



# PayPass - M/Chip Requirements

5 December 2011

---

## Notices

### 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 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.

### Billing

For printed documents, MasterCard will bill principal members. Please refer to the appropriate *MasterCard Consolidated Billing System* (MCBS) document for billing-related information.

### Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, excerpted text, and contact information—on the Member Publications Support page available on MasterCard OnLine®. Go to Member Publications [Support](#) for centralized information.

### Translation

A translation of any MasterCard manual, bulletin, release, or other MasterCard document into a language other than English is intended solely as a convenience to MasterCard members and other customers. MasterCard provides any translated document to its members and other customers “AS IS” and makes no representations or warranties of any kind with respect to the translated document, including, but not limited to, its accuracy or reliability. In no event shall MasterCard be liable for any damages resulting from members’ and other customers’ reliance on any translated document. The English version of any MasterCard document will take precedence over any translated version in any legal proceeding.

### Address

MasterCard Worldwide  
Chaussée de Tervuren, 198A  
B-1410 Waterloo, Belgium  
email: [specifications@paypass.com](mailto:specifications@paypass.com)

---

# Table of Contents

<b>Chapter 1 Using This Manual .....</b>	<b>1-i</b>
Purpose.....	1-1
Scope.....	1-1
Audience.....	1-2
Overview .....	1-2
Language Use .....	1-3
Requirements and Best Practices .....	1-3
Terminology.....	1-4
Reference Information .....	1-5
Conventions.....	1-5
<b>Chapter 2 PayPass Introduction .....</b>	<b>2-i</b>
Introduction.....	2-1
Participation.....	2-1
PayPass Operating Modes.....	2-2
PayPass Cards .....	2-2
PayPass Transaction Types .....	2-2
PayPass Acceptance.....	2-3
PayPass Transaction Flow.....	2-4
Other Transaction Types and Environments.....	2-7
<b>Chapter 3 Issuer Requirements .....</b>	<b>3-i</b>
General Requirements .....	3-1
Card Requirements .....	3-1
Card Delivery.....	3-13
Issuer Host Requirements .....	3-13
Clearing Requirements.....	3-15
Chargeback and Exception Processing .....	3-16
<b>Chapter 4 Acquirer Requirements.....</b>	<b>4-i</b>
General Requirements .....	4-1
Terminals .....	4-2
Offline Card Authentication.....	4-10

## Table of Contents

---

Cardholder Verification .....	4-11
Terminal Risk Management.....	4-14
Terminal Action Codes (TACs).....	4-14
Authorization Responses.....	4-14
Receipts .....	4-15
Subsequent Contact Transactions.....	4-15
Terminated Transactions .....	4-16
Cardholder Activated Terminals.....	4-16
Automated Teller Machines .....	4-17
Acquirer Network Requirements.....	4-18
Authorization Requirements.....	4-19
Clearing Requirements.....	4-19
Exception Processing.....	4-20
On-behalf Services.....	4-21
<b>Chapter 5 Data Requirements .....</b>	<b>5-i</b>
Terminal Action Codes .....	5-1
Offline Only Terminals .....	5-3
Payment Scheme Specific Data Objects.....	5-5
Application Capabilities Information .....	5-6
<b>Appendix A Abbreviations .....</b>	<b>A-i</b>
Abbreviations.....	A-1

---

## Chapter 1 Using This Manual

*This chapter provides information on the purpose, overview, reference information, and conventions used.*

---

Purpose.....	1-1
Scope .....	1-1
Audience.....	1-2
Overview .....	1-2
Language Use .....	1-3
Requirements and Best Practices .....	1-3
Terminology.....	1-4
Reference Information .....	1-5
Conventions.....	1-5



---

## Purpose

This document provides the MasterCard requirements and best practices for issuers and acquirers when using contactless chip technology with their MasterCard *M/Chip*<sup>™</sup> products.

It contains the requirements relating to MasterCard®, Debit MasterCard and Maestro® *PayPass*<sup>™</sup> card programs, and the requirements for performing contactless payment transactions at attended Point of Sale (POS) terminals, ATMs and Cardholder Activated Terminals (CAT).

This document does not provide an introduction to *PayPass* or explanation as to how *PayPass* works, nor does it duplicate or reproduce existing standards such as EMV or the existing MasterCard requirements for other technologies. The purpose of the manual is to:

- Define the *PayPass* requirements that MasterCard has established for use with MasterCard brands
- Propose recommendations that constitute best practices for *PayPass* implementations
- Define when and how the functions must be used as a requirement or should be used as a best practice

## Scope

This document does not discuss general brand rules or requirements, except to explain how certain rules are implemented in *PayPass*.

