

# Information about this New Guide

---

**New Guide** This *PayPass POS Host/Payment Software Implementation Guide*, dated September 2007, is an entirely new guide.

---

**Contents** This guide helps point-of-sale (POS) host/payment software developers and their customers to implement POS host/payment software applications that will ensure a quality consumer experience when using MasterCard® *PayPass*™ products.

Please refer to “[Using this Guide](#)” for a complete list of the contents of this guide.

---

**Billing** MasterCard will not bill principal members for this document.

---

**Questions?** If you have questions about this guide, please send an e-mail message to [paypass@mastercard.com](mailto:paypass@mastercard.com). Please refer to “[Using this Guide](#)” for more contact information.

---

**MasterCard is Listening...** Please take a moment to provide us with your feedback about the material and usefulness of the *PayPass POS Host/Payment Software Implementation Guide* using the following e-mail address:

[publications@mastercard.com](mailto:publications@mastercard.com)

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

---





# *PayPass* POS Host/Payment Software Implementation Guide

September 2007

## Proprietary Rights

The information contained in this document is proprietary and confidential to MasterCard International Incorporated, one or more of its affiliated entities (collectively “MasterCard”), or both.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

## Trademarks

Trademark notices and symbols used in this document reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

## Media

This document is available on [www.paypass.com](http://www.paypass.com).

MasterCard Worldwide  
2200 MasterCard Boulevard  
O’Fallon MO 63368-7263  
USA

1-636-722-6100

[www.mastercard.com](http://www.mastercard.com)

## Using this Guide

Purpose .....	1
Scope of These Requirements .....	1
Audience .....	1
Overview .....	2
Revisions .....	2
Related Information .....	2
Support .....	3
Effect of These Requirements .....	3

## Chapter 1 Software Development Guidelines

Overview .....	1-1
POS Host/Payment Application Software Configurations .....	1-1
Implementing the <i>PayPass</i> Specifications .....	1-4
Requirement 1: <i>PayPass</i> Transaction Data Editing .....	1-4
Requirement 2: Data Validation .....	1-4
Requirement 3: PCI DSS General Requirements .....	1-5
Requirement 4: <i>PayPass</i> Reader to POS Terminal Interface Requirements .....	1-5
Payment Processing .....	1-6
Requirement 5: Identification of <i>PayPass</i> Transactions and Terminal Capabilities .....	1-6
Requirement 6: Processing Time .....	1-7
Requirement 7: Indicating Payment Method .....	1-9
Requirement 8: <i>PayPass</i> Transaction Identification .....	1-9
Requirement 9: Authorization Message Changes .....	1-10
Requirement 10: Customer Receipts .....	1-12
Requirement 11: Terminal or POS Generated Transaction Reports .....	1-13
Requirement 12: Refunds and Reversals .....	1-13

## Chapter 2 Testing

*PayPass* POS Host/Payment Application Software Testing Cycles ..... 2-1

## Appendix A Requirements Summary

Requirements ..... A-1

---

## Using this Guide

*This chapter contains information that helps you understand and use this document.*

---

Purpose .....	1
Scope of These Requirements .....	1
Audience .....	1
Overview .....	2
Revisions .....	2
Related Information.....	2
Support .....	3
Effect of These Requirements .....	3



## Purpose

The MasterCard *PayPass POS Host/Payment Software Implementation Guide* helps point-of-sale (POS) host/payment software developers and their customers to implement POS host/payment software applications that will ensure a quality consumer experience when using MasterCard® *PayPass*™ products.

*PayPass* enables consumers to tap their *PayPass* card or device on *PayPass*-enabled terminals, allowing for a quicker and more convenient payment experience. These requirements

- Help POS software developers to understand *PayPass* and implement POS payment application that provide *PayPass* acceptance.
- Provide guidance on integrating *PayPass* functionality into retail systems.

## Scope of These Requirements

The requirements outlined in this document apply to all POS host/payment software applications that accept MasterCard *PayPass* products.

This document includes the requirements for implementing *PayPass* within a magnetic stripe card payment environment and an overview of the requirements for implementing *PayPass* within an EMV contact chip payment environment. It further describes the incremental changes required to enable merchants' POS host/payment application software to accept *PayPass* transactions.

## Audience

MasterCard provides this guide for members and their authorized agents.

Specifically, this guide is intended for POS host/payment software developers.

## Overview

The following table provides an overview of this guide.

Chapter	Description
Table of Contents	A list of the guide's chapters and subsections. Each entry references a chapter and page number.
Using this Guide	A description of the guide's purpose and its contents.
1 <a href="#">Software Development Guidelines</a>	This chapter provides guidelines about <i>PayPass</i> -compliant POS host/payment application software design and implementation.
2 <a href="#">Testing</a>	This chapter provides recommendations about testing.
A <a href="#">Requirements Summary</a>	This appendix provides a high-level summary of the requirements.

## Revisions

MasterCard periodically will issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a "Summary of Changes" describing how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appear at the right of each revision marker.

