EPC020-08 08.12.2015

(Vol Ref. 7.6.2.1)

**SEPA CARDS STANDARDISATION (SCS) "VOLUME"**

# 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 | EPC020-08 |
| Issue | Book 7.6.2.1 |
| Date of Version | 08 December 2015 |
| Reason for Issue | Publication |
| Reviewed by | Approved for publication by the EPC Board of 19 November 2015 and endorsed by the CSG GM of 10 November 2015 |
| Produced by | CSG Secretariat |
| Owned and Authorised 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 |

## 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.

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;
- 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, these are:

1. Cardholder present Payment in attended environment, Cardholder Verification performed and final amount known;
2. Cardholder present Payment in an unattended environment, Cardholder Verification performed and final amount known;
3. Cardholder present Payment in attended and unattended environment, "No CVM Required" and final amount known;
4. Deferred Payments in an attended and unattended environment with an estimated amount at payment initiation, Cardholder is present with cardholder verification;
5. Pre-Authorisation Services in an attended and unattended environment to reserve an amount, Cardholder present;

6. Basic e-commerce payment using static authentication and 3 domain security;
7. Contactless payment with no Cardholder Verification Method required in attended and unattended environment, Cardholder is present and final amount known.

Additional contexts will be described in future versions of this document, including for example transit payments or 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:

- Current requirements and implementation options;
- Future Volume conformant requirements and implementation options with roadmaps for implementing the options by a given date.

## 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:

1. Contexts added:
    a. Basic e-commerce payment using static authentication and 3 domain security.
    b. Contactless payment with no Cardholder Verification Method required in attended and unattended environment, Cardholder is present and final amount known.
2. Section 2.5 on Security and Functional certification has been reworked and now no longer contains a migration roadmap for a harmonised terminal security certification evaluation methodology.
3. Guidance on Choice of the Application.

# 2 GENERAL IMPLEMENTATION GUIDELINES

## 2.1 Introduction

Books 2 to 5 describe general requirements for card payments with a view to harmonising common implementation options for future implementations. Currently, this section describes common implementation requirements valid for all Local contact transactions for the following topics:

- Card Data Authentication Methods;
- PIN Based Cardholder Verification Methods;
- Data Capture.

In addition, this section covers guidance on the implementation of Choice of Application for Local and Remote Transactions.

## 2.2 Card Data Authentication Method

DDA is the minimum card data authentication method in SEPA. The objective is to cease support of SDA.

### 2.2.1 Card Data Authentication Method (Issuance)

#### *2.2.1.1 Current Implementations*

| | SDA | DDA | CDA |
|---|---|---|---|
| **Online only cards** | Optional | Optional | Optional |
| **Offline with online capability cards** | Optional | Required | Optional |

TABLE 1: CURRENT CARD DATA AUTHENTICATION METHOD (ISSUANCE)

#### 2.2.1.2 *Volume Conformant Implementation*

| | SDA | DDA | CDA |
|---|---|---|---|
| **Online only cards**[1] | Not Permitted for all newly issued and replacement cards 2018 | Required for all newly issued and replacement cards 2018 | Required for all newly issued and replacement cards 2018 |
| **Offline with online capability cards** | Not Permitted for all newly issued and replacement cards | Required for all newly issued and replacement cards | Required for all newly issued and replacement cards 2018 |

TABLE 2: VOLUME CONFORMANT CARD DATA AUTHENTICATION METHOD (ISSUANCE)

Note:

- For issuance, all SEPA cards shall support DDA and CDA and shall not support SDA in the future;
- Since offline enciphered PIN is mandated for online only cards supporting PIN, it is not an additional technology requirement to mandate DDA and CDA.

### 2.2.2 Card Data Authentication Method (Acceptance)

#### 2.2.2.1 *Current Implementations*

| | SDA | DDA | CDA | OMA |
|---|---|---|---|---|
| **Online only terminals** | Optional | Optional | Optional | Required |
| **Offline with online capability terminals** | Required | Required | Optional | Required |

TABLE 3: CURRENT CARD DATA AUTHENTICATION METHOD (ACCEPTANCE)

[1] If the card supports PIN.

#### 2.2.2.2 *Volume Conformant Implementation*

| | SDA | DDA | CDA | OMA |
|---|---|---|---|---|
| **Online only terminals** | Optional from 2020 (not used for SEPA cards)[2] | Optional | Optional (Recommended) | Required |
| **Offline with online capability terminals** | Optional from 2020 (not used for SEPA cards)[2] | Required | Required for newly installed terminals as of 2015 | Required |

TABLE 4: VOLUME CONFORMANT CARD DATA AUTHENTICATION METHOD (ACCEPTANCE)

[2] SDA is still required by some non-SEPA general purpose Card Schemes.

## 2.3 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.

### 2.3.1 PIN Based Cardholder Verification Methods (Issuance)

#### *2.3.1.1 Current Implementations*

There are no mandatory requirements to support a specific CVM from an issuer perspective however within the SEPA area PIN is the recommended method.

#### *2.3.1.2 Volume Conformant Implementation*

| | **Offline Plaintext PIN** | **Offline enciphered PIN** | **Online PIN** |
|---|---|---|---|
| **Online only cards** | Not used within SEPA as of 2018 | Required for newly issued or replacement cards as of 2018 | Required |
| **Offline with online capability cards** | Not used within SEPA as of 2018 | Required for newly issued or replacement cards as of 2018 | Required |

TABLE 5: VOLUME CONFORMANT CARDHOLDER VERIFICATION METHOD (ISSUANCE)

Note:

- The above guidelines only apply if the card supports PIN as CVM;
- Offline Plaintext PIN may still be present in the CVM list for use outside SEPA, but only with a lower priority than offline enciphered PIN and online PIN.

### 2.3.2 PIN Based Cardholder Verification Methods (Acceptance)

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

#### *2.3.2.1 Current Implementations*

| | Offline Plaintext PIN | Offline enciphered PIN | Online PIN |
|---|---|---|---|
| **Online only terminals** | Conditional[3] | Conditional[3] | Conditional[3] |
| **Offline with online capability terminals** | Required[4] | Required | Optional[4] |

TABLE 6: CURRENT CARDHOLDER VERIFICATION METHOD (ACCEPTANCE)

#### *2.3.2.2 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[3] | Conditional[3] |
| **Offline with online capability terminals** | Not used for SEPA Cards and shall not be mandatory on the POI from 2020 | Required | Optional[4] |

TABLE 7: VOLUME CONFORMANT CARDHOLDER VERIFICATION METHOD (ACCEPTANCE)

[3] Either

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

[4] Currently only required for some debit brands.

