EPC020-08 11.02.2015

(Vol Ref. 7.6.1.05)

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.

Abstract	This document contains the work on SEPA cards standardisation to date
Document Reference	EPC020-08
Issue	Book 7.6.1.05
Date of Version	11 February 2015
Reason for Issue	Consultation
Reviewed by	CSG
Produced by	CSG Book 6 Expert Team
Owned by	EPC
Circulation	Public

Change history of Book 6		
6.6.0.x		Working version of Book 6
7.6.1.0		EPC Published version – Volume v7.0
7.6.1.01		Working version 2014
7.2.1.05		Consultation version 2015

15

16 **Table of Contents**

74

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 creating 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. Cardholder present Pre-Authorisation Services in an attended and unattended environment to reserve and secure an amount for a certain time.
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 0 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 contexts were added since the last version of Book 6:

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

The other contexts were harmonised in consequence.

Change history of Book 6		
7.6.1		Working version 2014 (post SCS Volume v7.1 published 7 Jan. 2014)

2 GENERAL IMPLEMENTATION GUIDELINES

2.1 Introduction

Books 2 to 5 describe general requirements for card payments. In order to harmonise common implementation options for future implementations, this section describes common implementation requirements valid for all payment contexts for the following topics:

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

In addition, this section covers the agreement on the POI Certification Process.

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)

158 *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

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

160 Note:

161 • For issuance, all SEPA cards shall support DDA and CDA and shall not support SDA in the
162 future;

163 • Since offline enciphered PIN is mandated for online only cards supporting PIN, it is not an
164 additional technology requirement to mandate DDA and CDA.

165 ### 2.2.2 Card Data Authentication Method (Acceptance)

166 *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

167 TABLE 3: CURRENT CARD DATA AUTHENTICATION METHOD (ACCEPTANCE)

[1] If the card supports PIN

168 *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

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

170 2.3 PIN based Cardholder Verification Methods

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

173 2.3.1 PIN Based Cardholder Verification Methods (Issuance)

174 *2.3.1.1 Current Implementations*

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

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

177 *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

178 TABLE 5: VOLUME CONFORMANT CARDHOLDER VERIFICATION METHOD (ISSUANCE)

179 Note:

180 • The above guidelines only apply if the card supports PIN as CVM;

181 • Offline Plaintext PIN may still be present in the CVM list for use outside SEPA, but only with
182 a lower priority than offline enciphered PIN and online PIN.

183

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]	Conditional3	Conditional3
Offline with online capability terminals	Required4	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	Conditional3	Conditional3
Offline with online capability terminals	Not used for SEPA Cards and shall not be mandatory on the POI from 2020	Required	Optional4

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:

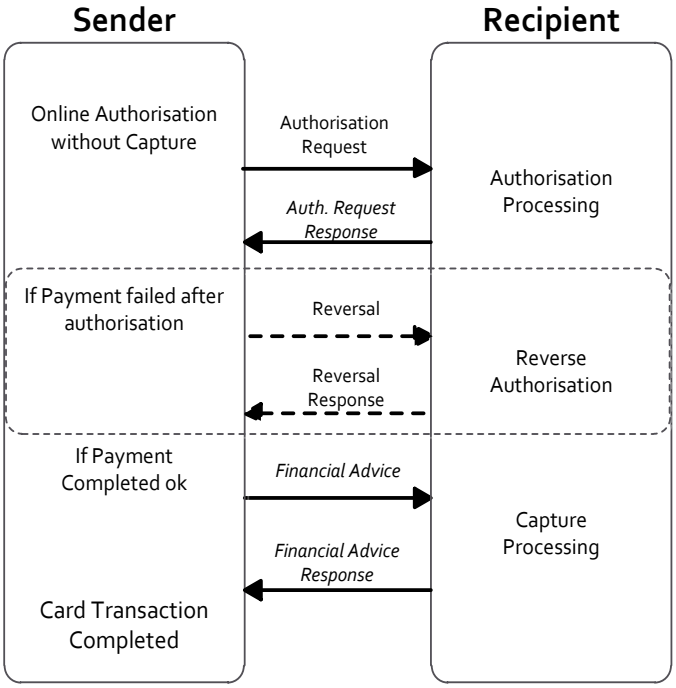
- Capture with Authorisation for transactions Authorised online;
- Capture immediately after transaction finalisation if Authorisation was performed offline.

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 without Capture Capture immediately after transaction finalisation