MasterCard may publish revisions to this document in a MasterCard bulletin, another MasterCard publication, or on MasterCard OnLine. A subsequent revision is effective as of the date indicated in that publication or on MasterCard OnLine and has precedence over any previous edition. In the event of a conflict between this document and a subsequently published edition, the subsequently published edition shall have precedence.

## Related Information

An overview of the requirements for implementing *PayPass* and background educational information is available in the *PayPass Product Guide*.

All other publicly available documents are available online at [www.paypass.com](http://www.paypass.com). Please check this site for the latest updated documents.

## Support

Please address your questions using the e-mail addresses listed.

<b>For information about...</b>	<b>Contact...</b>
<i>PayPass</i> products and procedures	<a href="mailto:paypass@mastercard.com">paypass@mastercard.com</a>
<i>PayPass</i> licenses	<a href="mailto:license@paypass.com">license@paypass.com</a>
<i>PayPass</i> specifications	<a href="mailto:specifications@paypass.com">specifications@paypass.com</a>
<i>PayPass</i> vendors	<a href="mailto:vendor_support@paypass.com">vendor_support@paypass.com</a>
<i>PayPass</i> testing and certification	<a href="mailto:testing@paypass.com">testing@paypass.com</a>
<i>PayPass</i> product approval by MasterCard Worldwide	<a href="mailto:approvals@paypass.com">approvals@paypass.com</a>

## Effect of These Requirements

These requirements are intended to provide general guidance to help POS host/payment software vendors develop or upgrade their POS host/payment application software to accept MasterCard *PayPass* transactions. The responsibility for the content and execution of any implementation for such developments will remain with the POS software vendors.

To the extent permitted by law, neither MasterCard Worldwide nor any of its affiliates, employees, or offices shall be liable to any recipient of these requirements, or any other third party for any loss, damages (including direct, special, punitive, exemplary, incidental or consequential damages), or costs (including attorneys' fees) which arise out of, or are related to these requirements. The foregoing limitation of liability shall apply to any claim or cause of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if MasterCard has been notified of the possibility of such damages or claim.

Where these requirements refer to the availability of services and/or documentation from MasterCard, the terms on which such services or documentation are made available shall be specified by MasterCard as and when such services or documentation are requested.



# 1

## Software Development Guidelines

*This chapter provides guidelines about PayPass-compliant POS host/payment application software design and implementation.*

---

Overview .....	1-1
POS Host/Payment Application Software Configurations .....	1-1
Implementing the <i>PayPass</i> Specifications .....	1-4
Requirement 1: <i>PayPass</i> Transaction Data Editing .....	1-4
Requirement 2: Data Validation .....	1-4
Requirement 3: PCI DSS General Requirements .....	1-5
Requirement 4: <i>PayPass</i> Reader to POS Terminal Interface Requirements.....	1-5
Payment Processing .....	1-6
Requirement 5: Identification of <i>PayPass</i> Transactions and Terminal Capabilities .....	1-6
Requirement 6: Processing Time.....	1-7
Requirement 7: Indicating Payment Method .....	1-9
Requirement 8: <i>PayPass</i> Transaction Identification.....	1-9
Requirement 9: Authorization Message Changes .....	1-10
Credit Authorization.....	1-10
Credit Clearing .....	1-11
Debit Authorization .....	1-11
Additional Debit Requirements .....	1-11
Requirement 10: Customer Receipts .....	1-12
Additional Consideration for Cardholder Name Field.....	1-13
Requirement 11: Terminal or POS Generated Transaction Reports .....	1-13
Requirement 12: Refunds and Reversals.....	1-13



## Overview

MasterCard *PayPass*<sup>™</sup> is a contactless payment feature developed by MasterCard that allows consumers to make Tap & Go<sup>™</sup> payments without having to hand over or swipe a payment card. *PayPass* is ideal for those environments where speed and convenience are valued—for example, at fuel pumps, quick-service restaurants (QSRs), drive-thrus, convenience stores, vending machines, and toll booths.

MasterCard *PayPass* cards appear similar to standard MasterCard cards, except that they include the *PayPass* identifier on the front and a shorter signature panel, as used for chip cards, on the back. However, in addition to a magnetic stripe on the back, embedded inside the card there is a contactless chip that stores and processes the payment account data and a connected antenna that typically runs around the perimeter of the card.

