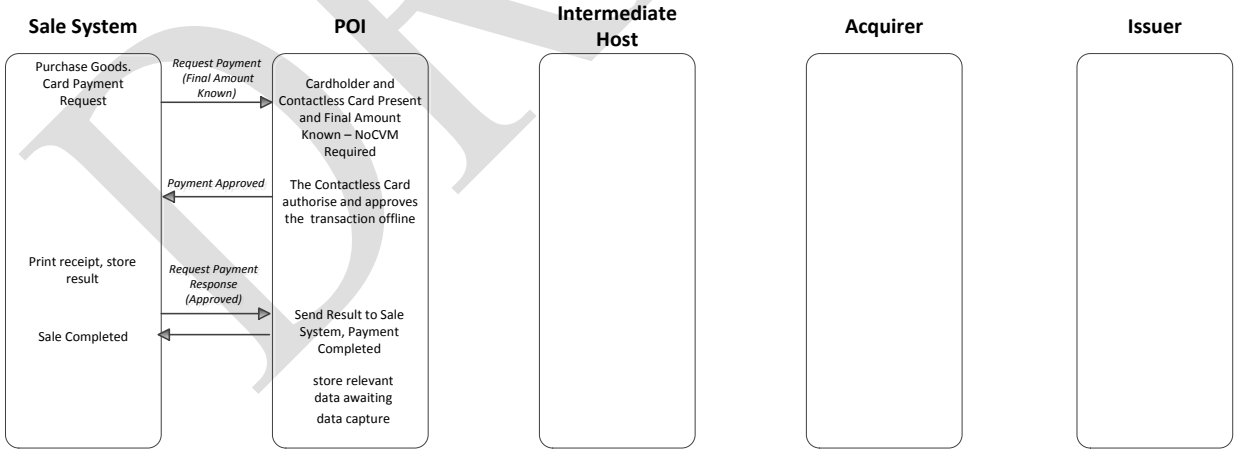


Figure 37: Example Flow: Contactless Payment (Offline Authorisation) with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known. Capture by Batch

DRAFT

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

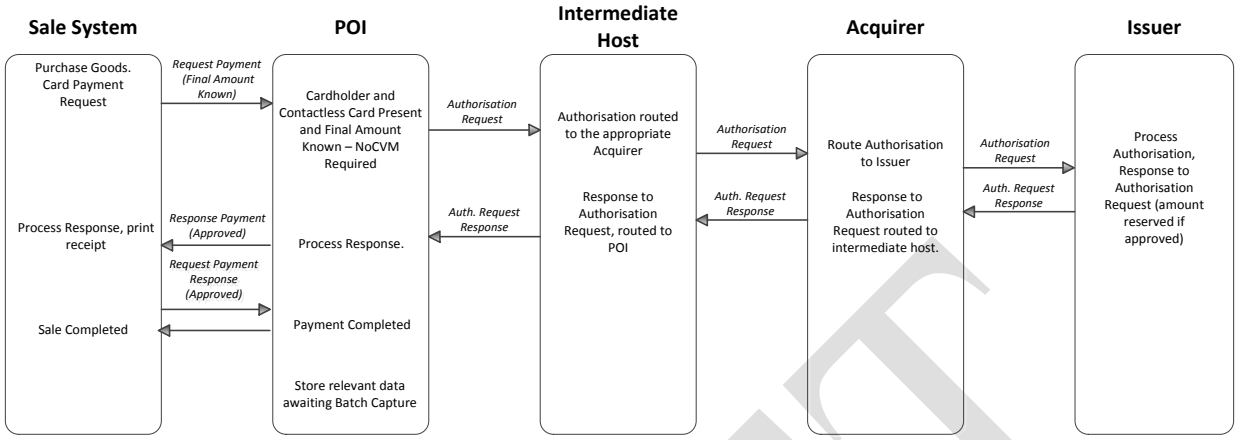


Figure 38: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH

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 contains 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 a so-called 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	

DRAFT

Characteristics of the context	Virtual POI	
	with Cardholder Verification	without Cardholder Verification
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][12], 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	

[11] 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]

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

DRAFT

Characteristics of the context	Virtual POI	
	with Cardholder Verification	without Cardholder Verification
Card Authentication	Static authentication for low risk payments (see [EBA]) Dynamic Authentication[13]	
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

614 *3.2.1.2. Card services*

615

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

616 Table 39: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

617

[13] 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]

DRAFT

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[14]		Mobile Contactless Single tap/Double Tap

The use cases provided below 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.