## 2.4 Data Capture

### 2.4.1 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.

### 2.4.2 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.

### 2.4.3 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.

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

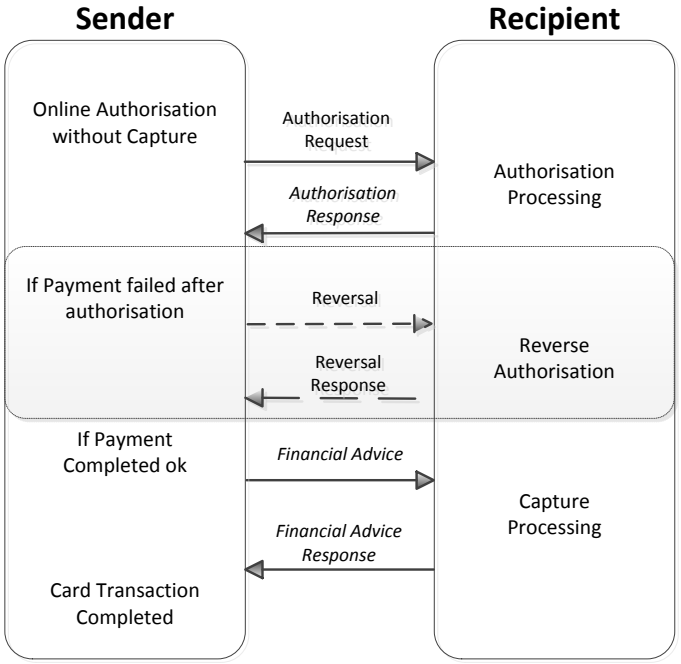



FIGURE 8: MODE 1

# Mode 2: Online Authorisation, Capture by Batch

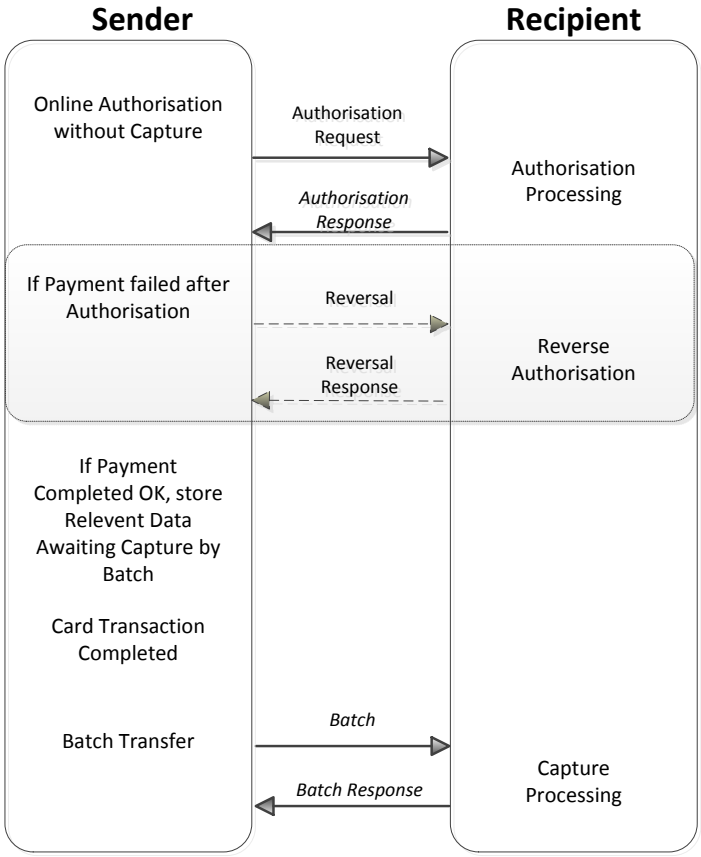



FIGURE 9: MODE 2

# Mode 3: Online Authorisation with Capture

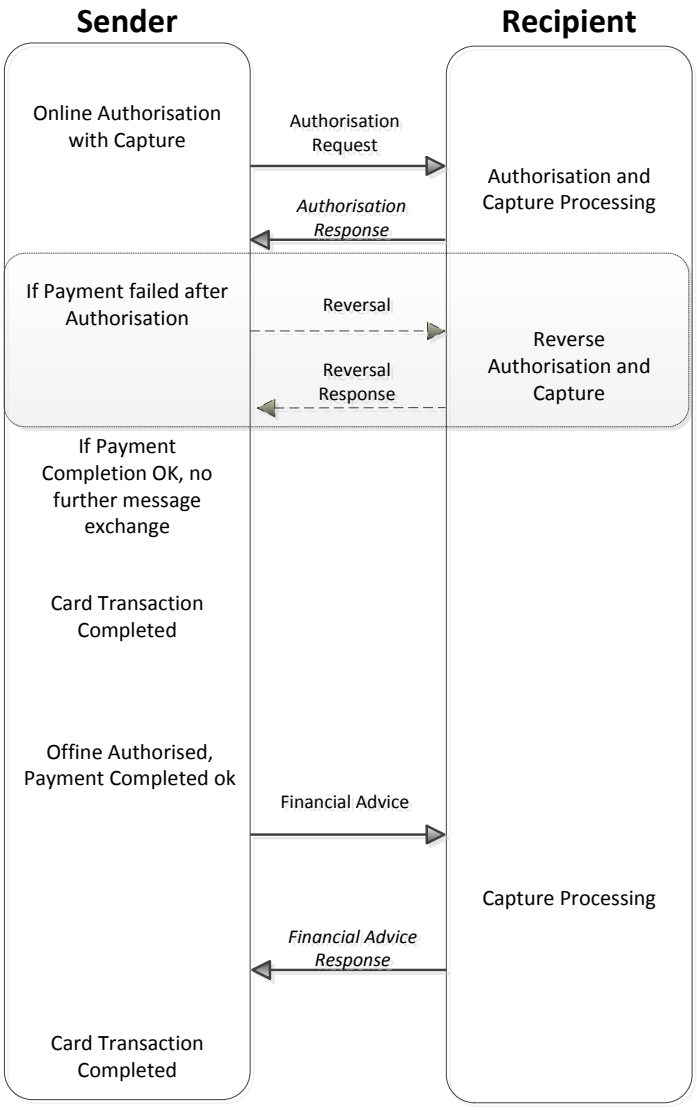



FIGURE 10: MODE 3

## 2.5 Migration Paths for SEPA Security and Functional Certification

### 2.5.1 Security Certification

For all Volume conformant CPS/ABs the relevant security requirements as described in Book 4 of the Volume apply.

Evidence that the security requirements are met is provided by security evaluations performed by laboratories accredited by certification bodies. Certification bodies issue certificates based on the results of those evaluations. These processes are as described in Book 5 of the Volume.

Security evaluations and certifications can be performed using different evaluation and certification methodologies. These methodologies provide for different levels of assurance for the CPS/ABs which take responsibility for transactions being performed.

The Security specification provider(s) determine the security evaluation process and methodology to be used.

### 2.5.2 Functional Certification

Functional Certification is out of scope for this release of the Volume. It will be included in a later release, based on the CSG work on labelling in collaboration with the different standardisation initiatives working on functional standards used in SEPA e.g.: EMVCo, ISO 20022, etc.

It is expected that the Functional specification provider(s) will determine the functional evaluation process and methodology to be used.

## 2.6 Implementation guidance of Choice of the Application

### 2.6.1 Local Transactions

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.

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


FIGURE 11: 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 12: EXAMPLE: CHOICE OF APPLICATION IN THE CASE OF ACCEPTOR PRE-SELECTION THAT INCLUDES THE TOTAL AMOUNT AND PIN ENTRY

### 2.6.2 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.

# 3 IMPLEMENTATION GUIDELINES PER PAYMENT CONTEXT

## 3.1 Context: Payment in attended environment, Cardholder is present, Cardholder Verification performed and final amount known

### 3.1.1 Definition of the payment context

This context is used for the majority of card payments. The POI is normally a desktop device that is used by most acceptors providing goods or services. The POI could either be a standalone device or a device integrated with the point of sale.

- Attendant Present (attended/semi-attended);
- Card and Cardholder are present;
- Cardholder verification performed;
- Final amount known;
- Physical POI (Chip and PIN capable).

### 3.1.2 Implementation Requirements and Options

#### *3.1.2.1 Card services*

##### *3.1.2.1.1 Current Implementations*

From an acceptance perspective, the following card services are supported for this context:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |
| **Cancellation** | Conditional[5] | Conditional[5] | Conditional[5] | Optional |
| **Refund** | Optional | Optional | Optional | Optional |

TABLE 13: CARD SERVICES - CURRENT IMPLEMENTATIONS

##### *3.1.2.1.2 Volume Conformant Implementation*

From an acceptance perspective, the following card services shall be supported for this context:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

[5] Issuers, Schemes and Acquirers shall support Cancellation if refund is not supported.

| | | | | |
|---|---|---|---|---|
| **Cancellation** | Required 2019 | Required 2019 | Required 2019 | Optional |
| **Refund** | Required 2019 | Required 2019 | Required 2019 | Optional |

TABLE 14: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATION

#### *3.1.2.2 Acceptance technology*

##### *3.1.2.2.1 Current Implementations*

POI shall either be:

- Offline with online capability,

  Or
- Online only.

##### *3.1.2.2.2 Volume Conformant Implementation*

POI shall either be:

- Offline with online capability,

  Or
- Online only.

  However, it is recommended to be offline with online capability.

#### *3.1.2.3 Cardholder Verification Method*

There are no mandatory requirements to support a specific CVM from an issuer perspective however within the SEPA area PIN is the recommended method.

From an acceptance perspective PIN CVM is required.