219

220 FIGURE 8: MODE 1

Mode 2: Online Authorisation without Capture Capture by Batch

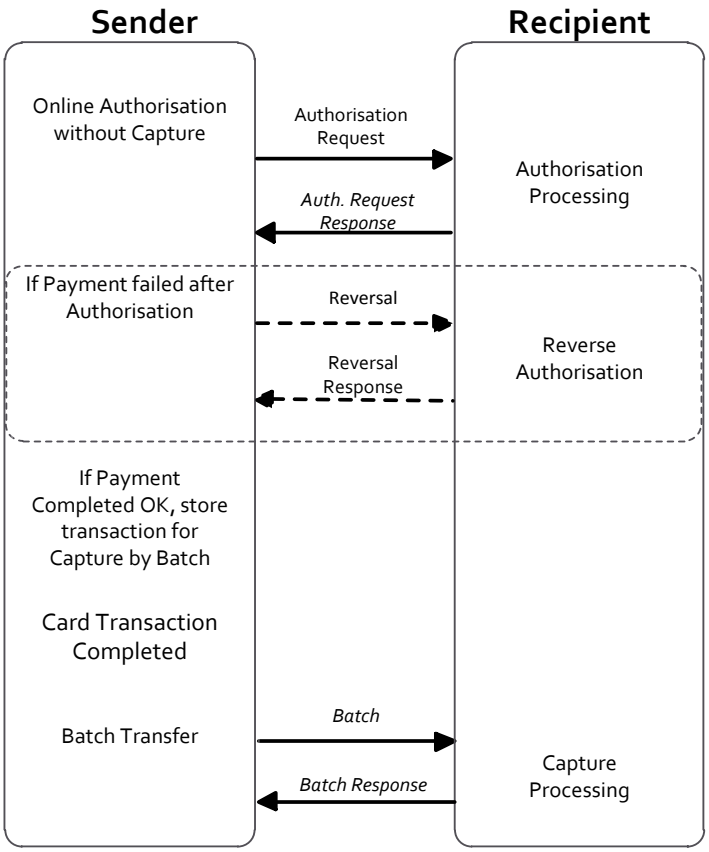


FIGURE 9: MODE 2

Mode 3: Online Authorisation with Capture

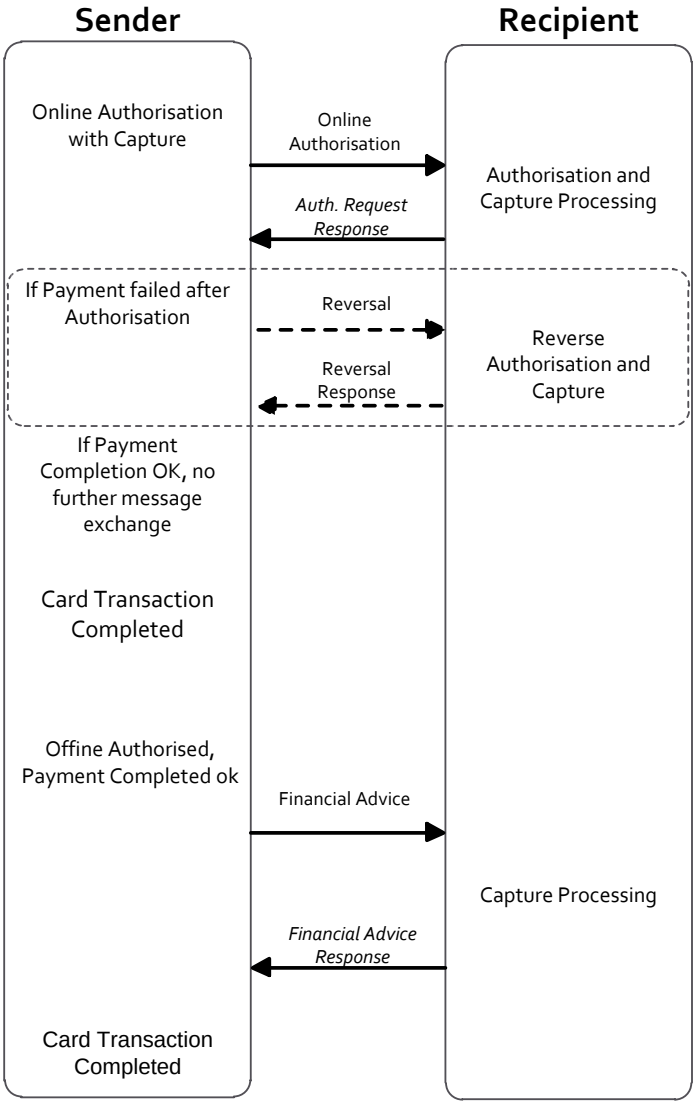


FIGURE 10: MODE 3

2.5 Migration Paths for SEPA Security and Functional Certification

2.5.1 Migration Path for POI Security Certification (Attended, Unattended and Chip only)

For all Volume conformant Card Payment Schemes / Approval Bodies the security requirements as described in Book 4 of the Volume, section 2.6 apply.

Evidence that the security requirements are met is provided by security evaluations performed by laboratories which are accredited by certification bodies; certification bodies issue certificates based on the results of these 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 card CPS/ABs which take the responsibility for transactions being performed by approved POI. The end state target is expected to be achieved through a convergence process whereby ISO 15408 Common Criteria will be used for the evaluation of all Volume conformant POI being newly approved in SEPA. This end state target is subject to a positive outcome of the evaluation of the OSeC pilot by the CSG, based on the evaluation criteria that it has defined, including evidence that a CC evaluation report can be used by PCI PTS. By following this common evaluation process a PCI SSC and a CC certificate may be delivered for newly approved POIs. CPS/ABs can choose to ask for one or the other or both certificates resulting from the CC evaluation process. OSeC protection profiles will be used for evaluation and certification. This applies to attended, unattended, chip only and hybrid POI.

Note for v7.05 of this document:

Shortly before the release of this document for public consultation, the CSG decided that it is no longer realistic to believe that the target outcome in Figure 11 can be reached in the given timeframe. Consequently, the CSG concluded that the convergence process as described in chapter 2.5.1 will not be referred to within the Volume.

This decision will be reflected in the final release of Book 6.