[14] With appropriate risk management in the MCP Application

DRAFT

4.1. Contactless

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

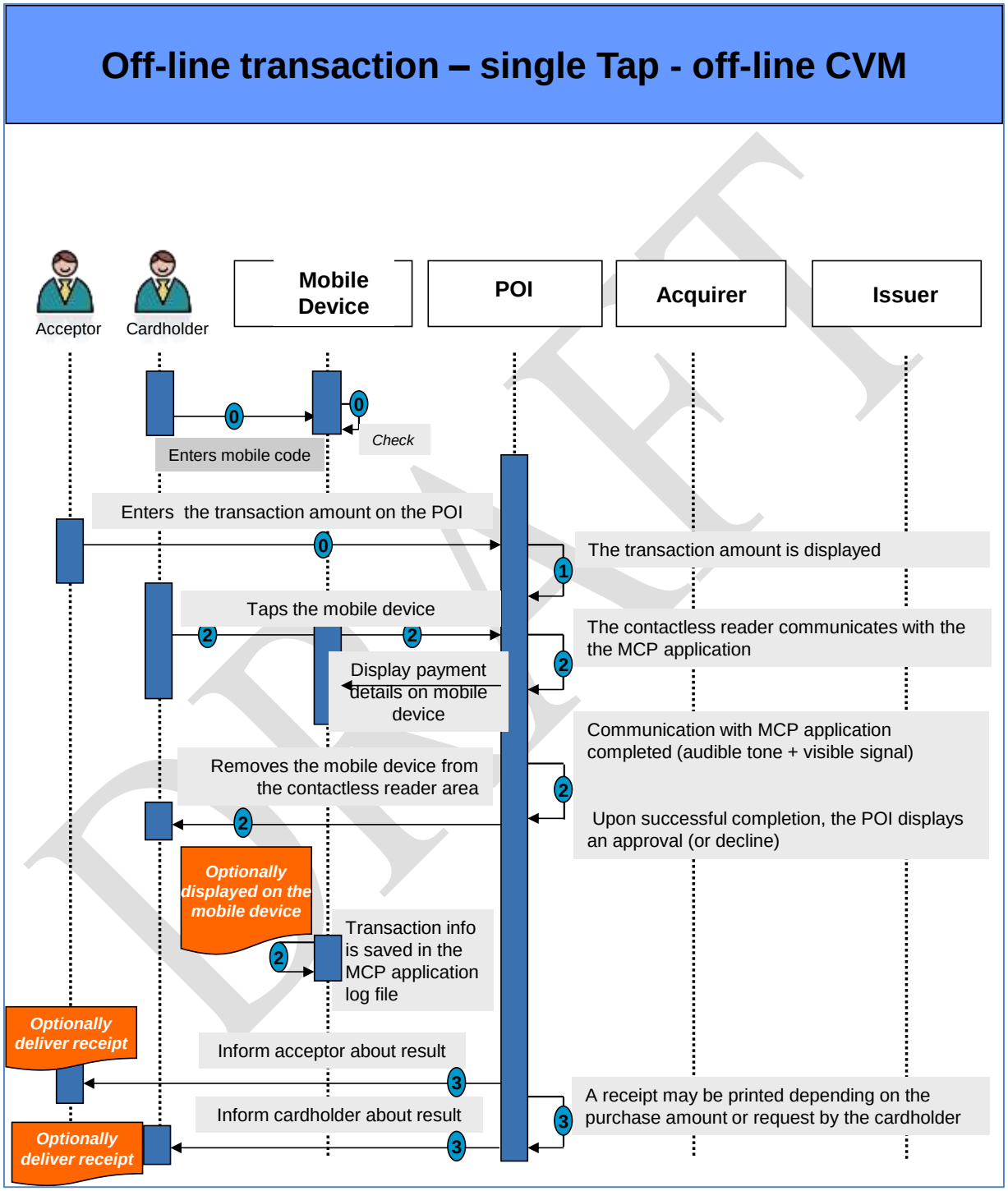


Figure 40: Single Tap - off-line transaction - off-line CVM

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 cardholder is invited to enter his/her 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 selects the contactless technology 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.