#### *3.1.2.4 Data Capture*

All 3 modes defined in section 2.4 are applicable

### 3.1.3 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.

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

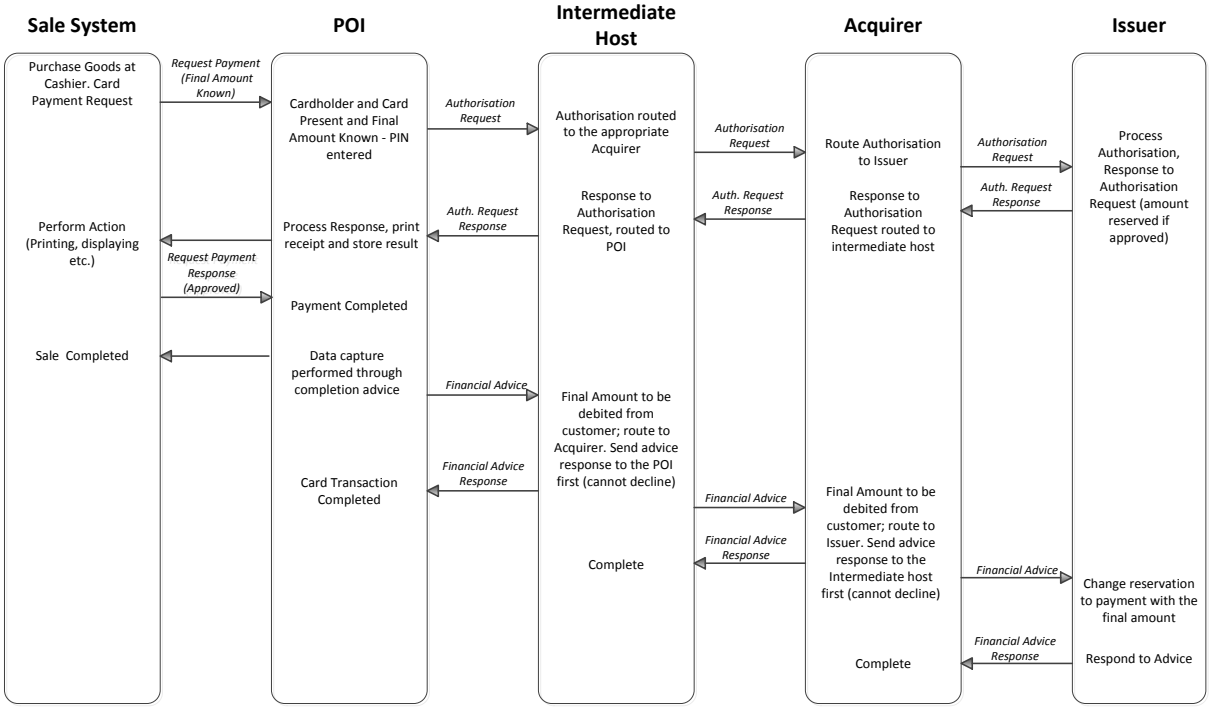



FIGURE 15: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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

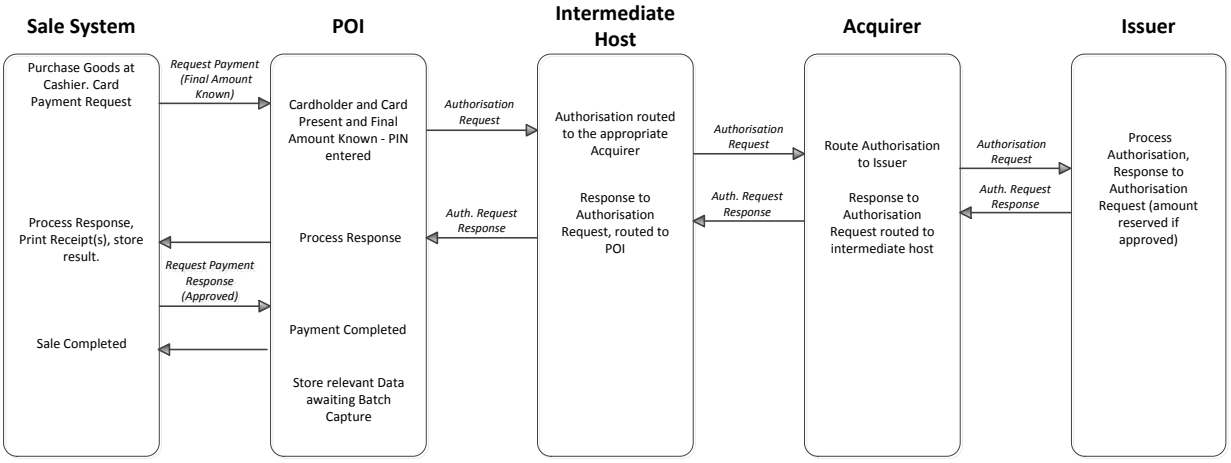



FIGURE 16: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

## 3.2 Context: Payment in an unattended environment, Cardholder is present Cardholder Verification method is PIN and final amount known

### 3.2.1 Definition of the payment context

This payment context is used for unattended vending machines, ticketing machines etc. Cardholder is present. The POI is always integrated with a sales system.

- Attendant Not Present (unattended);
- Card and Cardholder are present;
- Cardholder verification Method is PIN;
- Final amount known;
- Physical POI (Chip and PIN capable).

### 3.2.2 Implementation Requirements and Options

#### *3.2.2.1 Card services*

##### *3.2.2.1.1 Current Implementations*

From an acceptance perspective, only the following card service is supported for this context:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

TABLE 17: CARD SERVICES - CURRENT IMPLEMENTATIONS

#### 3.2.2.1.2 *Volume Conformant Implementation*

From an acceptance perspective, only the following card service shall be supported for this context:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

TABLE 18: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

### 3.2.2.2 *Acceptance technology*

#### 3.2.2.2.1 *Current Implementations*

POI shall either be:

- Offline with online capability,

  Or

- Online only.

#### 3.2.2.2.2 *Volume Conformant Implementation*

POI shall either be:

- Offline with online capability,

  Or

- Online only.

However, it is recommended to be offline with online capability.

### 3.2.2.3 *Cardholder Verification Method*

#### 3.2.2.3.1 *Cardholder Verification Method (Issuance)*

##### 3.2.2.3.1.1 *Current Implementations*

There are no mandatory requirements to support a specific CVM from an issuer perspective however within the SEPA area PIN is the recommended method for this context.

##### 3.2.2.3.1.2 *Volume Conformant Implementation*

Cards that are intended to be accepted in this context must support PIN.

#### 3.2.2.3.2 *Cardholder Verification Method (Acceptance)*

##### 3.2.2.3.2.1 *Current Implementations*

The only CVM method to be supported for this context is PIN.

##### 3.2.2.3.2.2 *Volume Conformant Implementation*

The only CVM method to be supported for this context is PIN.

#### 3.2.2.4 *Data Capture*

All 3 modes defined in section 2.4 are applicable

### 3.2.3 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.

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

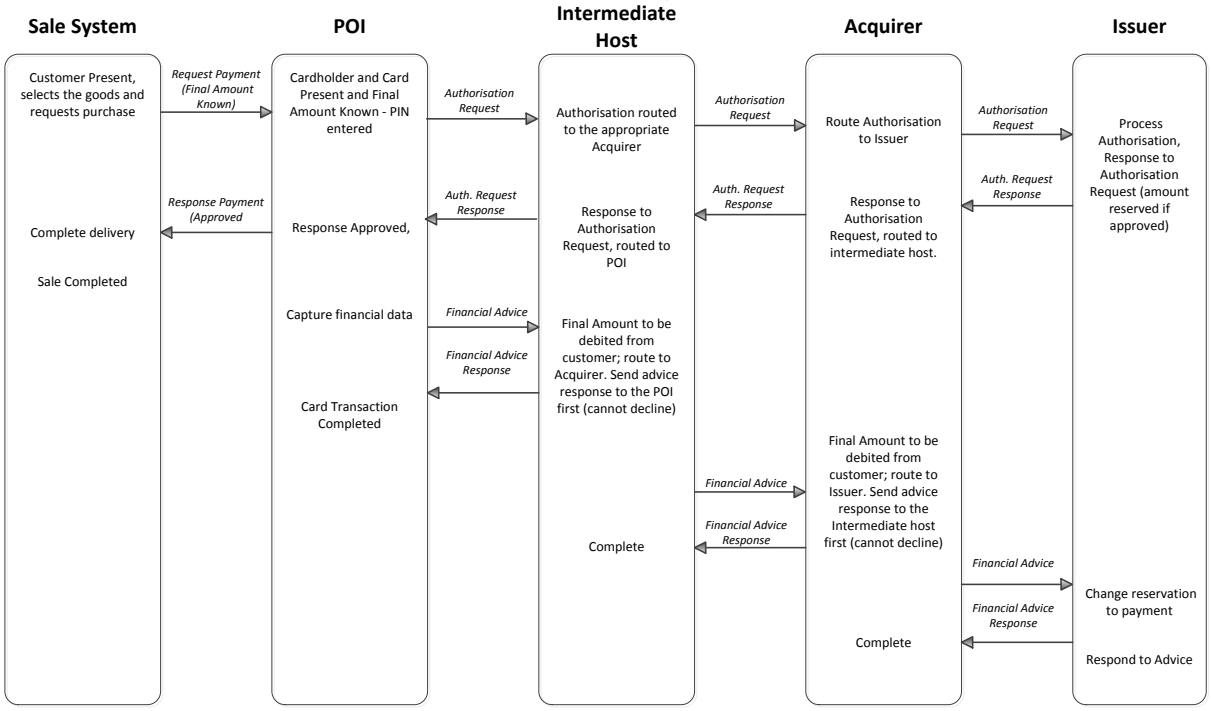



Figure 19: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION IS PIN AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