In general, the brand rules continue to apply to *PayPass* transactions except when modified for *PayPass* and as explained in this document. For example, chargeback rights are the same for *PayPass* except in connection with the chargeback protection limits described here. For full details of the rules and requirements for specific card brands, refer to the relevant brand-specific documentation on MasterCard OnLine (see the *Reference Information* below).

These requirements have been written for *PayPass - M/Chip* so also cover the *PayPass - Mag Stripe* requirements.

## Using This Manual

### Audience

---

This document does not introduce new technical requirements that are not already included in the existing card and reader specifications. The following products, services, or environments are not in the scope of this document because they are already addressed in other dedicated documents:

- Card Application Specifications (for example, *PayPass - M/Chip Flex*, *PayPass - M/Chip 4*)
- Terminal and reader specifications
- Contact card interface and transactions (for example, *M/Chip Requirements*)
- Personalization Data
- Data Storage applications used with *PayPass*
- Transit specific *PayPass* implementations
- MasterCard Cash

## Audience

This document is intended for use by MasterCard customers and product vendors involved in *PayPass* implementation projects who already have a general understanding of how the contactless chip product works.

The target audience includes:

- Staff working on *PayPass - M/Chip* implementation projects
- Operations staff who need to understand the impact of *PayPass* on their activities

## Overview

This document supports issuers and acquirers implementing *PayPass - M/Chip*. It details the requirements and best practices for effective deployment of *PayPass* solutions.

The following table provides an overview of the chapters in this manual:

Chapter	Description
Chapter 1: Using this Manual	This chapter contains information that helps you understand and use this document.
Chapter 2: Introduction	This chapter introduces the basic principles of <i>PayPass</i> .
Chapter 3: Issuer Requirements	This chapter details the requirements from an issuer perspective including requirements for configuring cards and devices.
Chapter 4: Acquirer Requirements	This chapter details the requirements from an acquirer perspective including requirements for terminals and networks.
Chapter 5: Data Requirements	This chapter lists values of certain data elements that are not defined in other documents (for example, the <i>PayPass Personalization Data Specifications</i> )

## Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in Webster's New Collegiate Dictionary.

An exception to the above concerns the spelling of proper nouns. In this case, we use the local English spelling.

Requirements are documented using the following definitions:

- **Must**—indicates a mandatory requirement
- **Should**—indicates a recommendation or best practice
- **May**—defines a product or system capability that is optional or a statement that is informative only

## Requirements and Best Practices

Requirements, as identified in this document, are functional elements which must be implemented as stated in the text to achieve the required level of acceptance for MasterCard or Maestro branded *PayPass* cards on *PayPass*-enabled terminals.

Requirements are always expressed using the word **must**. Requirements are contained in tables and are indicated by a capital R in the left column.

Best practices are MasterCard recommendations for the best ways to implement different options. If customers choose not to follow them, their *PayPass* implementation will still work but may not be as effective or efficient as it could be.

Best practices are written using the word **should**. Best practices are formatted in the same way as requirements but are preceded by the letters BP.

Requirements and best practices include an indication of whether they apply to all products or just to the MasterCard or Maestro brand.

<b>R</b>	<b>All</b>	Requirement applies to all <i>PayPass</i> cards or terminals.
<b>R</b>	<b>MC</b>	Requirement applies to MasterCard branded <i>PayPass</i> cards or terminals.
<b>R</b>	<b>MS</b>	Requirement applies to Maestro branded <i>PayPass</i> cards or terminals.

## Terminology

### PayPass Cards and Devices

*PayPass* devices can be issued in form factors other than that of a traditional payment card, for example: mobile phones, key fobs, watches. Throughout this document a reference to *PayPass* cards includes other devices unless specifically excluded.

A dual interface card refers to a chip card that can perform both contact and *PayPass* transactions.

### PayPass Terminals and Readers

Functionality for the acceptance of *PayPass* cards may be provided by the *PayPass* reader or by the accompanying POS terminal. Throughout this document a reference to a *PayPass* terminal includes both the reader and terminal functionality and unless specifically stated does not imply the function should be in a specific part of the terminal system.