DRAFT

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

DRAFT

4.1.2. Use case 2: Mobile Contactless - Double Tap - Off-line transaction – Off-line CVM

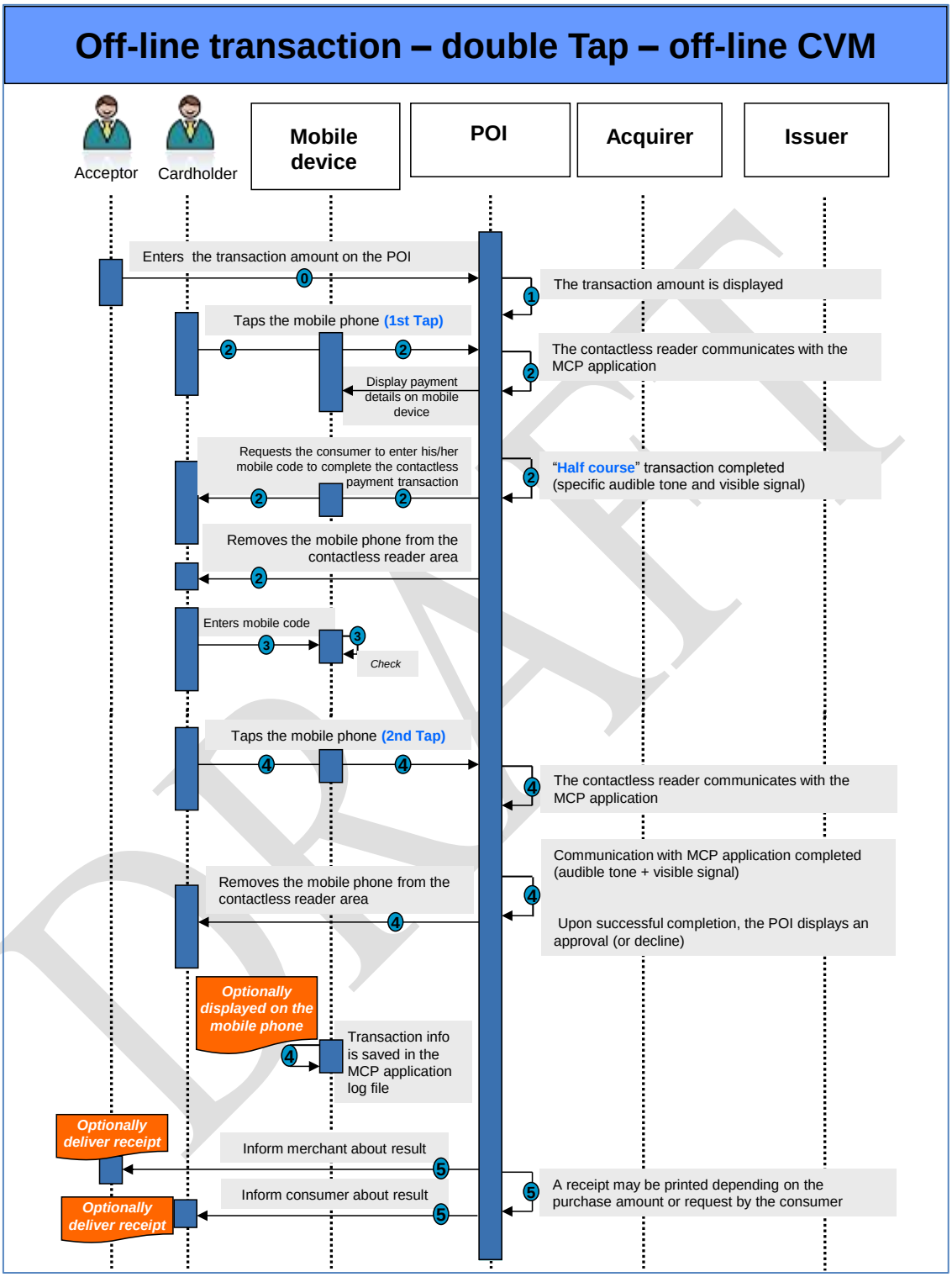


Figure 41: Double Tap - Off-line transaction – Offline CVM

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 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 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 "half-course" transaction is completed and that the cardholder is requested to enter his/her 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.

DRAFT

- 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 merchant'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 merchant is informed about result of the transaction.
- The cardholder is informed about result of the transaction.
- Depending on the purchase amount, the merchant's POI terminal features and cardholder choice, a transaction receipt may be printed.