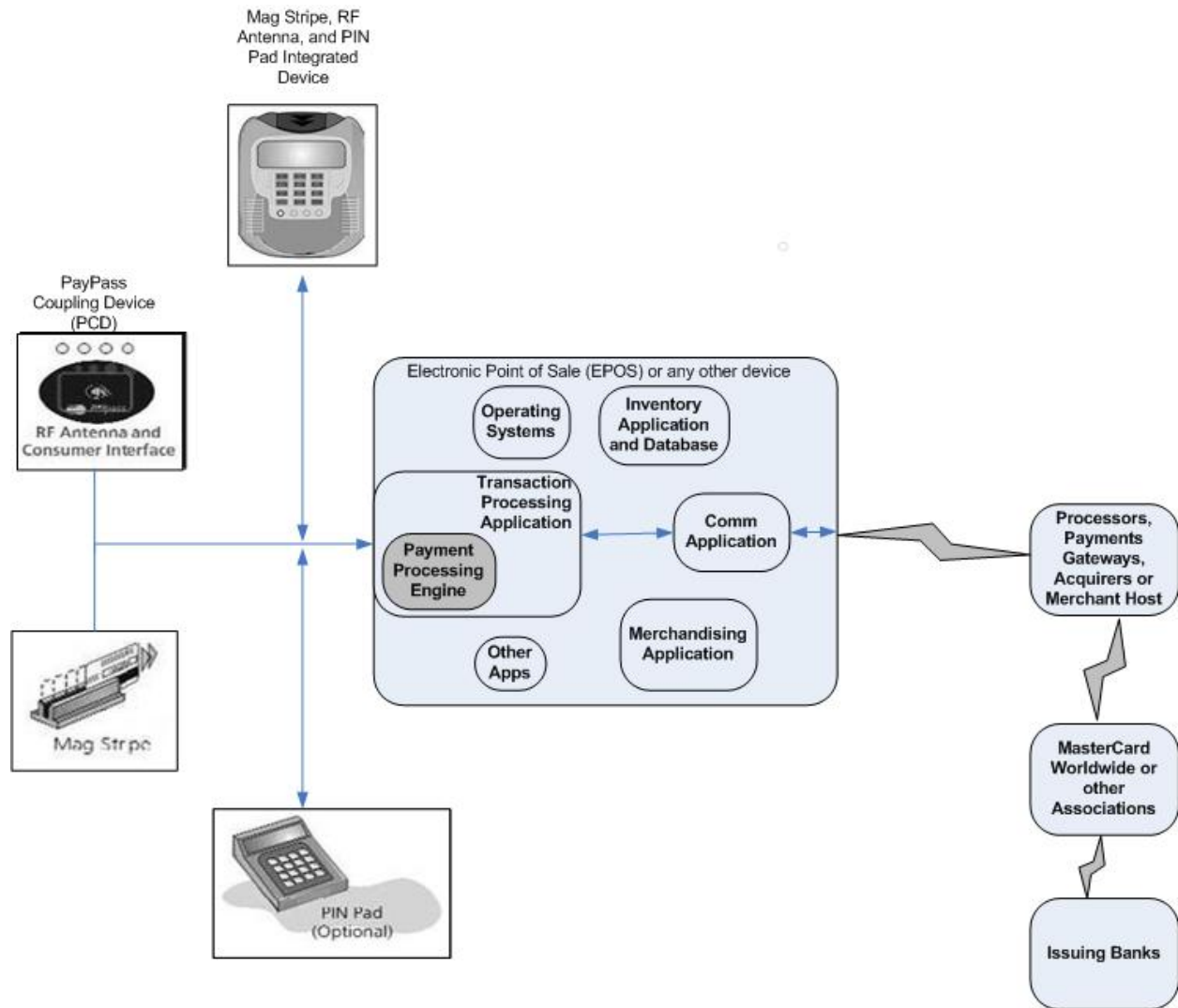
To make a payment, the consumer simply taps their *PayPass* card or device on a *PayPass* reader. The details are read from the card or device using the contactless interface, and an enhanced payment transaction is then performed over the standard magnetic stripe network infrastructure.

There are a number of ways in which *PayPass* can be implemented, so compliance with these requirements will ensure the optimal level of quality for MasterCard *PayPass* POS host/payment application software.

## POS Host/Payment Application Software Configurations

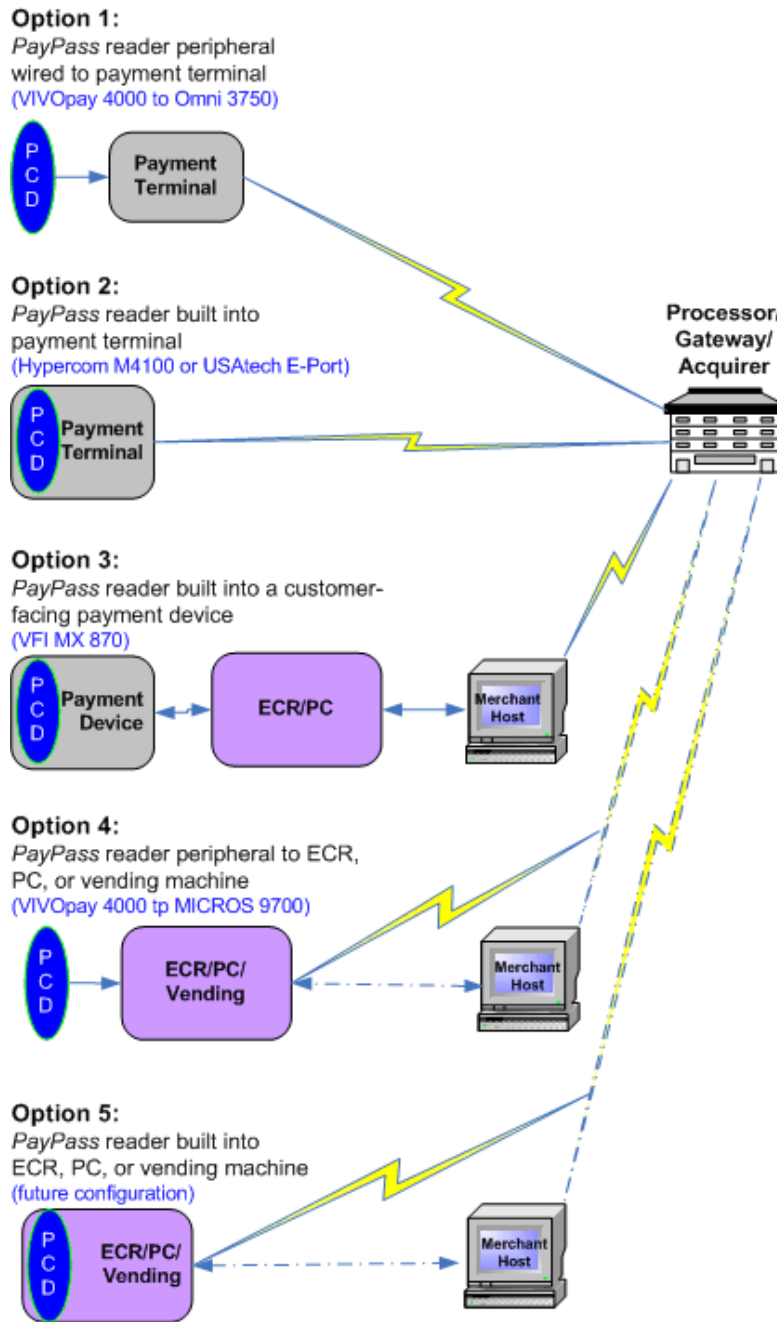
*PayPass* acceptance functionality may be included within, or added to, existing POS host/payment application software in a number of ways. For the purpose of these requirements, a functional block diagram of a *PayPass* acceptance terminal system is shown in [Figure 1.1](#).