### Hard/Soft Limit Implementations

**Soft limit**—refers to implementations where transactions over a given value require cardholder verification.

**Hard limit**—refers to implementations where a maximum transaction amount is set and cardholder verification is never required below this limit.

The configuration of *PayPass - M/Chip* limits results in one of these implementation types within a region or market.

### **Magnetic Stripe Grade Issuers**

Magnetic stripe grade issuers receive additional information produced during a chip transaction, but do not process it. If the magnetic stripe grade issuer uses the Chip Conversion service, the issuer does not receive the additional information.

## **Reference Information**

The following references are used in, or are relevant to, this document. The latest version applies unless a publication date is explicitly stated.

- *Chargeback Guide*
- *M/Chip Card Personalization Standard Profiles (Including PayPass)*
- *M/Chip Requirements*
- *Maestro Global Rules*
- *Maestro PayPass Branding Standards*
- *MasterCard PayPass Branding Standards*
- *MasterCard Rules*
- *PayPass - Mag Stripe Acquirer Implementation Requirements*
- *PayPass On-behalf Services Guide*
- *PayPass Personalization Data Specification*
- *PayPass Vendor Product Approval Process Guide (Cards and Devices)*
- *PayPass Vendor Product Approval Process Guide (Terminals)*
- *PayPass on Mobile Requirements Document*
- *PayPass – M/Chip Issuer Guide*
- *PayPass Mag Stripe Issuer Implementation Requirements*

## **Conventions**

A generic reference to *PayPass* includes all applicable products. The terms MasterCard *PayPass* or Maestro *PayPass* is used to identify specific product requirements.

A reference to the MasterCard product or MasterCard brand includes MasterCard and Debit MasterCard® unless specifically addressed.

MasterCard brands refers to MasterCard and Maestro products.

Values expressed in hexadecimal form ('0' to '9' and 'A' to 'F') are enclosed in single quotes. For example, a hexadecimal value of ABCD is indicated as 'ABCD'.

## Using This Manual

### Conventions

---

Values expressed in binary form are followed by a lower case b. For example, 1001b

EMV Card commands are indicated in bold capitals, for example, **GENERATE AC**.

Specific byte/bit references within a data object are included in square brackets. For example, [1][3] means the third bit of the first byte of the given data object.

---

## Chapter 2 PayPass Introduction

*This chapter provides information on PayPass participation, transaction types, and transaction flows.*

---

Introduction .....	2-1
Participation .....	2-1
PayPass Operating Modes .....	2-2
PayPass Cards .....	2-2
PayPass Transaction Types .....	2-2
PayPass Acceptance .....	2-3
PayPass Transaction Flow .....	2-4
Other Transaction Types and Environments .....	2-7



## Introduction

*PayPass* is the proximity payments program from MasterCard Worldwide.

It allows cardholders to make payments without having to hand over, dip or swipe a payment card. To make a payment, the cardholder simply taps their *PayPass* card onto a *PayPass* terminal. The details are read from the card over a contactless interface using radio frequency communications and a payment transaction is performed over the existing MasterCard payment networks and infrastructure.

Primary characteristics of *PayPass* transactions are speed and convenience for merchants and cardholders.

*PayPass* is supported on the MasterCard and Maestro brands. It is not supported on the Cirrus® brand. The *PayPass* contactless functionality can be used at any merchant location that has *PayPass* terminals and accepts the underlying payment brand. The merchant segments where *PayPass* is expected to be most attractive include those environments with high transaction volumes and where fast transaction times are important.

## Participation

To issue *PayPass* cards or acquire *PayPass* transactions customers must enroll in the *PayPass* program.

Vendors are required to obtain a license agreement before developing and selling *PayPass* cards and devices.

All cards, devices and readers used for performing *PayPass* transactions must have been approved and licensed by MasterCard. Customers must only purchase and deploy cards and terminals from properly licensed vendors. Detailed information about the type approval process can be found in the *PayPass Vendor Product Approval Process Guide (Cards and Devices)* and the *PayPass Vendor Product Approval Process Guide (Terminals)* documents.

Issuers and acquirers must start a project with the relevant MasterCard project team in order to define and complete various certification steps that are required. This can include Network Interface Validation for issuers or Terminal Integration Process for acquirers.

Questions about the enrollment or license process should be directed to [license@PayPass.com](mailto:license@PayPass.com).