DRAFT

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

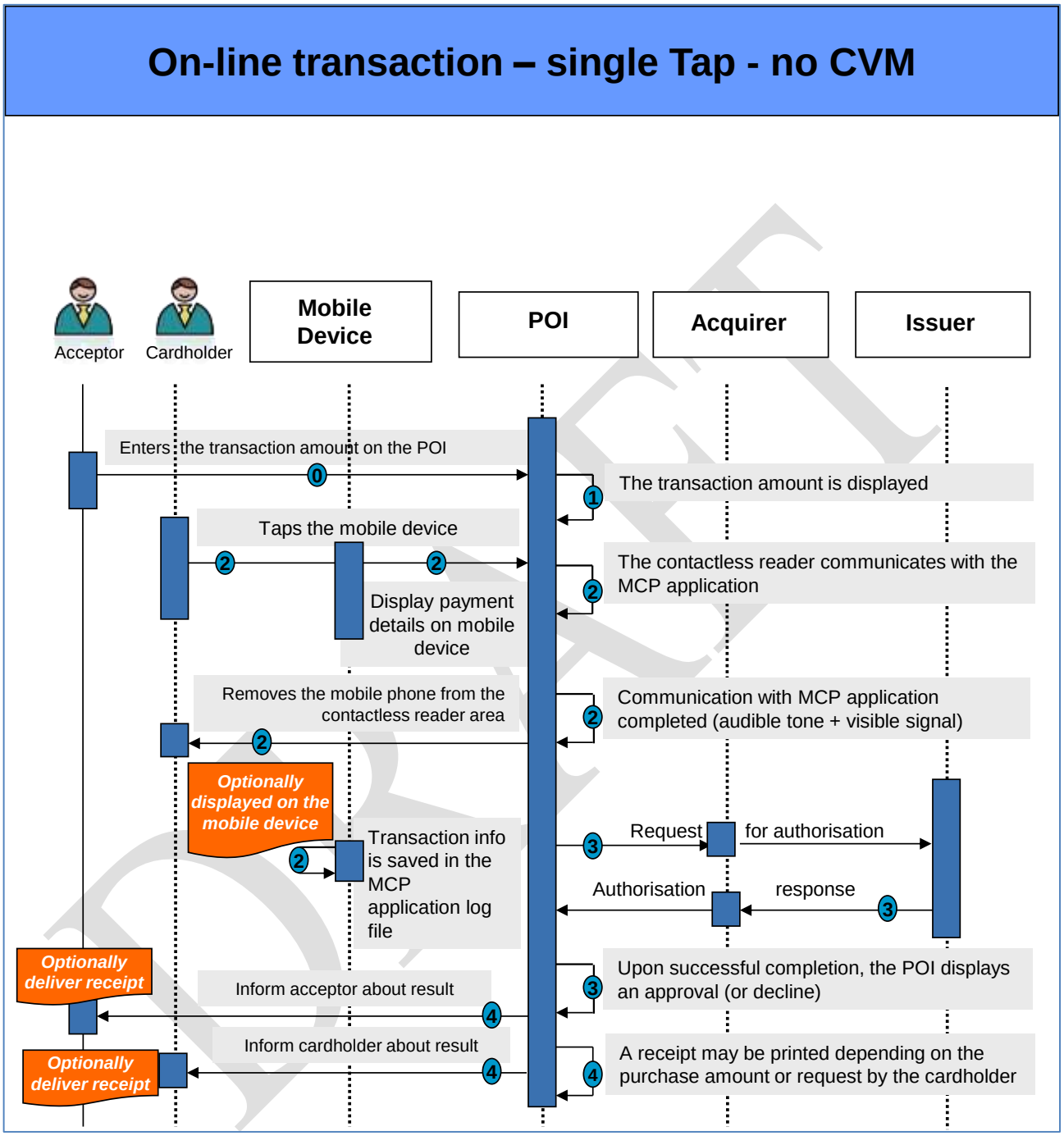


Figure 42: Single Tap - On-line transaction – no CVM

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

DRAFT

- 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.