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

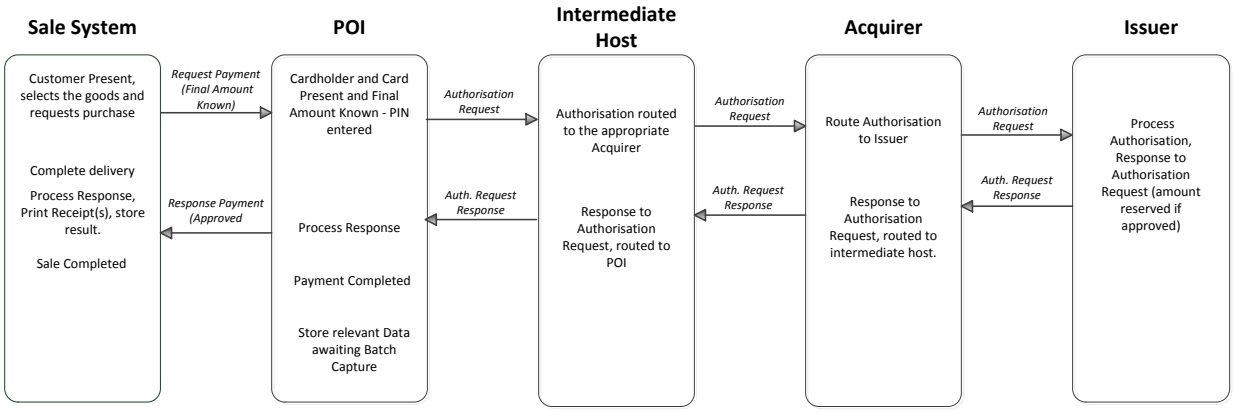



Figure 20: EXAMPLE FLOW: PAYMENT IN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT, CARDHOLDER VERIFICATION IS PIN AND FINAL AMOUNT KNOWN, CAPTURE BY BATCH

## 3.3 Context: Payment with 'No CVM Required' in attended or unattended environment, Cardholder is present and final amount known

### 3.3.1 Definition of the payment context

This payment context is restricted to certain Acceptor Categories where risk assessment allows low value transaction with "No CVM Required". This context can be used for low value transactions where the interaction with the cardholder must be minimized because of the need for speed or safety reasons. A PIN Entry Device is not mandatory.

- Card and Cardholder are both present;
- Final amount known;
- Cardholder Consent (by presenting the card);
- Physical POI (Chip capable);
- Attendant Present (attended/semi-attended) and unattended.

### 3.3.2 Implementation Requirements and Options

#### *3.3.2.1 Card services*

##### *3.3.2.1.1 Current Implementations*

In an attended environment, the following card services are supported for this context from an acceptance perspective:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |
| **Cancellation** | Conditional[6] | Conditional | Conditional | Optional |
| **Refund** | Optional | Optional | Optional | Optional |

Table 21: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR ATTENDED

In an unattended environment, the following card services are supported for this context from an acceptance perspective:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 22: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR UNATTENDED

#### *3.3.2.1.2 Volume Conformant Implementation*

For attended environment:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |
| **Cancellation** | Required 2019 | Required 2019 | Required 2019 | Optional |
| **Refund** | Required 2019 | Required 2019 | Required 2019 | Optional |

Table 23: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 24: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR UNATTENDED

### *3.3.2.2 Acceptance technology*

#### *3.3.2.2.1 Current Implementations*

POI shall be:

- Offline with online capability,

[6] Issuers, Schemes and Acquirers shall support Cancellation if refund is not supported

Or

- Online only.

#### 3.3.2.2.2 Volume Conformant Implementation

POI shall be:

- Offline with online capability,

  Or

- Online only.

However, it is recommended to be offline with online capability.

### 3.3.2.3 Cardholder Verification Method

#### 3.3.2.3.1 Cardholder Verification Method (Issuance)

##### 3.3.2.3.1.1 Current Implementations

There are no mandatory requirements to support a specific CVM from an issuer perspective however within the SEPA area "No CVM Required" is the recommended method for this context.

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.

##### 3.3.2.3.1.2 Volume Conformant Implementation

Cards that are intended to be accepted in this context must support "No CVM Required".

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.

#### 3.3.2.3.2 Cardholder Verification Method (Acceptance)

##### 3.3.2.3.2.1 Current Implementations

The CVM method to be supported for this context is "No CVM Required".

##### 3.3.2.3.2.2 Volume Conformant Implementation

The only CVM method to be supported for this context is "No CVM Required".

#### *3.3.2.4 Data Capture*

All 3 modes defined in section 2.4 are applicable.

### 3.3.3 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.

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

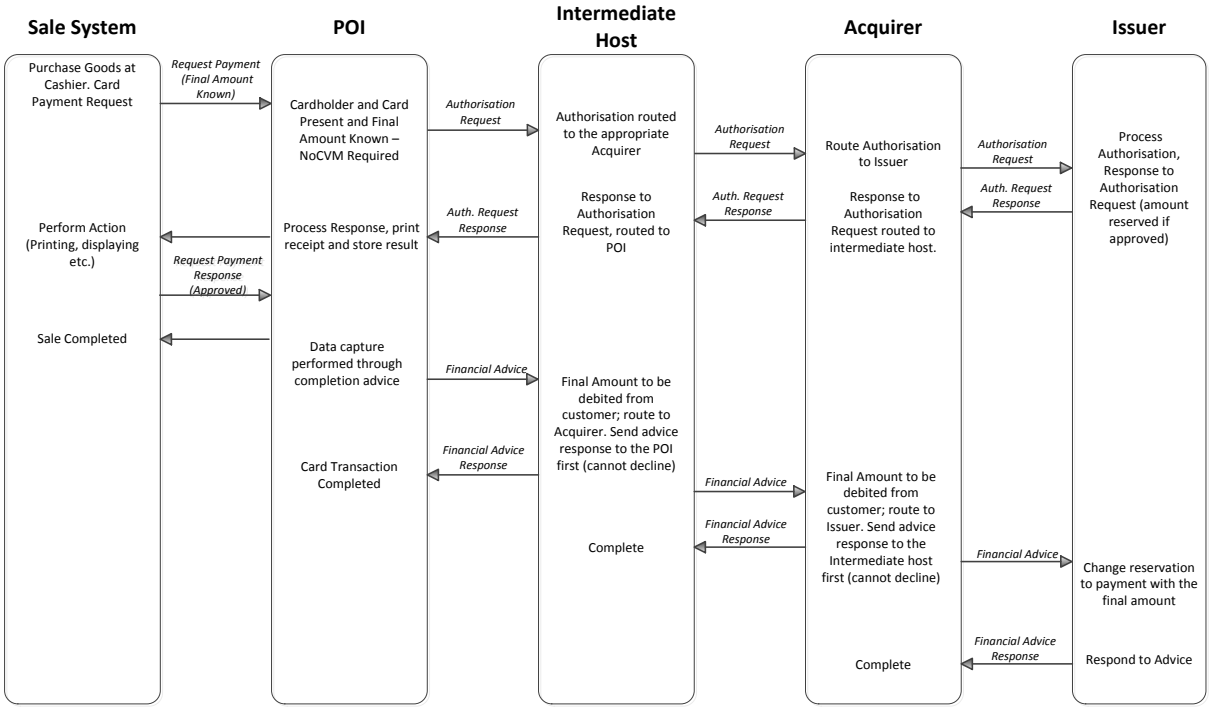



Figure 25: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION.

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

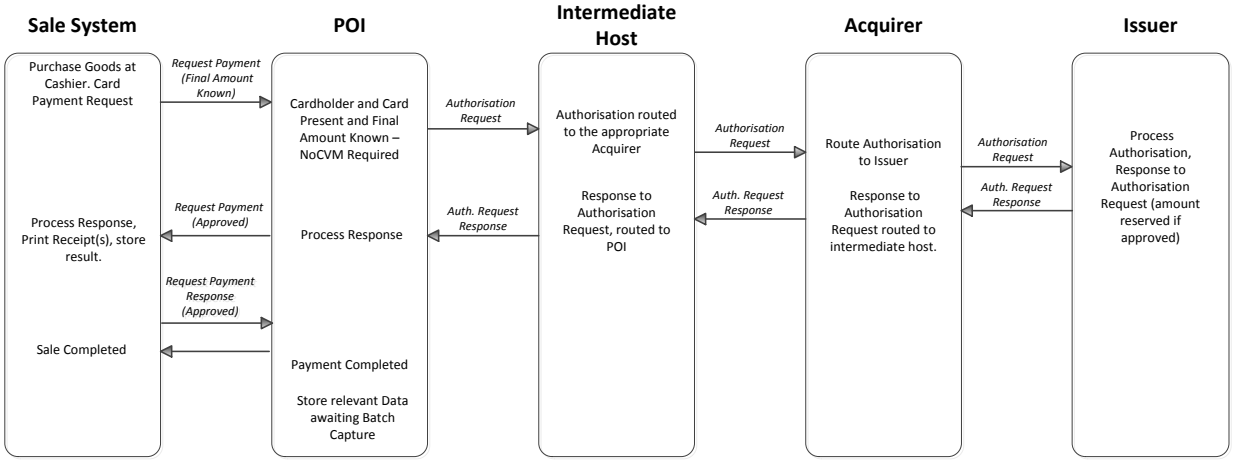



Figure 26: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH.