The following Roadmap has been planned for POI Security certification:

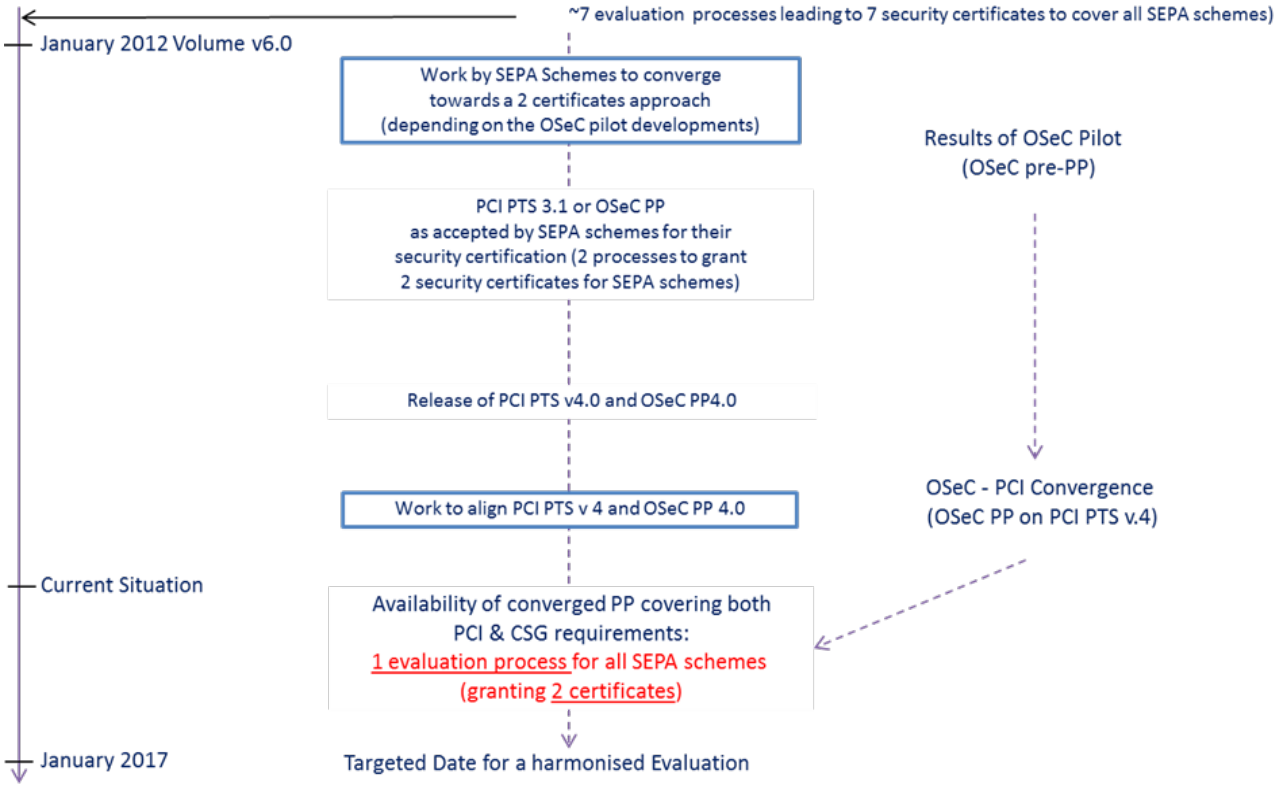


FIGURE 11: MIGRATION PATH FOR POI SECURITY CERTIFICATION

Note:

- This migration path only applies for newly approved POIs;
- It is anticipated that this target outcome in Figure 11 can be reached upon a positive evaluation of the OSeC pilot by the CSG.

2.5.2 Migration Path for Smartcard Security Certification

For all Volume conformant CPS/ABs the security requirements as described in Book 4 of the Volume, section 2.5 apply.

Evidence that the security requirements are met is provided by security evaluations performed by laboratories accredited by certification bodies that in turn issue certificates based on the results of these 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 the responsibility for transactions being performed by approved smartcards.

It will be possible to deliver the required certificates for the evaluation of all Volume conformant smartcards by using a single evaluation laboratory which provides reports accepted for the purpose of issuing these required certificates.

The security evaluation process and methodology to be used for the card payment application is determined by the specification provider of the related application as several application specifications will co-exist.

2.5.3 Migration Path for Functional Certification

The subject of functional certification is currently out of scope for this release of the Volume. It will be developed at a later stage, on the basis of the results of the different works on security certification and on labelling, as well as on the discussions with the different standardisation initiatives working on functional standards in use in SEPA such as: EMVCo, ISO 20022, etc. (non-exhaustive list).

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;
- 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]	Conditional5	Conditional5	Optional
Refund	Optional	Optional	Optional	Optional

TABLE 12: CARD SERVICES - CURRENT IMPLEMENTATIONS

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

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
Cancellation	Required 2019	Required 2019	Required 2019	Optional
Refund	Required 2019	Required 2019	Required 2019	Optional

TABLE 13: 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 Flow

A typical message flow can be seen below. Note that this is just one example of an implementation:

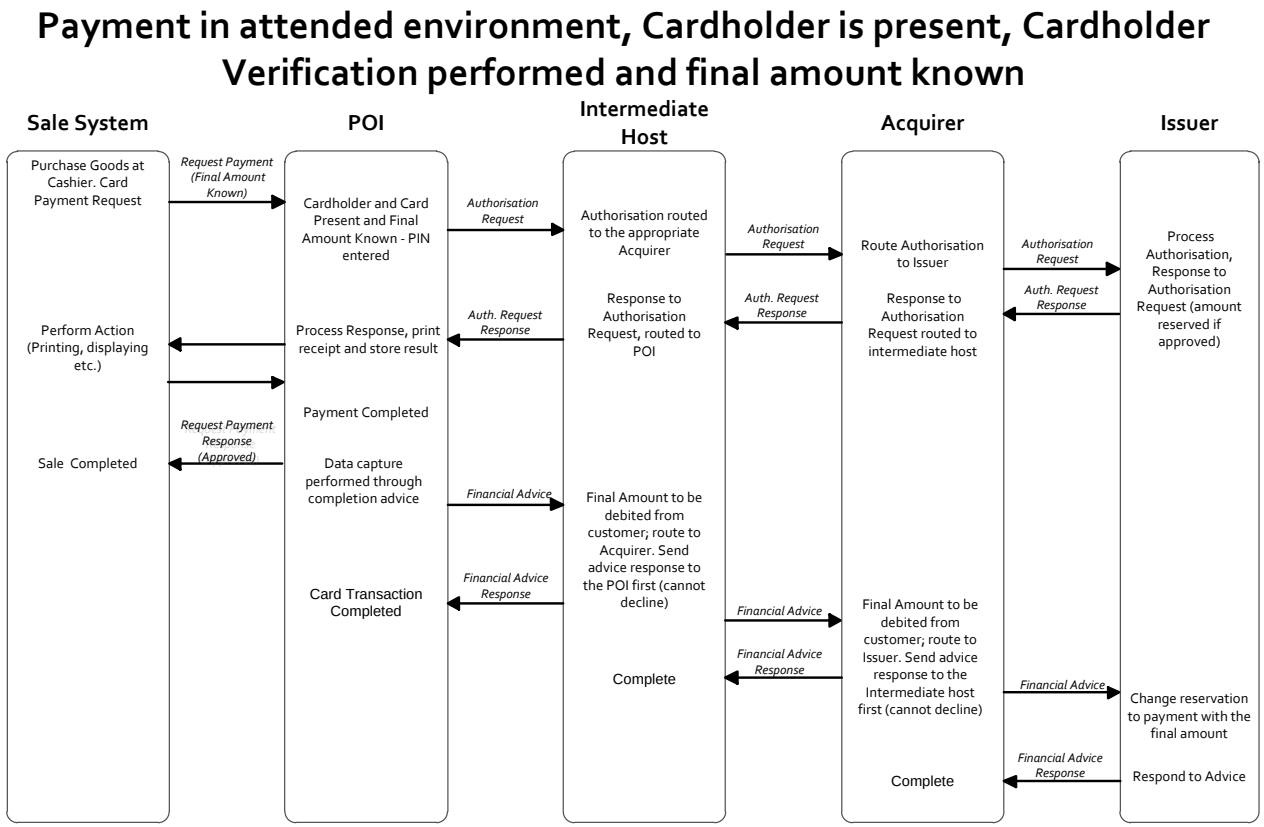


FIGURE 14: EXAMPLE FLOW: PAYMENT IN ATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT ,CARDHOLDER VERIFICATION PERFORMED AND FINAL AMOUNT KNOWN

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;
- 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 15: 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 16: 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 Flow

A typical message flow can be seen below. Note that this is just one example of an implementation:

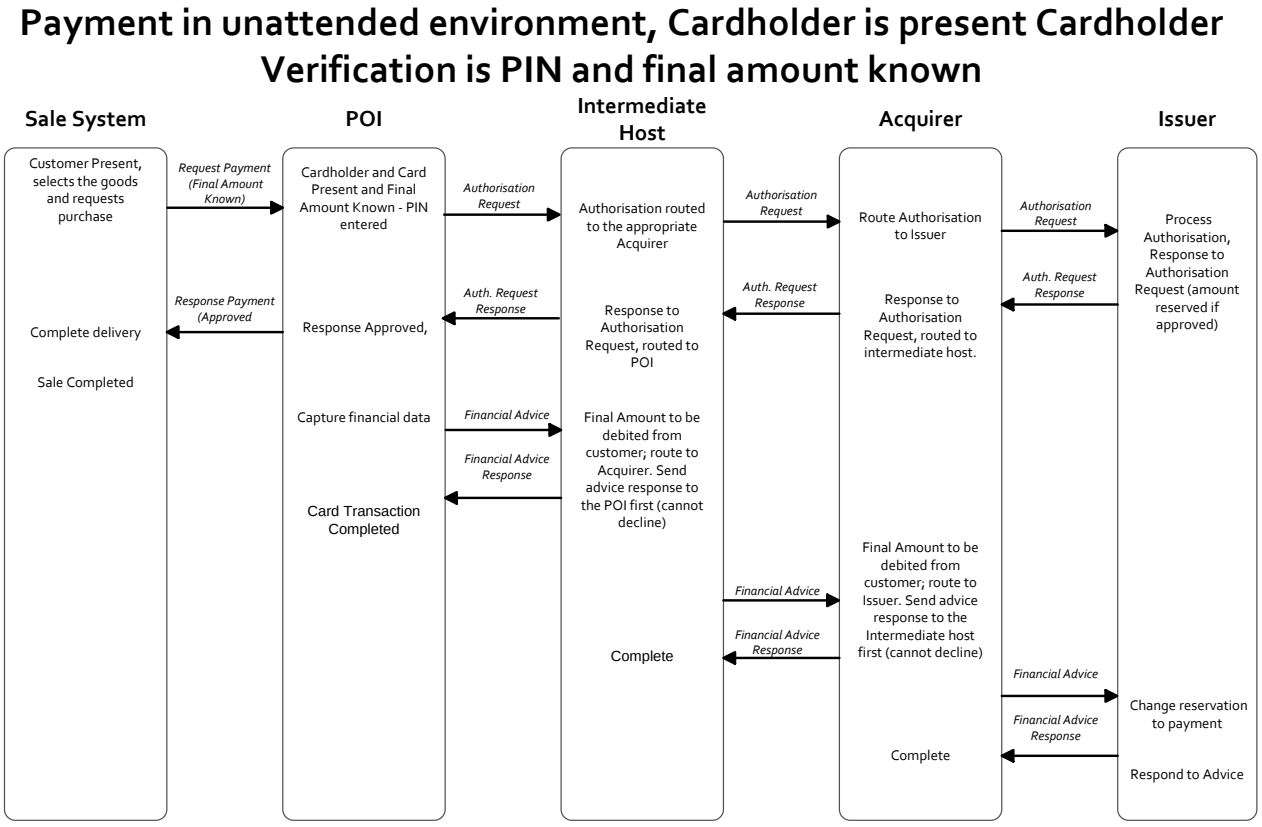


Figure 17: EXAMPLE FLOW: PAYMENT IN AN UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT CARDHOLDER VERIFICATION METHOD IS PIN AND FINAL AMOUNT KNOWN