DRAFT

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

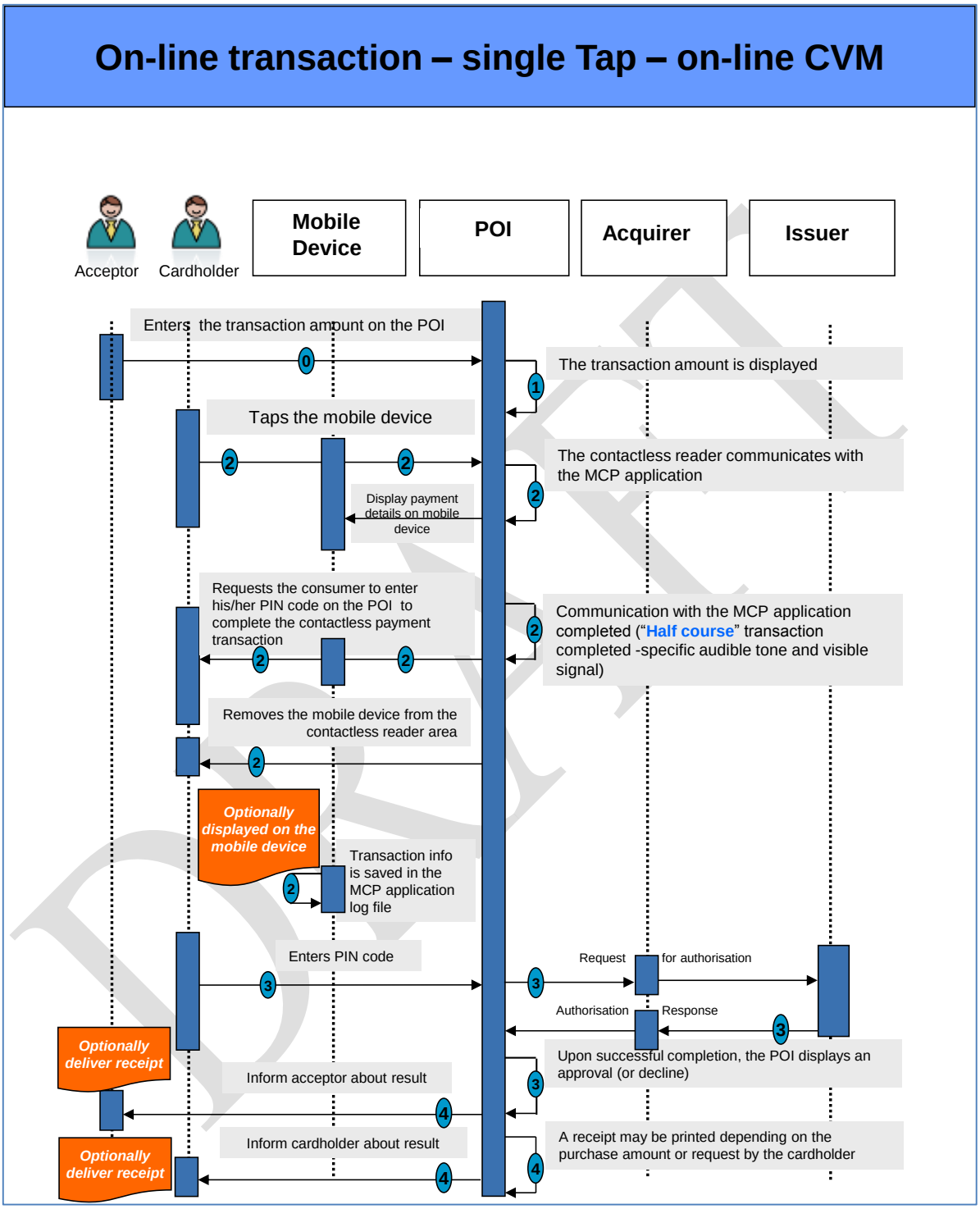


Figure 43: Single Tap - On-line transaction – On-line CVM

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.

DRAFT

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.