## 3.4 Context: Deferred Payments in an attended and unattended environment with an estimated amount at payment initiation, cardholder is present with cardholder verification

### 3.4.1 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.

- Card and Cardholder are present;
- Final amount is not known at the time of the authorisation;
- Cardholder Consent (by using one cardholder verification method);
- Physical POI (PIN and Chip capable);
- Attendant Present/Not Present (attended/unattended).

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 T180, 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”.

### 3.4.2 Implementation Requirements and Options

#### *3.4.2.1 Payment services*

##### *3.4.2.1.1 Current Implementations*

Today there is no commonly accepted method that is used by all schemes and countries. Those that are in use are often incompatible.

##### *3.4.2.1.2 Volume Conformant Implementation*

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Deferred Payment with Partial Approval** | Required 2019 | Required 2019 | Required 2019 | Required 2019 |

Table 27: PAYMENT SERVICES - VOLUME CONFORMANT IMPLEMENTATION

#### *3.4.2.2 Acceptance environment*

##### *3.4.2.2.1 Current Implementations*

POI shall either be:

- Online only

  Or

- Offline with online capability

##### *3.4.2.2.2 Volume Conformant Implementation*

POI shall either be:

- Online only

  Or

- Offline with online capability

#### *3.4.2.3 Card Data Authentication method*

See section 2.2

*3.4.2.4 Cardholder Verification Method*

*3.4.2.4.1 Cardholder Verification Method (Issuance)*

*3.4.2.4.2 Current Implementations*

There are no mandatory requirements to support a specific CVM from an issuer perspective however within the SEPA area PIN is the recommended method for this context.

*3.4.2.4.2.1 Volume Conformant Implementation*

Cards that are intended to be used in this payment context shall support PIN.

*3.4.2.4.3 Cardholder Verification Method (Acceptance)*

*3.4.2.4.3.1 Current Implementations*

Whether PIN is the only CVM allowed in the unattended environment is a risk management decision depending on the amount value to be authorised, but at petrol stations there are no known implementations without PIN due to the high value of products and high fraud risk. In the attended environment there are no mandatory requirements to support a specific CVM.

*3.4.2.4.3.2 Volume Conformant Implementation*

For unattended, PIN is the only supported CVM. For attended, PIN is the recommended CVM. For low value transactions e.g., phone booths, "No CVM Required" may be acceptable.

*3.4.2.5 Data Capture*

*3.4.2.5.1 Current Implementations*

There are many national and/or scheme specific solutions to the basic logic problem of authorising online outdoor petrol card transactions where the amount is not known until the filling is complete.

*3.4.2.5.2 Volume Conformant Implementation*

This context does not apply to off-line situations. For a Volume conformant online implementation of outdoor petrol it is required that the acceptor, acquirer, issuer and all intermediate protocols all support the implementation rules described in 3.4.1. As the authorisation has to be performed online, the Mode 1 as described in section 2.4.2 is the only recommended Data Capture implementation. Mode 3 is not technically possible and Mode 2 does not meet these requirements.

### 3.4.3 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**

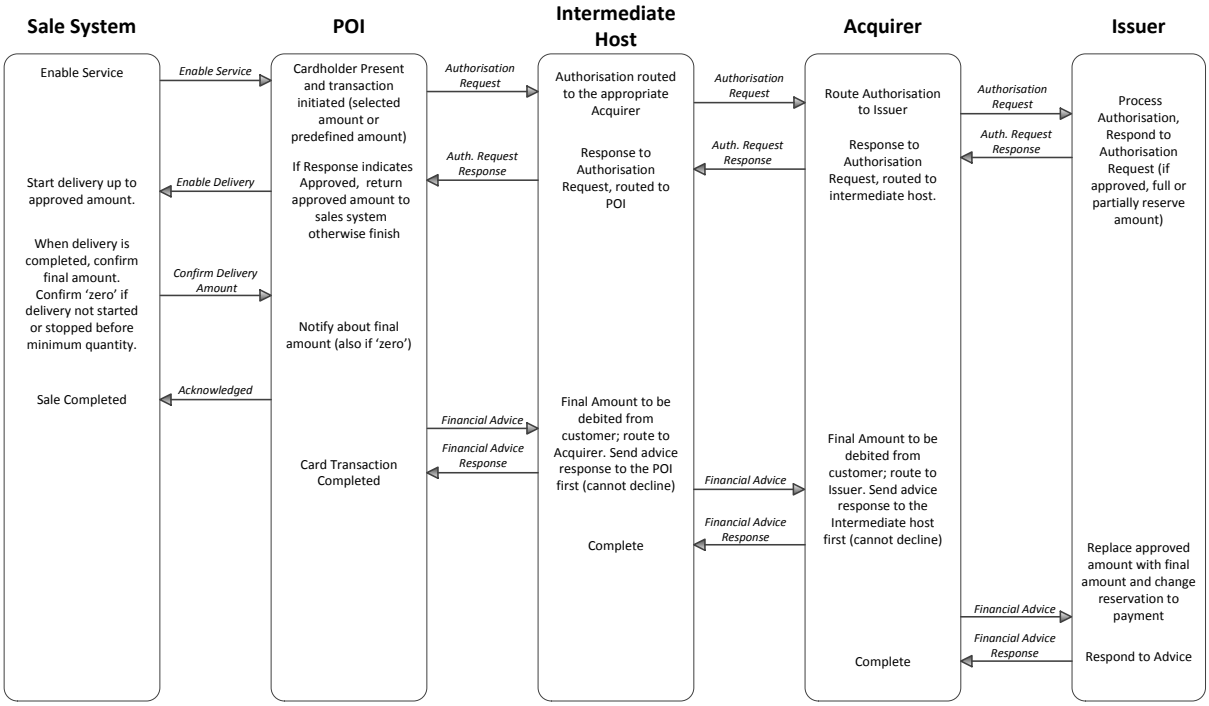



FIGURE 28: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

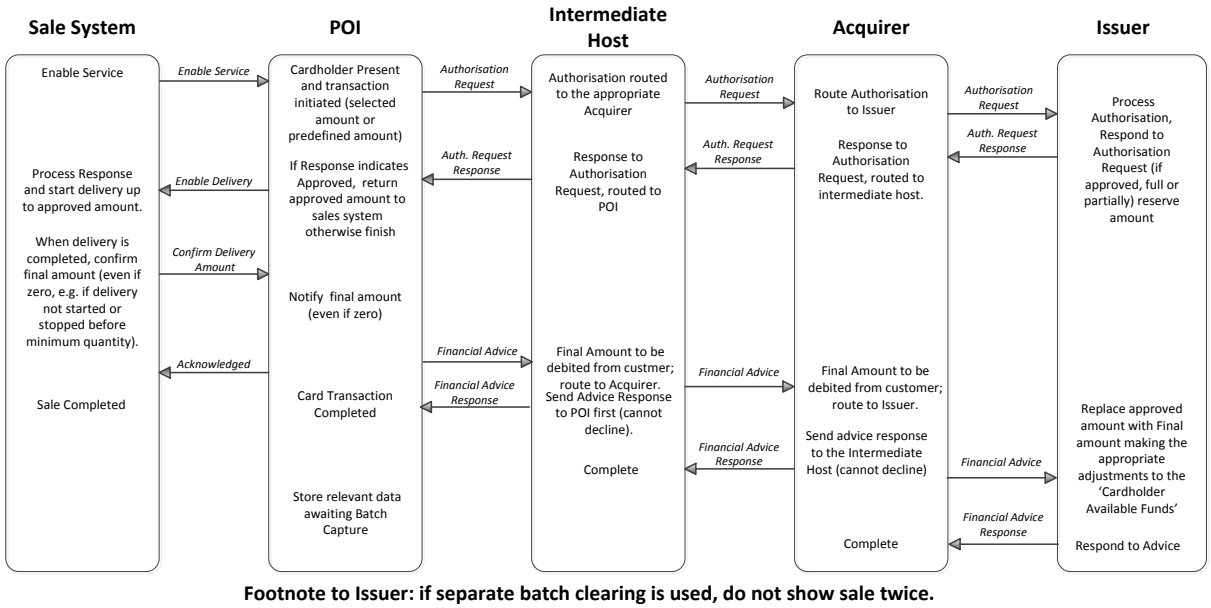



FIGURE 29: EXAMPLE FLOW: DEFERRED PAYMENT CARD MESSAGE FLOW, CAPTURE BY BATCH

## 3.5 Context: Pre-Authorisation Services in an attended or unattended environment to reserve an amount, Cardholder present

### 3.5.1 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 the estimated amount. Thereafter, the estimated amount can be incremented or decremented 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 either a Cancellation or an Update Pre-Authorisation to restore the "cardholders' available funds". In this case Payment Completion shall not follow.