Figure 1.1—PayPass Payment Processing Systems Data Flow



*PayPass* terminals can be configured in any of the following five ways, as shown in Figure 1.2.

**Figure 1.2—*PayPass* Terminal Configurations**



**PCD – PayPass Coupling Device**

## Implementing the *PayPass* Specifications

This section provides details about specific requirements for designing *PayPass*-enabled POS host/payment application software. These requirements must be fulfilled by the POS host/payment application software and, where appropriate, other components of the POS system. Refer to [Appendix A](#) for a list summarizing these requirements.

The basic requirements are as follows:

- *PayPass* POS host/payment application software should interface with all MasterCard certified *PayPass* terminals and device readers either wired or wireless.
- To ensure an acceptable cardholder experience the interaction between the *PayPass* cardholder card or device and the POS terminal must complete in as short a time as possible.

Details of specific requirements are listed in the following subsections.

### Requirement 1: *PayPass* Transaction Data Editing

**All *PayPass* transaction data received from the *PayPass* reader, with the exception of any processing requirements specified in the relevant application specification, must be presented to the processor, payment gateway, merchant host, or acquirer host without any modification.**

Issuers use *PayPass* transaction data received from the *PayPass* reader during any online authorization to validate that the card is genuine; therefore, all *PayPass* data retrieved from the *PayPass* card or device must be presented to the processor, payment gateway, merchant host, or acquirer host without any modification. Unspecified modification of data may result in the transaction being declined during online authorization.

### Requirement 2: Data Validation

**No additional data validation is required by the existing POS/host payment application through the introduction of *PayPass* functionality, unless required by the *PayPass* application specifications.**

The introduction of *PayPass* does not require any additional data validation to be performed unless specifically stated in the *PayPass* application specifications.

Data validation carried out by any existing POS host/payment application terminal functionality before *PayPass* has been implemented is not affected by the introduction of *PayPass*.

## Requirement 3: PCI DSS General Requirements

**A company that is processing card payments must be compliant with the Payment Card Industry (PCI) Data Security Standards (DSS). Companies that are not compliant with these security standards risk losing the ability to process credit card payments.**

The PCI Data Security Standards represent a common set of industry tools and measurements to help ensure the safe handling of sensitive information.

Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with the MasterCard Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process—including preventing, detecting and reacting to security incidents.

Merchants and service providers must either validate compliance with an audit by a PCI DSS Qualified Security Assessor (QSA) or via self assessment.



**Note**

For more information about the PCI Data Security Standard, go to [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

## Requirement 4: *PayPass* Reader to POS Terminal Interface Requirements

**The POS/host payment application software must not buffer or store card data. The terminal should accept *PayPass* card data only after the payment stage of the sales transaction process begins.**

The POS host/payment application software must not buffer or store card details in advance of a new transaction starting. The sales transaction must have started before any card details are captured. This is to ensure that details from a previous transaction are not mistakenly used.

## Payment Processing

Processing MasterCard payment transactions that have been obtained using the *PayPass* interface is fundamentally the same as processing the payment details obtained by swiping the magnetic stripe of a traditional card, or processing via a contact EMV interface, with the underlying scheme and payment product rules defining the process and requirements. However, there are some significant variations that the POS host/payment application software must provide.