DRAFT

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

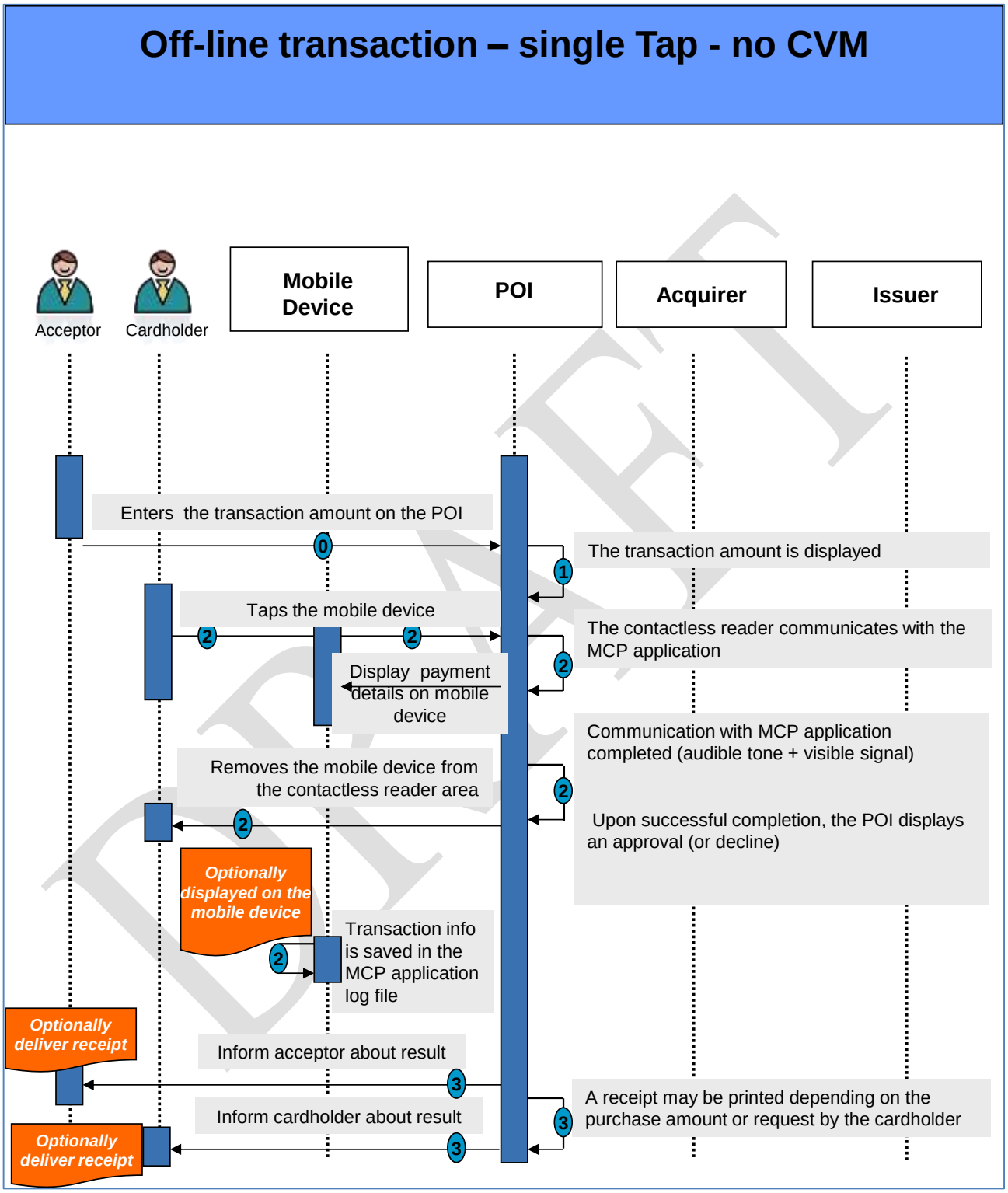


Figure 44: Single Tap - Off-line transaction - no CVM

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[15] 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.

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

DRAFT

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

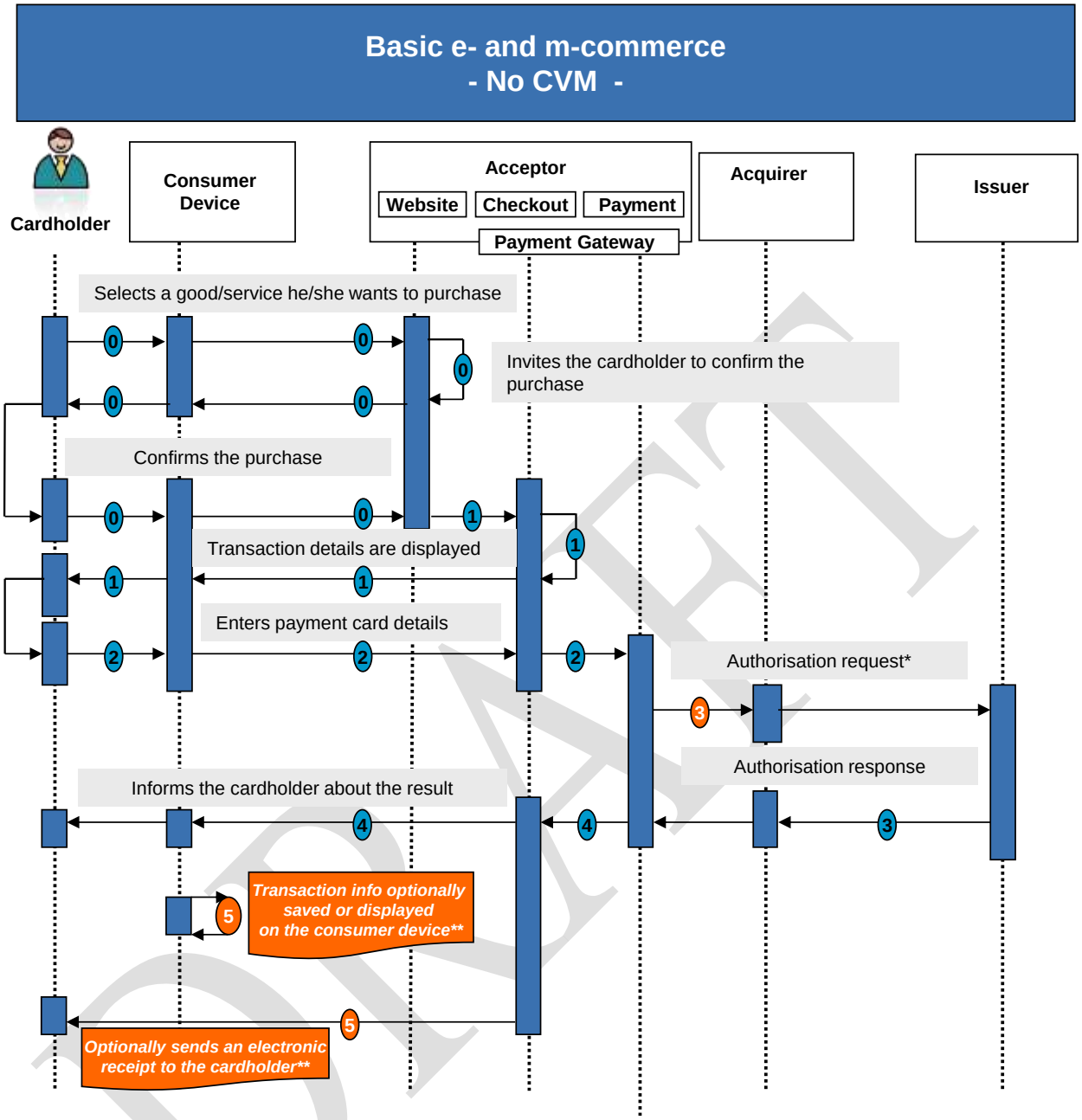
Note: A similar use case can be described for an offline contactless card transaction (single brand) with "no CVM".