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 is 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 18: CARD SERVICES - CURRENT IMPLEMENTATIONS FOR ATTENDED

[6] 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 19: 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 20: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

Table 21: 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,

  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 Flow

A typical message flow can be seen below. Note that this is just one example of an implementation:

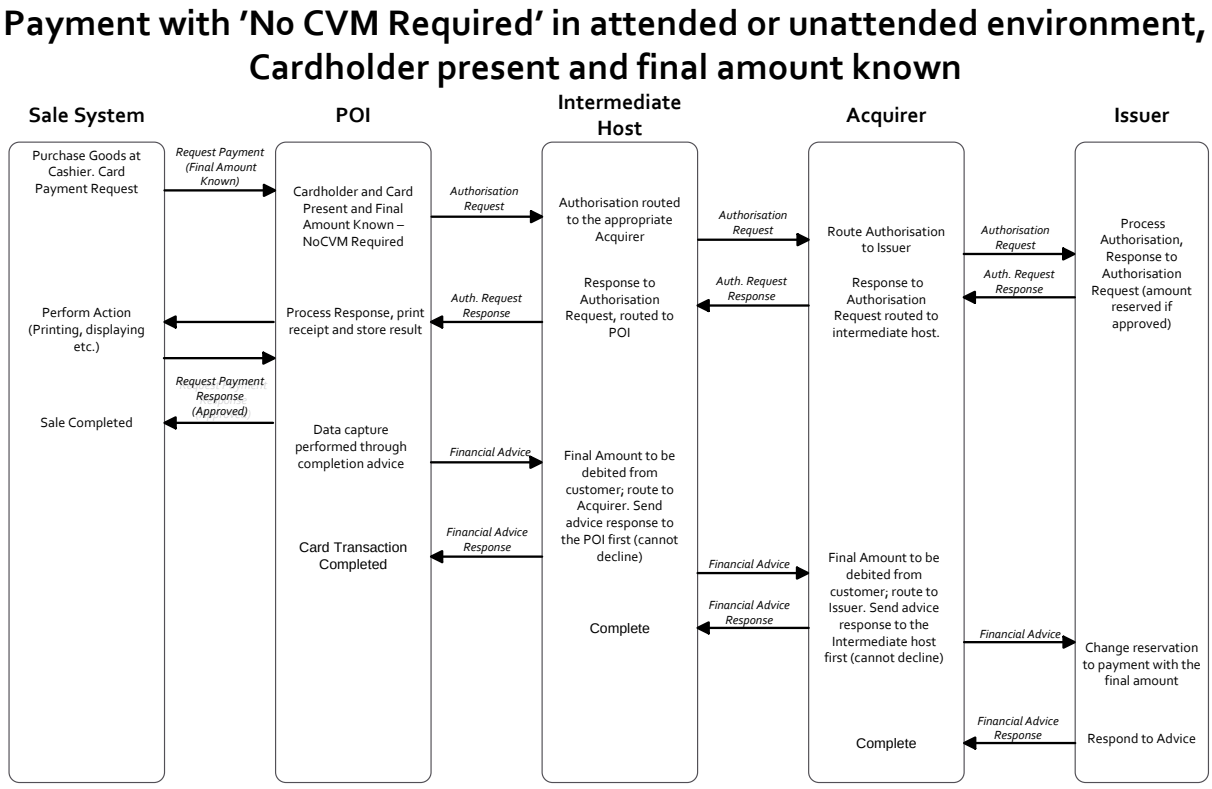


Figure 22: EXAMPLE FLOW: PAYMENT WITH 'NO CVM REQUIRED' IN ATTENDED OR UNATTENDED ENVIRONMENT, CARDHOLDER PRESENT AND FINAL AMOUNT KNOWN

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 pumps (“outdoor petrol”), attended and unattended. The following rules apply:

1) The amount that is requested to be authorised online is, as described in Book 2 T55, 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 23: 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

493 *3.4.2.4 Cardholder Verification Method*

494 *3.4.2.4.1 Cardholder Verification Method (Issuance)*

495 *3.4.2.4.1.1 Current Implementations*

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

498 *3.4.2.4.1.2 Volume Conformant Implementation*

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

500 *3.4.2.4.2 Cardholder Verification Method (Acceptance)*

501 *3.4.2.4.2.1 Current Implementations*

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

506 *3.4.2.4.2.2 Volume Conformant Implementation*

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

509 *3.4.2.5 Data Capture*

510 *3.4.2.5.1 Current Implementations*

511 There are many national and/or scheme specific solutions to the basic logic problem of authorising
512 online outdoor petrol card transactions where the amount is not known until the filling is complete.
513 There is currently no commonly agreed approach without seriously disadvantaging the cardholder.