This context implies that:

- Card and Cardholder are present during the Pre-Authorisation Service;
- A Card Present chip transaction including Cardholder verification shall be performed;

- Stored Card Data may be used for the Update Pre Authorisation service and for the Payment completion service;
- Final amount is not known at the time of the Pre-Authorisation;
- Physical POI (Chip and PIN capable);
- Attendant Present (attended/semi-attended) or unattended.

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 or the Update Pre Authorisation service.

### 3.5.2 Implementation Requirements and Options

#### *3.5.2.1 Card Services*

##### *3.5.2.1.1 Volume Conformant Implementation(s)*

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)[7] 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 either:
    - A Cancellation, that cancels the Pre-Authorisation and any Update Pre-Authorisation linked to it

      Or

    - An Update Pre-Authorisation that decreases the authorised amount(s) to zero.

  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) which is created in the Pre-Authorisation transaction 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.

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.

From an acceptance perspective, 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 30: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

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

*3.5.2.2 Acceptance technology*

*3.5.2.2.1 Volume Conformant Implementation*

POI shall either be:

- Offline with online capability,

  Or

- Online only.

However, it is recommended to be offline with online capability.

*3.5.2.3 Cardholder Verification Method*

*3.5.2.3.1 Volume Conformant Implementation*

*3.5.2.3.1.1 Attended environment*

There are no mandatory requirements to support a specific CVM from an acceptance and issuer perspective however within the SEPA area PIN is the recommended method.

*3.5.2.3.1.2 Unattended environment*

PIN and - for low value transactions - “no CVM required” are the only supported CVM.

*3.5.2.4 Data Capture*

*3.5.2.4.1 Volume Conformant Implementation*

Card data can be retrieved from the Chip or from the stored data as defined in Book 2.

Capture can only take place after or when the transaction is finalised with a Payment Completion. Therefore, protocol configuration Mode 3 in section 2.4 is not applicable for this context.

### 3.5.3 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.

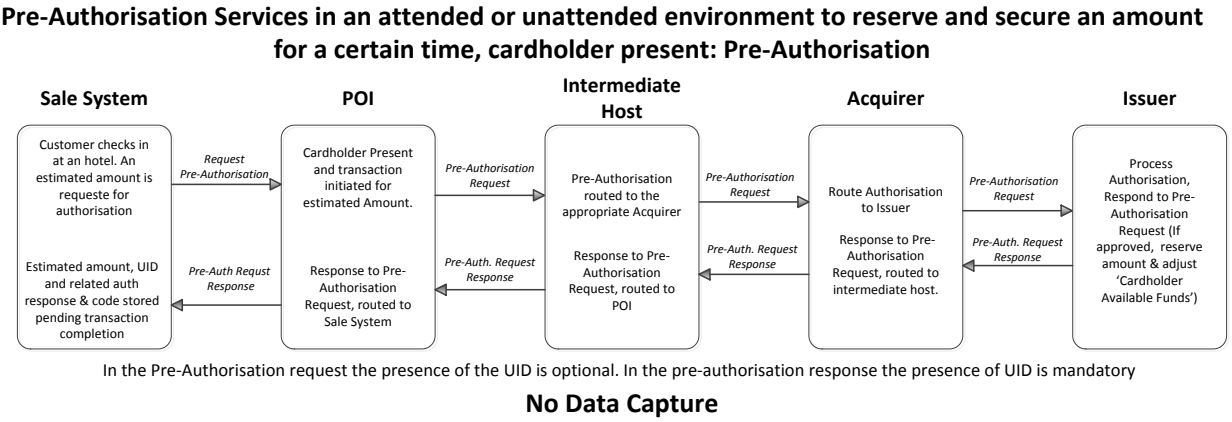
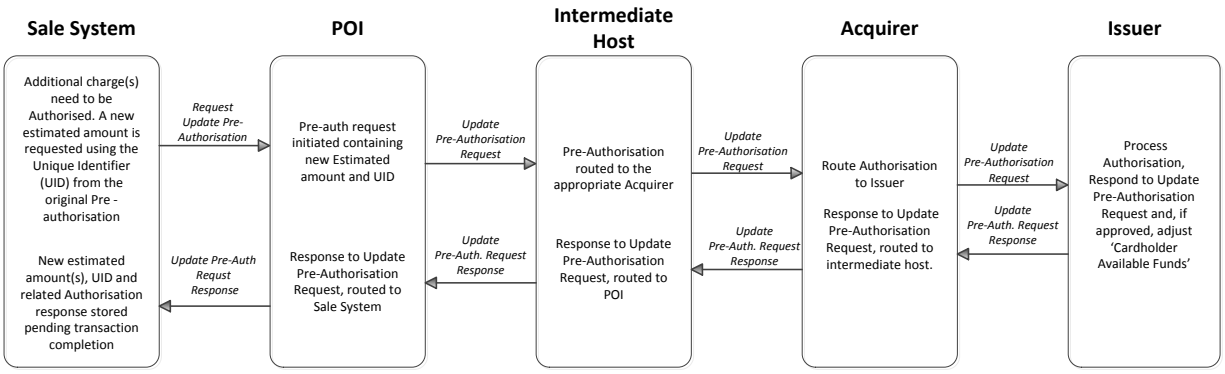



Figure 31: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT FOR A CERTAIN TIME, CARDHOLDER PRESENT: PRE-AUTHORISATION

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

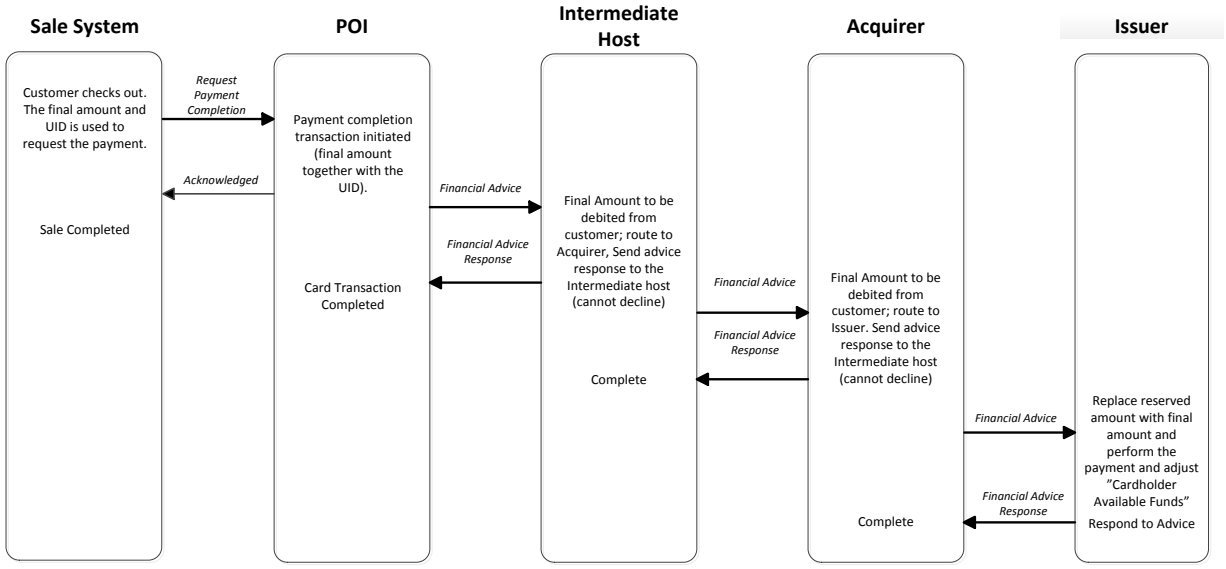



In the Update Pre-Authorisation request and response the presence of the UID is mandatory.