4.2. E and m commerce

4.2.1. Basic e- and m-commerce - 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 "basic" scenario, no CVM method is used.

DRAFT



*Authorisation request is optional if an (M)RP Application is present in the consumer device
**Implementation dependent

Figure 45: Basic e- and m-commerce - 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 typically16 involves an on-line authorisation request by the acceptor to the issuer.

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;
- 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 sent by the acceptor to the cardholder.

[16] 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.

DRAFT

4.2.2. Secured e- and m-commerce - Strong 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 "strong dynamic authentication method", i.e. a combination of card authentication with a CVM.

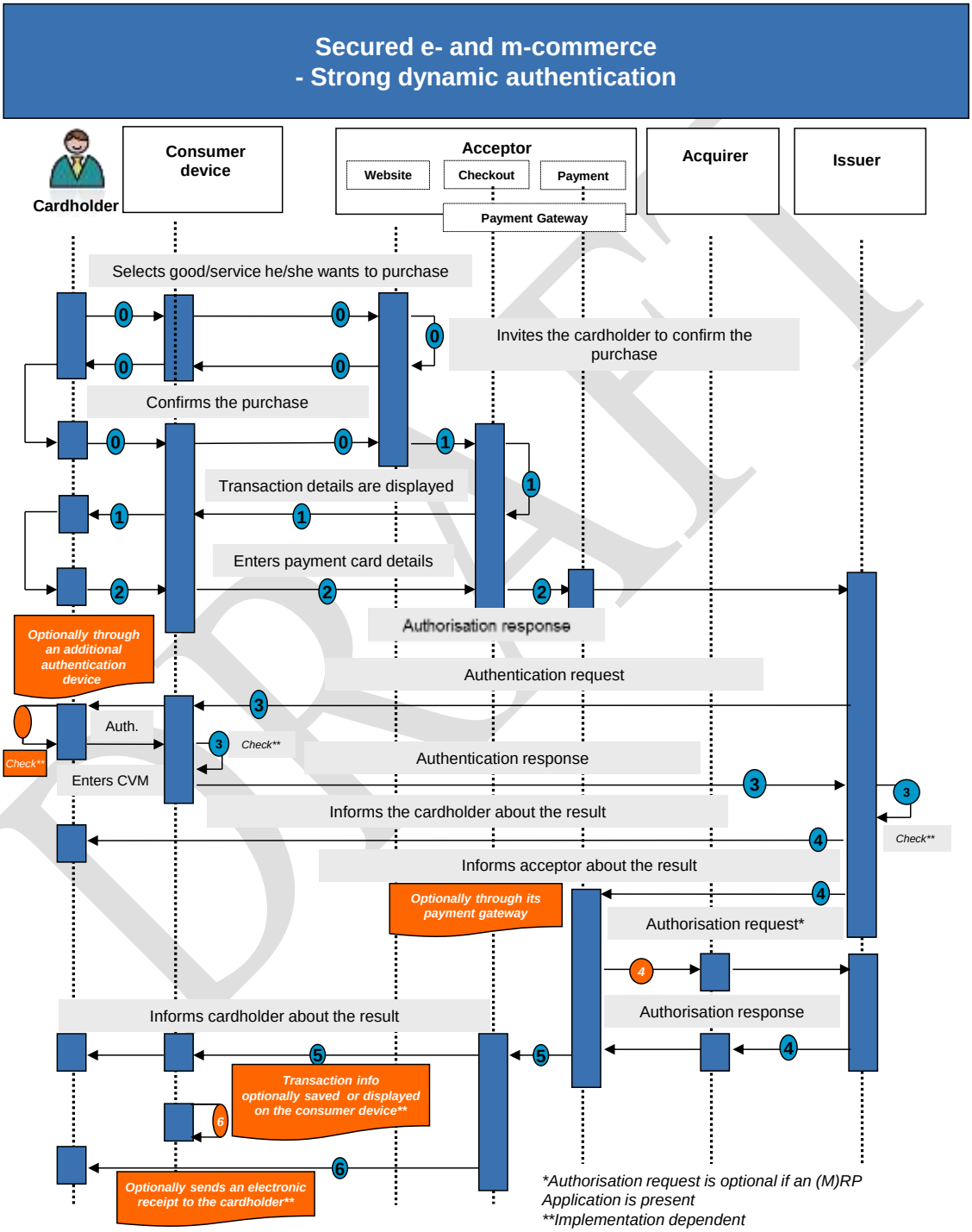


Figure 46: Secured e- and m-commerce - Strong dynamic authentication

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) [17]

The cardholder and the relevant data are subsequently authenticated[18] towards the issuer19 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 strong dynamic authentication method. Various methods may exist involving the usage of an additional authentication device. 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 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

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

[18] This authentication may involve transaction details.