514 *3.4.2.5.2 Volume Conformant Implementation*

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

3.4.3 Example of Message Flow

The following diagram illustrates a Deferred Payment Card Message Flow where all authorisation and message advices are online and real-time. Note that this is just one example of an implementation:

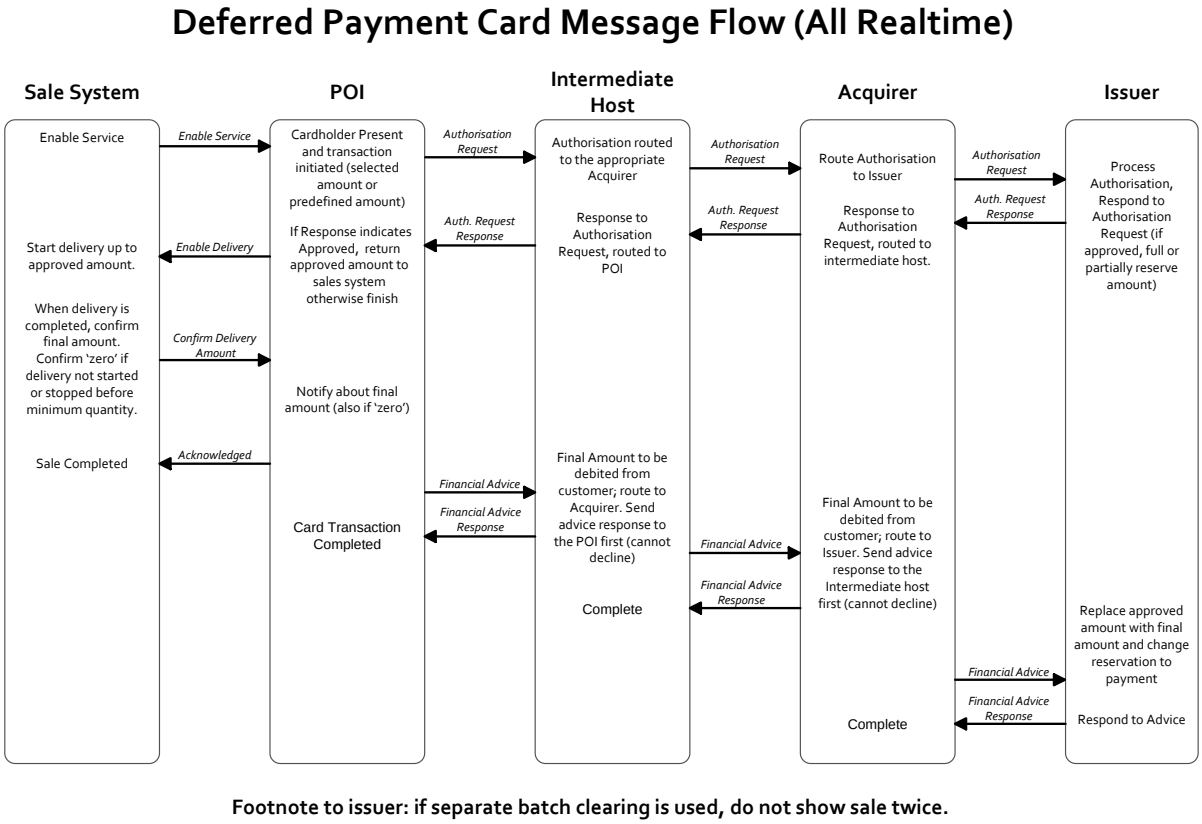


FIGURE 24: DEFERRED PAYMENT CARD MESSAGE FLOW

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. However, if a different card is used for Payment, then any amounts processed to other card(s) used for Pre-Authorisation shall be removed.

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.
- Payment completion for an equal or lesser amount than the amount previously Authorised when the final amount is known.

  Or

- As soon as it is known that a Pre-Authorisation and any Update Pre-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 identification (UID) which is created in the Pre-Authorisation transaction and reused in subsequent transactions.

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

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

Issuers shall adjust the “Open-to-Buy” 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 configurated overspent 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 25: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS

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.

3.5.2.3.1.1.1 Unattended environment

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

609 *3.5.2.4 Data Capture*

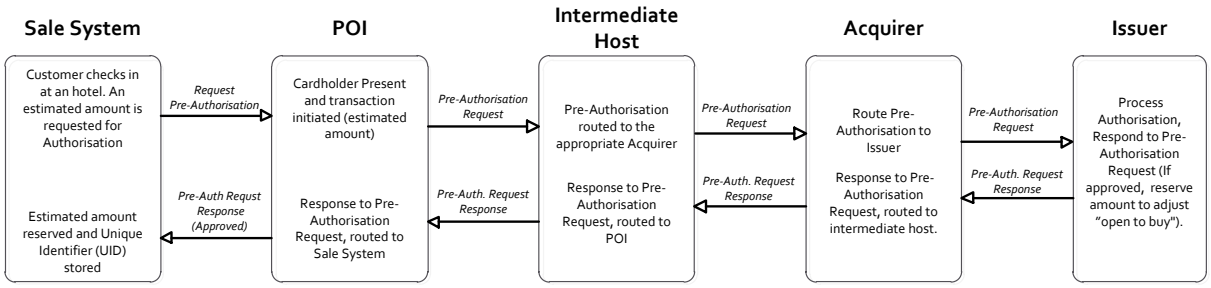
610 *3.5.2.4.1 Volume Conformant Implementation*