### Requirement 5: Identification of *PayPass* Transactions and Terminal Capabilities

**The POS host/payment application software must be capable of providing information to any connected system on the payment read process (magnetic swipe, contact chip read, contactless (*PayPass*) read) for each payment transaction.**

The acquirer of the transaction is required to provide confirmation to MasterCard and issuers of *PayPass* cards and devices that:

- The payment was transacted using the *PayPass* interface.
- The terminal was capable of transacting with a *PayPass* interface.

MasterCard has defined the process by which the acquirer communicates data through the MasterCard Banknet® telecommunications network and the Global Clearing Management System (GCMS). However, MasterCard does not specify the process for merchants to transfer this information to the acquirer because the data communications standards vary.

As a result, the POS host/payment application software should provide functionality that identifies the payment read process (that is, magnetic stripe swipe, contact chip read, or contactless (*PayPass*) read) for each payment transaction. This information should be provided to the acquirer with each transaction, in a manner and format agreed upon with the acquirer.

## Requirement 6: Processing Time

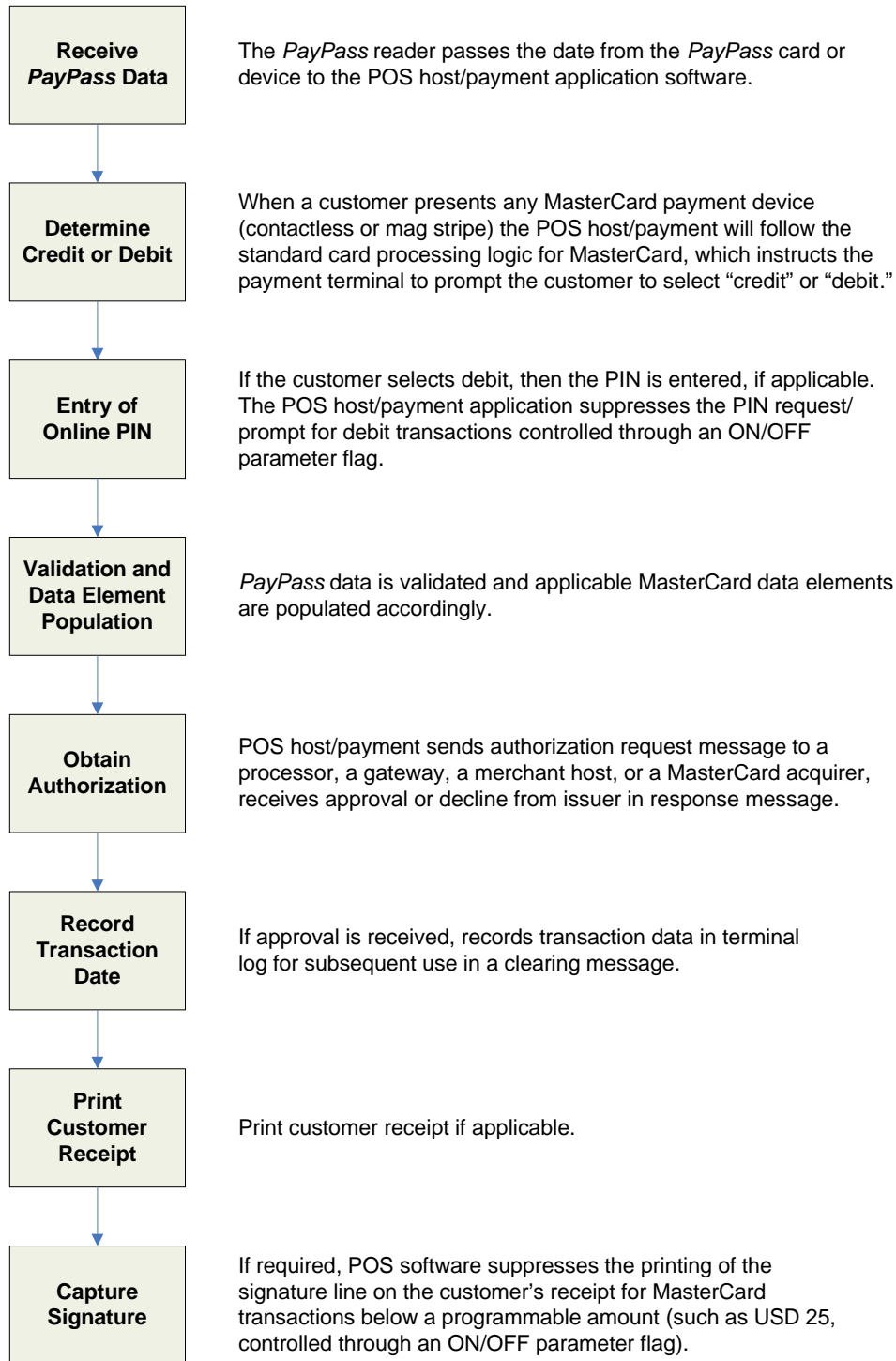
**It is important to ensure that the complete system facilitates a fast payment process for *PayPass* transactions.**

The specific configuration of the POS host/payment application software supporting *PayPass* is left open to accommodate differing merchant requirements; however, it is important to ensure that the complete system facilitates a fast payment process for *PayPass* transactions.