## PayPass Operating Modes

*PayPass* supports two modes of operation:

- *PayPass* - Mag Stripe mode
- *PayPass* - *M/Chip* mode

**PayPass - Mag Stripe transactions** are normally completed online. *PayPass* - Mag Stripe is designed for contactless payments using authorization networks that currently support only magnetic stripe authorization for MasterCard cards.

**PayPass - M/Chip transactions** use transaction logic similar to EMV contact chip. They may require online authorization but may be approved offline by the card and terminal. The *PayPass* - *M/Chip* mode is designed for contactless payments in markets that have migrated to chip technology for contact payments.

All MasterCard *PayPass* cards and terminals support *PayPass* - Mag Stripe mode. Cards and terminals may also support *PayPass* - *M/Chip* mode.

Maestro *PayPass* cards and terminals are configured to support *PayPass* - *M/Chip* mode for the Maestro product.

## PayPass Cards

*PayPass* functionality may be:

- Included in a standard ISO 7816 card
- Issued in another form factor, such as a mobile phone or key fob

All *PayPass* cardholder devices are valid for acceptance at *PayPass* terminals; not just cards.

## PayPass Transaction Types

Different transaction types are available for *PayPass*.

*PayPass* issuers and acquirers must support purchase transactions. Refunds must be supported by issuers and acquirers for *PayPass* although they may not be available at every *PayPass* terminal.

*PayPass* manual cash advance transactions are not allowed.

*PayPass* data should only be used for card present transactions. Electronic commerce or Mail Order/Telephone Order transactions should not be performed with Maestro *PayPass* data read through the contactless interface.

Purchase with Cash Back is not supported on Maestro *PayPass*.

The *PayPass* interface may be used for MasterCard Purchase with Cash Back transactions based on the existing product rules. Cardholder verification is always required for Purchase with Cash Back transactions.

MasterCard *PayPass* must not be used for Unique Transactions, as defined in the MasterCard Rules.

Maestro *PayPass* must not be used for Special Transactions, as defined in the Maestro rules.

## PayPass Acceptance

*PayPass* cards may be accepted at attended POS terminals and at CAT terminals. *PayPass* cards may be used at ATMs.

MasterCard defines several types of cardholder activated terminals (CATs).

*PayPass* may be used at CAT Level 1, 2, 3 and 4. Refer to the Chargeback Guide for full definitions.

As CAT Level 1 terminals require PIN based cardholder verification, only *PayPass* cards that support online PIN or On Device Cardholder Verification may be used at these terminals.

### Card Checking

*PayPass* transactions are carried out by the cardholder; therefore, the card does not need to be given to the merchant. Since the *PayPass* card may remain in the hands of the cardholder, the merchant is exempt from the visual inspection requirement to determine if the *PayPass* card is valid. The card only needs to be given to the merchant after the contactless interaction is complete if signature verification is to be performed.

### Transaction Amount

The transaction amount is usually known before the *PayPass* transaction is initiated to ensure fast processing of *PayPass* transactions. The amount should be displayed to the cardholder.

If the transaction amount exceeds the maximum amount for *PayPass* transactions, for the product or terminal, the terminal or merchant should prompt the cardholder to use a different technology to complete the transaction (for example a contact chip transaction). This ensures cardholders are not denied service when they have a valid MasterCard product for the transaction.

### Limits

For MasterCard *PayPass*, a Chargeback Protection Amount is published in the *Chargeback Guide*. Transactions equal to or less than this limit do not need cardholder verification. A receipt does not need to be routinely issued for these transactions.

In some specific markets, a maximum transaction amount may be published for MasterCard *PayPass*.

For Maestro *PayPass*, a Ceiling Limit is published in the *Maestro Global Rules*. Transactions are not allowed above this limit, except in certain markets specified by MasterCard where transactions are permitted with online PIN verification. In these situations, the published ceiling limit effectively becomes the chargeback protection amount.

- Markets in which Maestro *PayPass* transactions are not allowed above the ceiling limit are referred to as **hard limit** markets.
- Markets in which Maestro *PayPass* transactions are allowed above the ceiling limit with online PIN verification are referred to as **soft limit** markets.

The term chargeback protection amount is used generically in later sections to refer to both the MasterCard chargeback protection amount and the Maestro limit above which cardholder verification is required.

Floor limits for *PayPass* are as for contact chip (for *PayPass - M/Chip*) or magnetic stripe (for *PayPass - Mag Stripe*) transactions. The floor limit may vary per market.