611 Card data can be retrieved from the Chip or the from stored data as defined in book2

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

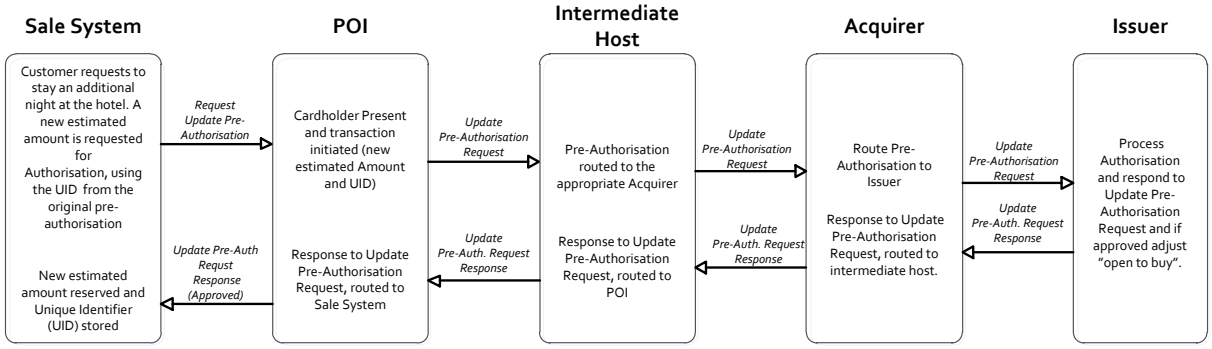
614 ### 3.5.3 Example of Message Flow

615 Examples of illustrative flows using Pre-Authorisation, update Pre-Authorisation and Payment
616 Completion can be seen below. Note that these constitute just one example of an implementation:



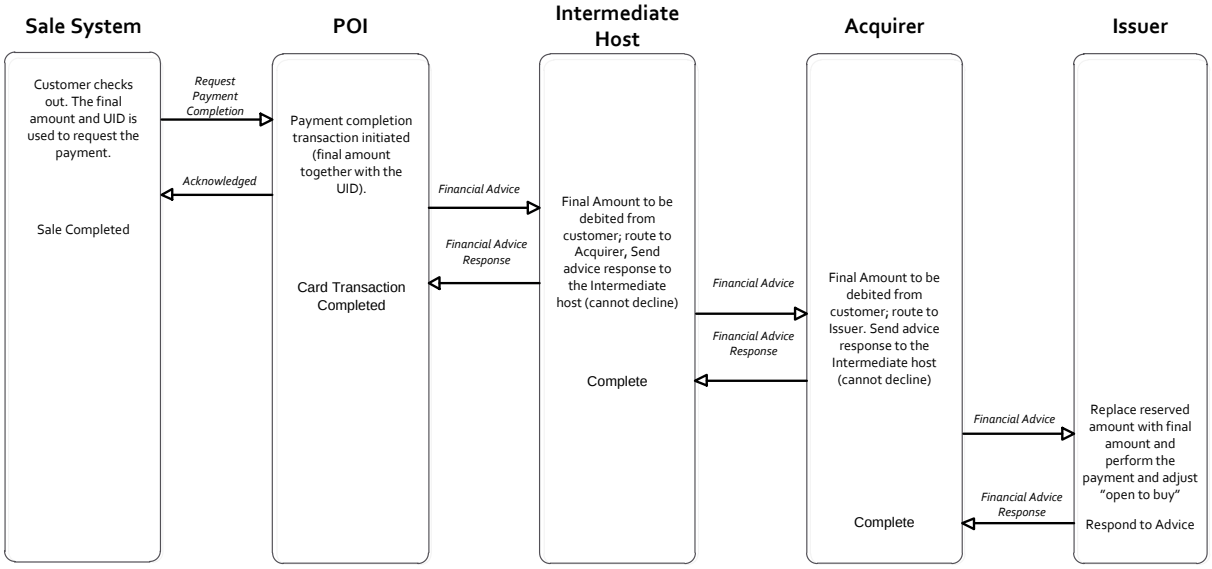
617 In the pre-authorisation request the presence of the UID is optional. In the pre-authorisation response the presence of UID is mandatory

618 Figure 26: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AN ESTIMATED AMOUNT,
619 CARDHOLDER PRESENT: PRE-AUTHORISATION



In the update pre-authorisation request and response the presence of the UID is mandatory.

Figure 27: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AN ESTIMATED AMOUNT, CARDHOLDER PRESENT: UPDATE PRE-AUTHORISATION



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

Figure 28: PRE-AUTHORISATION SERVICES IN AN ATTENDED OR UNATTENDED ENVIRONMENT TO RESERVE AND SECURE AN ESTIMATED AMOUNT, CARDHOLDER PRESENT: PAYMENT COMPLETION

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 with static authentication and 3 domain has been described in this book for e-commerce. This is because of the expected changes that 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 a consumer device accessing 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.
- Card Data Authentication is performed by the issuer verifying the static authenticator.
- Final amount is known at the time of the authorisation, however 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 addition 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 29: 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 30: 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 31: 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 32: 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[10]

Table 33: CARD SERVICES - VOLUME CONFORMANT IMPLEMENTATIONS FOR ATTENDED

For unattended environment:

Service	Issuers	Schemes	Acquirers	Acceptors
Payment	Required	Required	Required	Required

Table 34: 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.

[10] This service is optional awaiting a decision on a common approach

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 Flow

A typical message flow can be seen below. Note that this is just one example of an implementation:

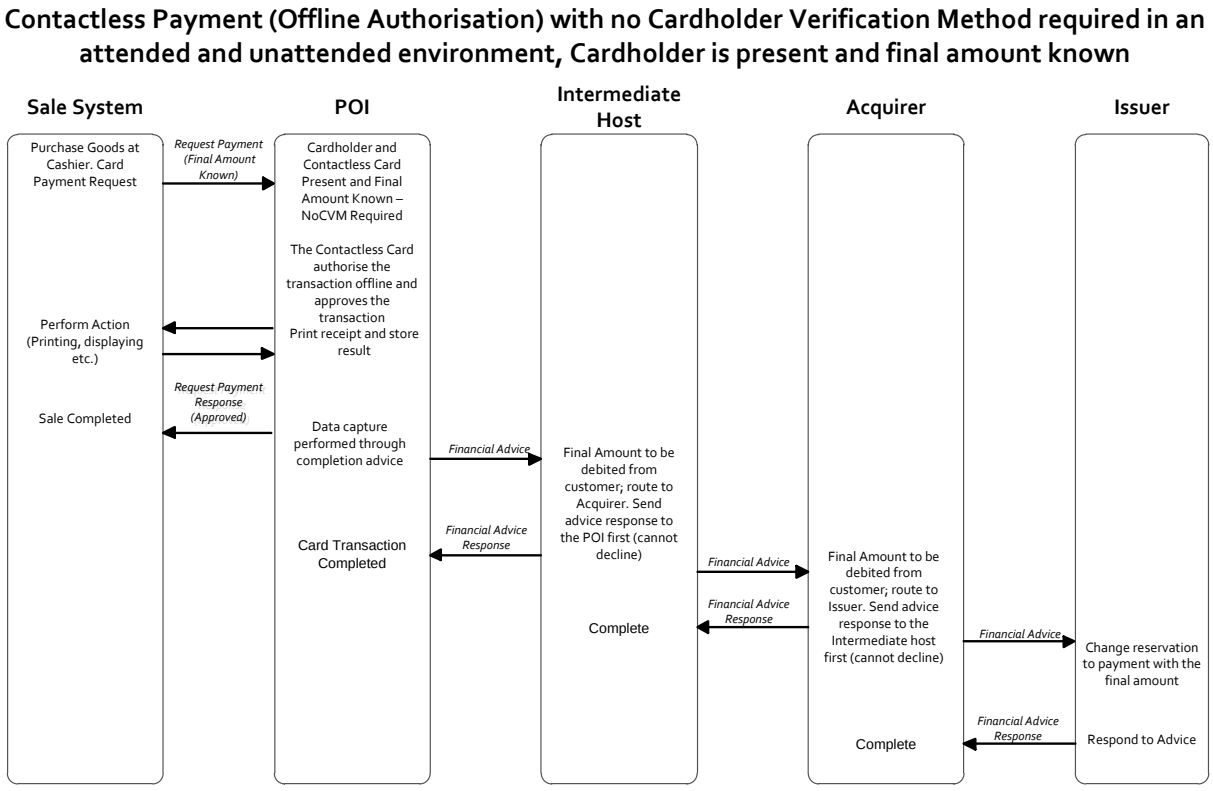


Figure 35: CONTACTLESS PAYMENT (OFFLINE AUTHORISATION)WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN

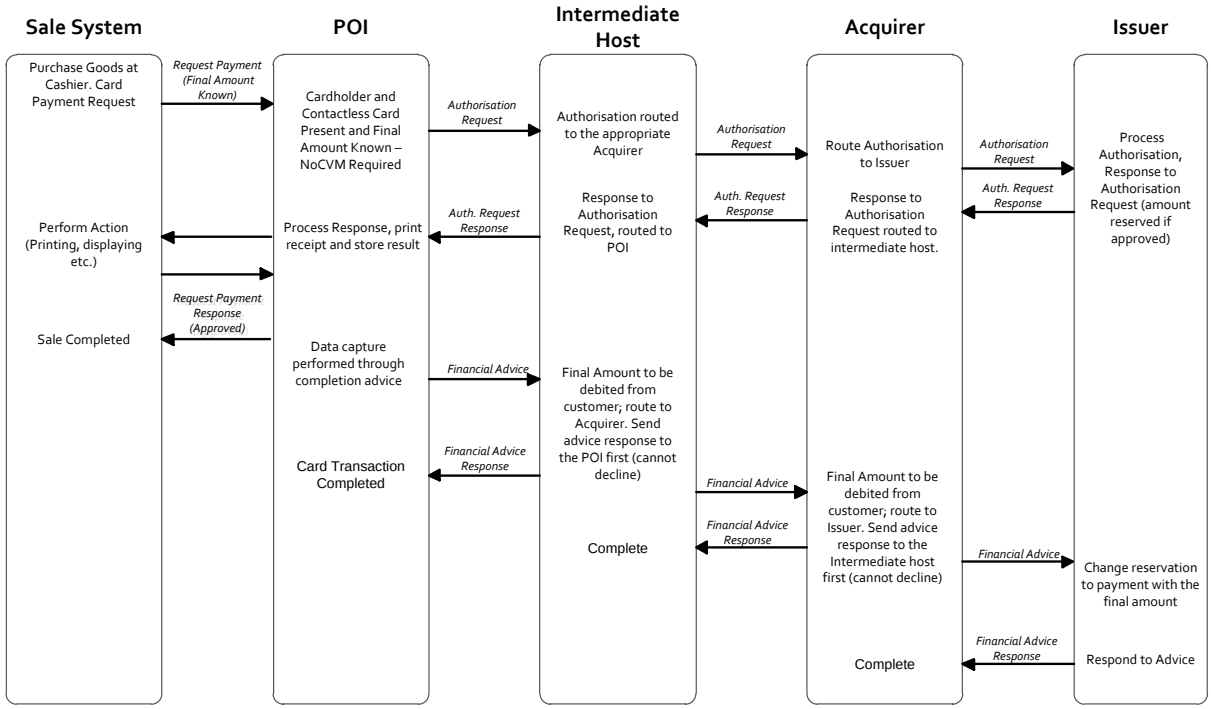


Figure 36: CONTACTLESS PAYMENT (ONLINE AUTHORISATION)WITH NO CARDHOLDER VERIFICATION METHOD REQUIRED IN AN ATTENDED AND UNATTENDED ENVIRONMENT, CARDHOLDER IS PRESENT AND FINAL AMOUNT KNOWN

4 FIGURES AND TABLES