This increased speed for payment processing is a key component supporting the merchant's business case and "The Simpler Way to Pay" proposition that *PayPass* delivers.

[Figure 1.3](#) illustrates the processing flow of typical payment application software.

Figure 1.3—PayPass Payment Application Software Processing flow



## Requirement 7: Indicating Payment Method

**The POS host/payment application needs to set an indicator in the terminal-to-host transaction request message indicating which method (tapped (contactless) or swiped) was used to initiate the payment.**

Integration of the *PayPass* reader into the POS system should require minimal software changes in the POS terminal or host/payment application software. The format of the customer account data that is read wirelessly is the same as if it were read via card swipe. Therefore, the POS system simply passes the data to the POS host/payment software in the same fields that it uses for magnetic stripe card data.

The POS host/payment software detects whether the *PayPass* card was tapped (contactless) or swiped, so the POS host/payment application software needs to set an indicator in the terminal-to-host transaction request message indicating which method was used.

The host needs to know that a MasterCard transaction was tapped rather than swiped so the appropriate indicators can be set in the MasterCard authorization request message. As indicated in requirement 9, MasterCard has specified new values for indicating the following:

- The terminal's reading capabilities.
- The actual entry mode for the transaction.

MasterCard is also requiring these new indicators to be passed through the settlement system for credit clearing, so POS host/payment applications need to forward the indicators to the merchant's processor or acquirer in their daily settlement file.

## Requirement 8: *PayPass* Transaction Identification

**Provide the required logical communication interface between the certified MasterCard *PayPass* readers and your POS host/payment application if applicable.**

The POS host/payment software and configuration changes required to implement *PayPass* are as follows:

- The POS host/payment application software requires the POS reader terminal to identify *PayPass* transactions and indicates which tracks are being sent in the request message.
- Developers must specify that the terminal sets the value of the Origin Indicator in the transaction request message to new values to indicate the presence of Track 1, Track 2, or both Track 1 and Track 2.

- The POS host/payment application software must be modified to recognize the new values. Additionally, the software must pass these Origin Indicator values through to a potential Mapper or Reformatter module, so that the appropriate indicators can be set in the authorization message.
- If a *PayPass* card is used to initiate a transaction via card swipe rather than by contactless, the POS host/payment software sets the value of the Origin Indicator to the existing values. In this scenario, the transaction will be processed just like any other swiped MasterCard transaction.

## Requirement 9: Authorization Message Changes

**MasterCard requires that Data Elements 22 and 61 be populated accordingly for authorization of contactless transactions.**

MasterCard requires that the following values to be used for Data Elements 22 and 61 for authorization of contactless transactions.

### Credit Authorization

MasterCard requires that *PayPass* transactions be coded as follows for credit authorization.

#### Data Element 22

Data Element (DE) 22 (Point of Service [POS] Entry Mode), subfield 1 (POS Terminal Primary Account Number [PAN] Entry Mode) must contain:

- The value of “91” indicating PAN auto-entry mode via contactless magnetic stripe (*PayPass*-mag stripe).
- The value of “7” indicating PAN auto-entry via contactless M/Chip (*PayPass*-M/Chip).

#### Data Element 61

DE 61 (Point of Sale [POS] Data), subfield 11 (POS Card Data Terminal Input Capability) must contain:

- The value of “4” to indicate contactless magnetic stripe (*PayPass*-mag stripe only capability, for example, No *PayPass*-M/chip capability).
- The value of “3” to indicate contactless M/Chip (*PayPass*-M/Chip and *PayPass*-mag stripe capability, for example, Both can be processed).

## Credit Clearing

MasterCard requires that *PayPass* transactions must be coded as follows for credit clearing.

Data Element 22, subfield 1 (POS Terminal Primary Account Number [PAN] Entry Mode) must contain:

- The value of “A” indicating Clearing Proximity Chip Online transaction (*PayPass*-mag stripe only capability, [for example, No *PayPass*-M/Chip capability]).
- The value of “M” to indicate Clearing Proximity Chip EMV transaction (*PayPass*-M/Chip and *PayPass*-mag stripe capability [for example, Both can be processed]).

Data Element 22, subfield 7 (Card Data: Input Mode) must contain:

- The value of “A” indicating PAN auto-entry mode was via contactless magnetic stripe (*PayPass*-mag stripe).
- The value of “M” indicating PAN auto-entry mode was via contactless M/Chip (*PayPass*-M/Chip-contactless M/Chip).

## Debit Authorization

MasterCard also provides *PayPass* to MasterCard debit cards. To support the requirements necessary to identify these transactions, the MasterCard® Debit Switch (MDS) supports specific values in the financial request message and in the 250-byte reconciliation file.

When a customer presents any MasterCard payment card or device, contactless or mag stripe, the POS host/payment software follows the standard card processing logic for MasterCard, which instructs the Payment terminal to prompt the customer for “Credit or Debit.” When the customer selects “Debit” and then enters the PIN, the transaction is sent to the merchant’s host.

To accommodate *PayPass* debit processing, the POS host/payment application software needs to provide a mechanism to suppress the PIN request/prompt for debit transactions. This feature should be available via an ON/OFF parameter flag.