[19] Or a TPP in the issuer domain.

DRAFT

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 typically20 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.

DRAFT

[20] 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

Figure 1: Example: Choice of Application in the case of Acceptor pre-selection with signature as CVM and without displaying the final amount 9

Figure 2: Example: Choice of Application in the case of Acceptor pre-selection that includes the total amount and PIN entry. 9

Figure 3: Example: Override Option Using an Upfront Selection Screen on the POI 10

Figure 4: Example: Choice of Application by the sole Cardholder among all mutually supported applications 12

Figure 5: Example: Choice of Application by the sole Cardholder after having selected their preferrable application 12

Table 6: Volume conformant cardholder verification method (acceptance) 15

Figure 7: Mode 1 17

Figure 8: Mode 2 18

Figure 9: Mode 3 19

Table 10: Local Transaction Contact Payment - Acceptance Characteristics 20

Table 11: Local Transaction Contact Payment - Issuance Characteristics 21

Table 12: Card Services - Volume Conformant Implementations for attended 21

Table 13: Card Services - Volume Conformant Implementations for unattended 21

Figure 14: Example Flow: Payment in attended environment, Cardholder is present, Cardholder Verification performed and final amount known. Capture immediately after Transaction Completion 22

Figure 15: Example Flow: Payment in attended environment, Cardholder is present, Cardholder Verification performed and final amount known. Capture by Batch. 23

Figure 16: Example Flow: Payment in unattended environment, Cardholder is present, Cardholder Verification is PIN and final amount known. Capture Immediately after Transaction Completion 24

Figure 17: Example Flow: Payment in unattended environment, Cardholder is present, Cardholder Verification is PIN and final amount known, Capture by Batch 25

Figure 18: Example Flow: Payment with 'No CVM Required' in unattended environment, Cardholder present and final amount known. Capture Immediately after Transaction Completion. 26

Figure 19: Example Flow: Payment with 'No CVM Required' in attended or unattended environment, Cardholder present and final amount known. Capture by Batch. 26

Table 20: Local Transaction Deferred Payment - Acceptance Characteristics 27

Table 21: Payment services - Volume Conformant Implementation 29

Figure 22: Example Flow: Deferred Payment Card Message Flow, Capture immediately after Transaction Completion 29

Figure 23: Example Flow: Deferred Payment Card Message Flow, Capture by Batch 30

DRAFT

Table 24: Local Transaction Pre-Authorisation and Update Pre-Authorisation Service - Acceptance Characteristics 32

Table 25: Local Transaction Payment Completion Service - Acceptance Characteristics 32

Table 26: Card services - Volume Conformant Implementations 35

Figure 27: Example Flow: Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount for a certain time, cardholder present: Pre-Authorisation 35

Figure 28: Example Flow: Pre-Authorisation Services in an attended or unattended environment to reserve an estimated amount: Update Pre-authorisation 36

Figure 29: Example Flow: Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount: Payment Completion. Capture immediately after Transaction Completion 36

Figure 30: Example Flow: Pre-Authorisation Services in an attended or unattended environment to reserve and secure an amount: Payment Completion. Capture by Batch 37

Table 31: Local Transaction Contactless Payment - Acceptance Characteristics 38

Table 32: Local Transaction Contactless Payment - Issuance Characteristics 38

Table 33: Card Services - Volume Conformant Implementations for attended 38

Table 34: Card Services - Volume Conformant Implementations for unattended 39

Figure 35: 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 39

Figure 36: 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 40

Figure 37: 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 40

Figure 38: 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 41

Table 39: Card Services - Volume Conformant Implementations 43

Figure 40: Single Tap - off-line transaction - off-line CVM 45

Figure 41: Double Tap - Off-line transaction – Offline CVM 48

Figure 42: Single Tap - On-line transaction – no CVM 51

Figure 43: Single Tap - On-line transaction – On-line CVM 54

Figure 44: Single Tap - Off-line transaction - no CVM 57

Figure 45: Basic e- and m-commerce - No CVM 60

Figure 46: Secured e- and m-commerce - Strong dynamic authentication 62

DRAFT

DRAFT