**No Data Capture**

Figure 32: 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 33: 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**

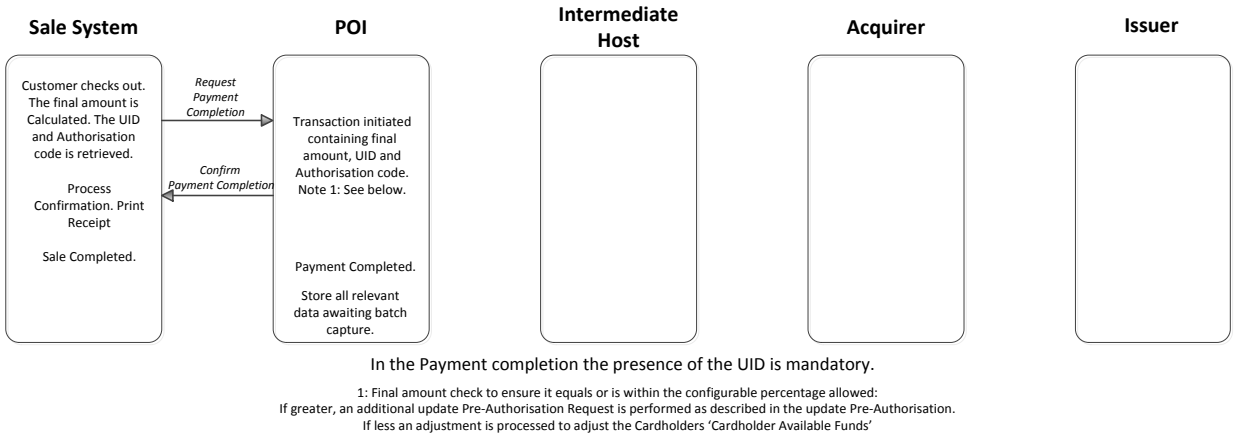



Figure 34: EXAMPLE FLOW: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN AMOUNT: PAYMENT COMPLETION. CAPTURE BY BATCH

## 3.6 Context: Basic e-commerce payment using static authentication and 3 domain security

Note that only a context describing a basic e-commerce transaction which also uses static authentication and 3 domain has been described in this book for e-commerce as this is how e-commerce transactions are currently handled in the marketplace. In the future, changes will apply to e-commerce transactions as mentioned in book 1 (section 1.2).

### 3.6.1 Definition of the payment context

This context is used for basic e-commerce payment where the cardholder enters static authentication from into a consumer device which accesses the acceptor's payment page on a browser.

- Card and Cardholder are not present in the acceptor's environment (they are interacting remotely);
- Card Data Retrieval may be through Manual Entry by Cardholder or from Stored Card Data. The CSC shall always be entered manually by the cardholder;
- Card Data Authentication is performed by the issuer verifying the static authenticator (CSC);
- Final amount is known at the time of the authorisation, however it is subject to alteration if some of the goods or services cannot be delivered;
- Cardholder Consent is implied through the entry of Card Data onto the Acceptor's payment page;

- Address information entered via an Address Verification Service (AVS) may also be used by the Issuer as an additional verification method in this context.

This usage of the static Authenticator:

- Implies that the Card is participating in the transaction;
- Enables the issuer to verify the Card Data.

This service is referred to as basic E commerce transaction.

The following rules apply:

4) the amount shall be authorised online by the issuer,
5) A secure channel shall be established for the processing and transmission of Card Data, as defined in Book 4 of the Volume.

### 3.6.2 Implementation Requirements and Options

#### *3.6.2.1 Payment services*

##### *3.6.2.1.1 Current Implementations*

Using a Virtual POI in a Remote Payment, the following card services are supported for this context from an acceptance perspective:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 35: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR REMOTE

This payment context may be impacted by market incentives and regulatory initiatives.

##### *3.6.2.1.2 Volume Conformant Implementation*

For remote environment:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 36: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR REMOTE

#### *3.6.2.2 Acceptance environment*

Virtual POI shall be online

*3.6.2.3 Acceptance Technologies*

*3.6.2.3.1 Current Implementations*

The following acceptance technologies may be supported:

- Manual entry by cardholder
- Stored Card Data ("Card on File").

*3.6.2.3.2 Volume Conformant Implementation*

The following acceptance technologies may be supported:

- Manual entry by cardholder;
- Stored Card Data ("Card on File").

*3.6.2.4 Card Data Authentication method*

*3.6.2.4.1 Current Implementations*

In this context Static Authentication is performed by the Issuer using a "*static authenticator*" i.e. the Card Security Code (CSC) manually entered into the payment page by the consumer/cardholder (e.g., CVV2, CVC2 or CID).

*3.6.2.4.2 Volume Conformant Implementation*

*The Card Data Authentication method should be based on strong authentication.*

*3.6.2.5 Cardholder Verification Method*

*3.6.2.6 Current Implementations*

In this context, the following CVM method may be used:

- 3 domain code, verified on-line by the issuer.

*3.6.2.7 Volume Conformant Implementation*

*The Cardholder Verification method should be based on strong authentication*

#### *3.6.2.8 Data Capture*

All 3 modes defined in section 2.4 are applicable.

## 3.7 Context: Contactless Payment with no Cardholder Verification Method required in an attended and unattended environment, Cardholder is present and final amount known

### 3.7.1 Definition of the payment context

This payment context is used for contactless transactions below an agreed terminal/POI CVM limit where cardholder verification[8] is not required. Setting the value of this CVM limit is out of scope of this document.

For this context:

- Card and Cardholder is present;
- Final amount known;
- Cardholder Consent (by presenting the card);
- Physical POI (Chip capable);
- Attendant Present (attended/semi-attended) and unattended.

### 3.7.2 Implementation Requirements and Options

#### *3.7.2.1 Card services*

##### *3.7.2.1.1 Current Implementations*

In an attended environment, the following card services are supported for this context from an acceptance perspective:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |
| **Cancellation** | Conditional[9] | Conditional | Conditional | Optional |
| **Refund** | Optional | Optional | Optional | Optional |

Table 37: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR ATTENDED

[8] The risk of not performing cardholder verification for this payment context is mitigated by the Card Issuers ability to periodically force contactless transactions to use another interface (through internal card risk management), where cardholder verification may be performed.

[9] Issuers, Schemes and Acquirers shall support Cancellation if refund is not supported.

In an unattended environment, the following card services are supported for this context from an acceptance perspective:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 38: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR UNATTENDED

#### *3.7.2.1.2 Volume Conformant Implementation*

For attended environment:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |
| **Cancellation** | Optional | Optional | Optional | Optional |
| **Refund** | Optional | Optional | Optional | Optional |

Table 39: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

| Service | Issuers | Schemes | Acquirers | Acceptors |
|---|---|---|---|---|
| **Payment** | Required | Required | Required | Required |

Table 40: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR UNATTENDED

### *3.7.2.2 Acceptance technology*

#### *3.7.2.2.1 Current Implementations*

POI shall be:

- Offline with online capability,

  Or
- Online only

#### *3.7.2.2.2 Volume Conformant Implementation*

POI shall be:

- Offline with online capability,

  Or
- Online only.

However, it is recommended to be offline with online capability.

#### *3.7.2.3 Cardholder Verification Method*

#### *3.7.2.3.1 Cardholder Verification Method (Issuance)*

##### *3.7.2.3.1.1 Current Implementations*

No specific requirements.

##### *3.7.2.3.1.2 Volume Conformant Implementation*

No specific requirements.

#### *3.7.2.3.2 Cardholder Verification Method (Acceptance)*

##### *3.7.2.3.2.1 Current Implementations*

No specific requirements.

##### *3.7.2.3.2.2 Volume Conformant Implementation*

No specific requirements.