## Additional Debit Requirements

MasterCard has included two values in DE 22 that indicate the method used to enter the PAN into the terminal and two values in DE 61 that indicate the terminal input capability. These requirements apply both to members that are serviced through the MDS and to all other debit networks and processors.

MasterCard requires that *PayPass* debit transactions must be coded as follows:

#### Data Element 22

DE 22, subfield 1 (POS Terminal PAN Entry Mode), positions 1–2, must contain:

- The value of “91” indicating PAN auto-entry mode via contactless magnetic stripe (*PayPass*-Mag stripe). The edits for value “91” are the same as the edits when DE 22, subfield 1 = 90
- The value of “07” indicating PAN auto-entry via contactless M/Chip (*PayPass*-M/Chip). The edits for value “07” are the same as the edits when DE 22, subfield 1 = 05

#### Data Element 61

DE 61, subfield 11 (POS Card Data Terminal Input Capability Indicator), position 11, must contain:

- The value of “4” to indicate contactless magnetic stripe (*PayPass*-mag stripe only capability, for example, No *PayPass*-M/chip capability)
- The value of “3” to indicate contactless M/Chip (*PayPass*-M/Chip and *PayPass*-mag stripe capability, for example, Both can be accepted)



#### Note

**A *PayPass* M/Chip card or device can be accepted at a *PayPass* magnetic stripe terminal. At a magnetic stripe terminal, the M/Chip card or device emulates a *PayPass* magnetic stripe card or device.**

## Requirement 10: Customer Receipts

**The POS host/payment application software transaction receipt module needs to be modified to suppress the printing of the signature line on the customer’s receipt.**

As with existing transactions, the POS host/payment application software determines if a receipt should be printed. Additionally, the customer may request a receipt. When a receipt is printed, the input method used for the transaction is identified. This helps both the consumer and the merchant identify to identify that the transaction was a *PayPass* transaction, in the event of a refund.

POS host software transaction receipt application module needs to be modified to suppress the printing of the signature line on the customers receipt for MasterCard transactions below a programmable amount (such as USD 25). This feature should be available via an ON/OFF parameter flag.

If the POS software prints a receipt, the input method is shown as “Contactless,” “CONTACTLESS,” “*PayPass*,” or “RFID” (Radio Frequency Identification) for *PayPass* transactions.

### **Additional Consideration for Cardholder Name Field**

As a security precaution against potential identity theft, the cardholder name field is not included in the card data obtained from the chip of a *PayPass* mag stripe card. If the field is populated, it may contain “not include.”



**Note**

***PayPass* cards are not required to include the cardholder name in Track 1 data. POS systems that normally obtain and make use of the cardholder name from Track 1 data obtained from a magnetic stripe read may need to accommodate this difference.**

## **Requirement 11: Terminal or POS Generated Transaction Reports**

**Any POS or merchant systems or reports should specifically identify *PayPass* transactions.**

To simplify transaction queries, the method of data input needs to be recorded on all transaction logs or reports produced by POS terminals or merchant systems.

## **Requirement 12: Refunds and Reversals**

**If a payment transaction was originated by a *PayPass* card or device, the merchant allows a transaction refund to be completed by the same *PayPass* card or device.**

MasterCard acceptance rules state the following:

- If a card acceptor issues a credit for the returned goods or cancelled services, it must apply the credit to the same MasterCard account that the cardholder used to purchase the goods or services.
- The card acceptor must not issue cash or check refund for goods or services purchased using MasterCard.

To adhere to these acceptance rules, merchants that accept *PayPass* cards or devices must be able to perform refunds using *PayPass* cards or devices.



---

# 2

## Testing

*This chapter provides recommendations about testing.*

---

*PayPass* POS Host/Payment Application Software Testing Cycles ..... 2-1



## PayPass POS Host/Payment Application Software Testing Cycles

There are no specific requirements for MasterCard *PayPass* POS host/payment application software certification. However, POS software vendors are encouraged to perform Unit, System, Situational, PCI Compliance, Regression, User Acceptance/Quality assurance, and Pilot testing to ensure that the POS host/payment application software performs per specifications.

Application testing is a critical phase of a development methodology. After specification coding has been completed, application developers should perform unit testing to ensure that the *PayPass* payment specifications and requirements have been met as a stand-alone application.

Usually, unit testing is followed by system testing. During system testing, *PayPass* host/payment application software is tested in conjunction with other applications in the unit (POS terminal or ECR). Specific testing of data exchange, hand-off, and interaction with other applications in the payment system or sub-system is recommended.

The “situational” testing includes testing scenarios such as unplugging the connecting cable from the *PayPass* terminal, powering off the *PayPass* terminal in the middle of a transaction, or presenting the *PayPass* card to the *PayPass* terminal multiple times for the same transaction.

The next testing phase may be PCI compliance and regression testing where the *PayPass* host/payment application software is tested against a set of pre-defined test scenarios to ensure that all the existing payment application functionality still works. Note all the new *PayPass* test cases must be included in the regression test suite for future regression testing.

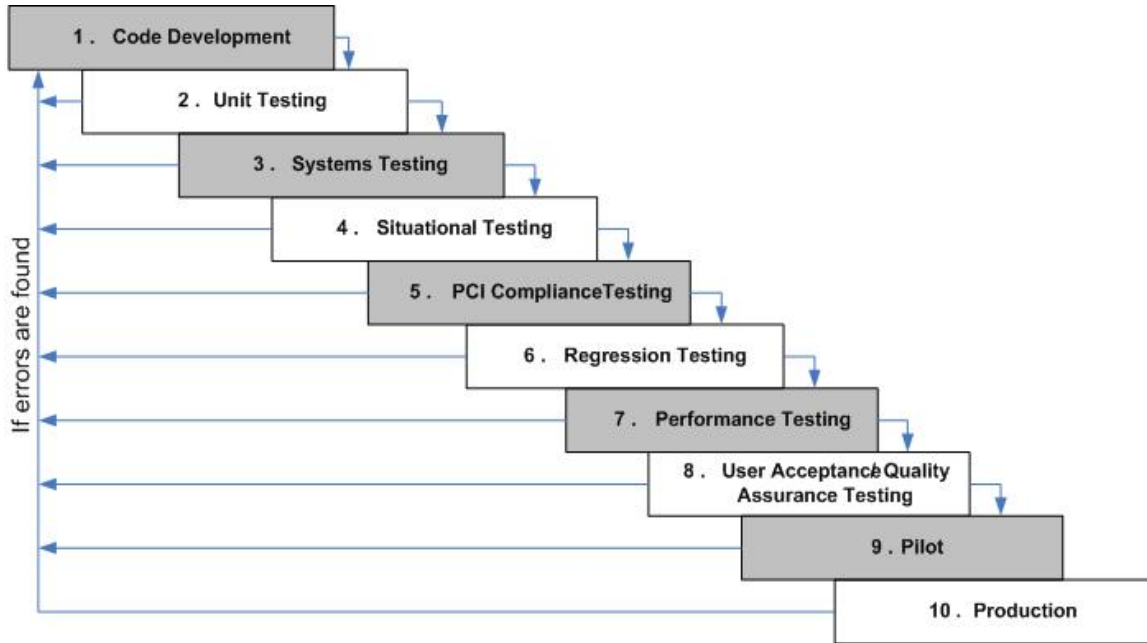
The performance testing needs to be conducted to ensure the POS host/payment application software does not impact the authorization time/length.

The last testing phase is User Acceptance Testing (UAT) or Quality Assurance Testing where usually non-developers or professional testers test the entire payment system from a user/customer point-of-view.

MasterCard recommends that software vendors pilot the first implementation in a controlled environment (merchant) to evaluate system performance before a large deployment.

Figure 2.1 illustrates the specific POS payment application software development testing cycles.

Figure 2.1—Testing Cycles



---

# A

## Requirements Summary

*This appendix provides a high-level summary of the requirements.*

---

Requirements .....	A-1
--------------------	-----



## Requirements

Requirement Description	Detailed Requirement
1. <i>PayPass</i> Transaction Data Editing	All <i>PayPass</i> transaction data received from the <i>PayPass</i> reader, with the exception of any processing requirements specified in the relevant application specification, must be presented to the processor, payment gateway, merchant host, or acquirer host without any modification.
2. Data Validation	No additional data validation is required by the existing POS payment application through the introduction of <i>PayPass</i> functionality, unless required by the <i>PayPass</i> application specifications.
3. PCI DSS General Requirements	A company that is processing card payments must be compliant with the Payment Card Industry (PCI) Data Security Standards (DSS). Companies that are not compliant with these security standards risk losing the ability to process credit card payments.
4. <i>PayPass</i> Reader to POS Terminal Interface Requirements	The POS host/payment application software must not buffer or store card data. The terminal should accept <i>PayPass</i> card data only after the payment stage of the sales transaction process begins.
5. Identification of <i>PayPass</i> Transactions and Terminal Capabilities	The POS host/payment application software must be capable of providing information to any connected system on the payment read process (magnetic swipe, contact chip read, contactless ( <i>PayPass</i> ) read) for each payment transaction.
6. Processing Time	It is important to ensure that the complete system facilitates a fast payment process for <i>PayPass</i> transactions.
7. Indicating Payment Method	The POS host/payment application needs to set an indicator in the terminal-to-host transaction request message indicating which method (tapped (contactless) or swiped) was used to initiate the payment.
8. <i>PayPass</i> Transaction Identification	Provide the required logical communication interface between the certified MasterCard <i>PayPass</i> readers and your POS host/payment application if applicable.
9. Authorization Message Changes	MasterCard requires that Data Elements 22 and 61 be populated accordingly for authorization of contactless transactions.
10. Customer Receipts	The POS host/payment application software transaction receipt module needs to be modified to suppress the printing of the signature line on the customer's receipt.
11. Terminal or POS Generated Transaction Reports	Any POS or merchant systems or reports should specifically identify <i>PayPass</i> transactions.
12. Refunds and Reversals	If a payment transaction was originated by a <i>PayPass</i> card or device, the merchant allows a transaction refund to be completed by the same <i>PayPass</i> card or device.