#### *3.7.2.4 Data Capture*

All 3 modes defined in section 2.4 are applicable

### 3.7.3 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**

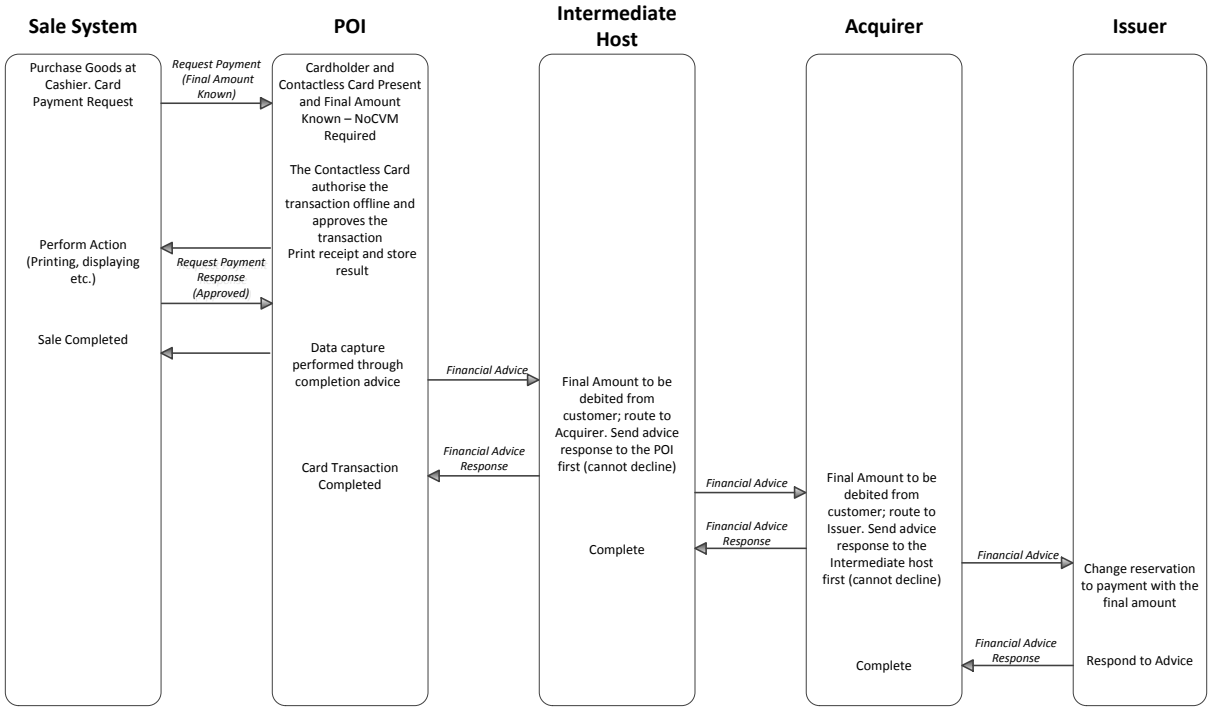



Figure 41: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION)WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

**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**

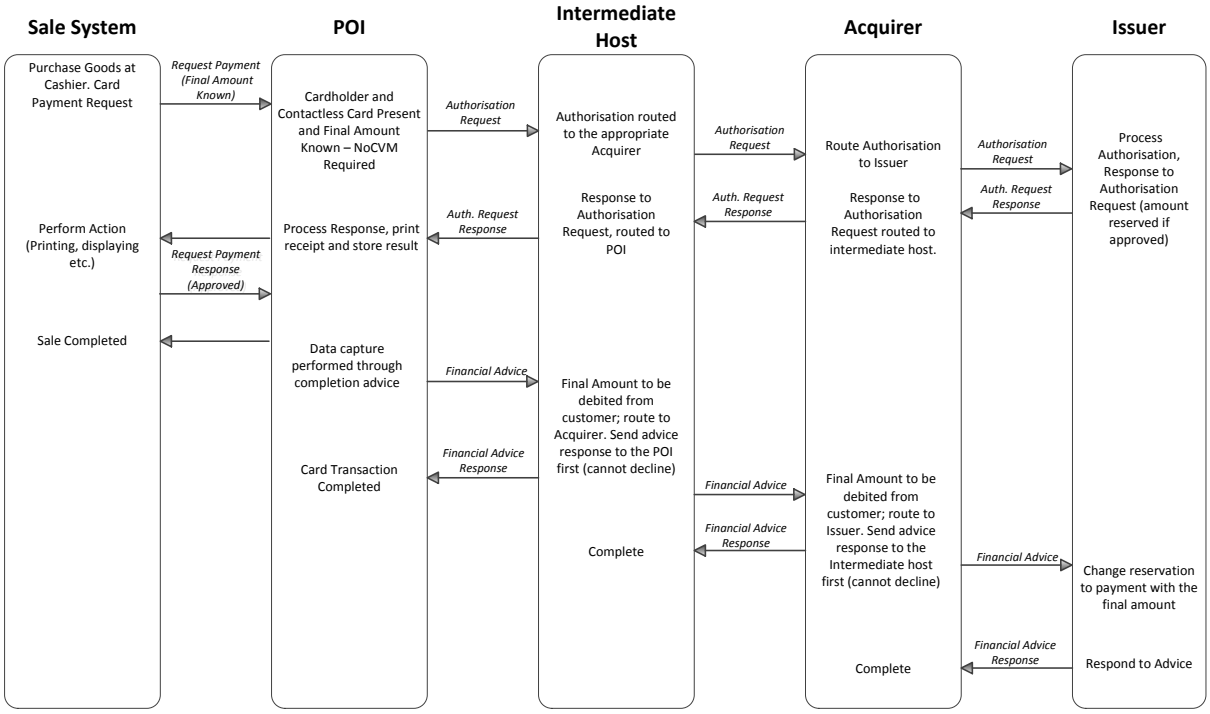



Figure 42: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE IMMEDIATELY AFTER TRANSACTION COMPLETION

**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**

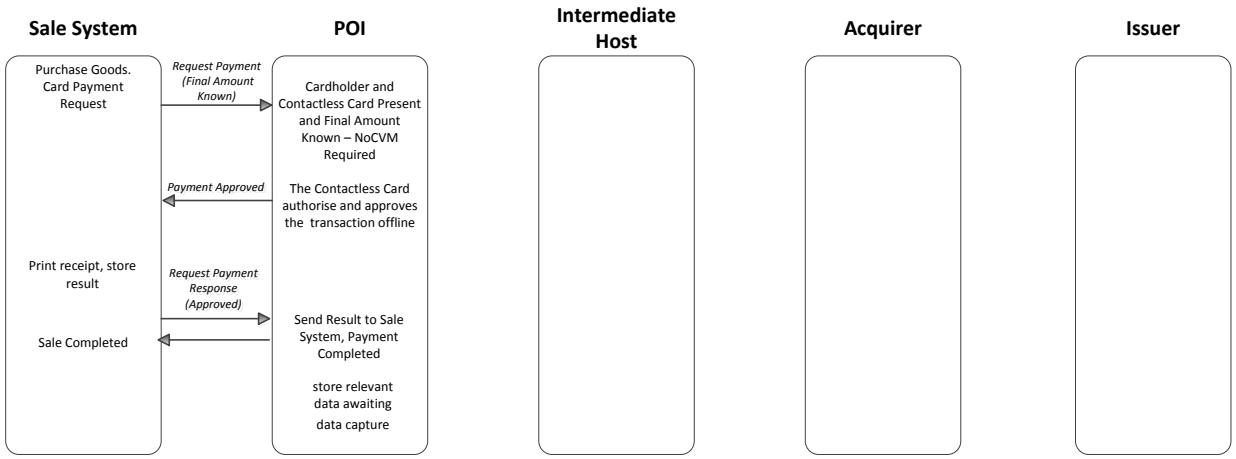



Figure 43: EXAMPLE FLOW: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH

**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**

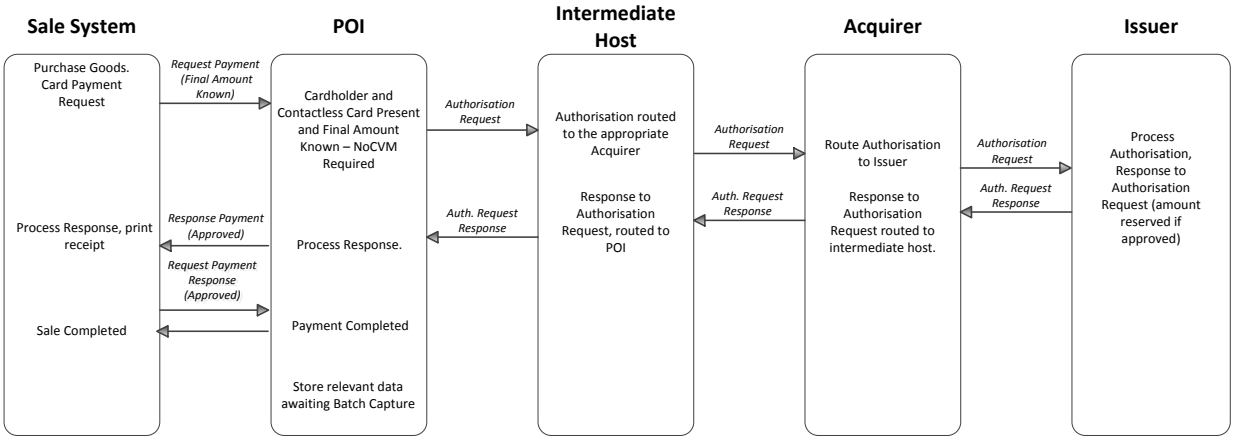



Figure 44: EXAMPLE FLOW: CONTACTLESS PAYMENT (ONLINE AUTHORISATION) WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN. CAPTURE BY BATCH

# 2 FIGURES AND TABLES