#### **Fallback**

If the contactless technology fails the transaction may be completed by any other technology available. A subsequent transaction is not considered a technical fallback transaction.

## PayPass Transaction Flow

Several steps are involved in the *PayPass* transaction.

#### **Technology Selection**

The cardholder decides whether to use *PayPass* or an alternative interface on the card. *PayPass* technology is used for the transaction when the *PayPass* card is presented by the cardholder to the *PayPass* reader.

If the card application selected and the terminal supports *PayPass - M/Chip* mode, then it is automatically used by the terminal to complete the transaction. Otherwise, *PayPass - Mag Stripe* mode is used.

#### **Application Selection**

If the cardholder has chosen to pay by *PayPass*, the terminal attempts to find an application via the contactless interface to complete the transaction.

When the terminal detects more than one application that it supports on the *PayPass* card, the terminal automatically selects the application with the highest priority set by the issuer. Interactive cardholder selection or confirmation is not supported for *PayPass* to improve the transaction speed.

If there are no available applications, given any relevant transaction limits, then the *PayPass* transaction cannot proceed.

For MasterCard products, the same Application Identifiers (AID) are used for *PayPass* transactions as for contact chip transactions. There are no *PayPass* specific AIDs.

### **Card Authentication**

For all *PayPass* transactions the card being used is authenticated. For *PayPass - M/Chip* transactions the card can be authenticated:

- Offline by the terminal

OR

- Online by the issuer

All offline approved Maestro *PayPass* transactions must be authenticated using CDA.

All offline MasterCard *PayPass - M/Chip* transactions must be authenticated by the terminal using either:

- CDA

OR

- SDA<sup>1</sup>

CDA is strongly recommended for MasterCard *PayPass - M/Chip* transactions and the use of SDA is being phased out. All *PayPass - M/Chip* terminals support CDA. *PayPass* does not support DDA.

**For online *PayPass - M/Chip* transactions** the issuer should perform online authentication by verifying the ARQC received in the online authorization.

**For *PayPass - Mag Stripe* transactions**, the transactions are authorized online by the issuer. The *PayPass* card produces a unique password, referred to as Dynamic CVC3, for each transaction. The value is placed by the terminal in issuer defined positions within the existing track data fields; therefore, no extra data needs to be transmitted. The issuer should perform online authentication by verifying the Dynamic CVC3 received in the online authorization.

If *PayPass - Mag Stripe* profile transactions are not authorized by the issuer, then the merchant may be liable for any disputed transactions.

Offline-only terminals may decline transactions with *PayPass - Mag Stripe* cards.

---

1. SDA authenticates the card, but not the transaction data. New *PayPass* cards cannot be issued supporting SDA. New *PayPass* terminals do not support SDA.

#### Cardholder Verification

*PayPass* transactions for amounts less than or equal to the chargeback protection amount do not require cardholder verification.

For transaction amounts above the chargeback protection amount, cardholder verification is required or the acquirer may be liable for disputed transactions.

**For MasterCard *PayPass***, acceptable cardholder verification methods are:

- Online PIN
- Signature
- On Device Cardholder Verification

**For Maestro *PayPass***, acceptable cardholder verification methods are:

- Online PIN
- On Device Cardholder Verification

*PayPass* does not support offline PIN.

**For *PayPass* - Mag Stripe transactions**, the CVM is determined by the terminal. This can be done in a similar way to swiped magnetic stripe transactions, based on the methods supported by the terminal. The terminal is not required to follow issuer instructions contained in the Service Code encoded in the magnetic stripe data. The device notifies the terminal if On Device Cardholder Verification is supported, in which case this method is used if supported by the terminal and cardholder verification is required.

**For *PayPass* - M/Chip transactions**, the CVM is determined by the *PayPass* reader application in the terminal, based on the CVM List or other information contained in the card. The actual CVM is completed after the interaction with the card is complete, except for On Device Cardholder Verification which is completed before the interaction begins.

#### Card Risk Management

The card risk management performed is at the discretion of the issuer.

#### Online Authorization

***PayPass* - M/Chip transactions** may be authorized offline by the *PayPass* card or the card may request online authorization by the issuer.

***PayPass* - Mag Stripe transactions** are usually authorized online by the issuer. If *PayPass* - Mag Stripe transactions are not authorized online, then the acquirer may be liable for any disputed transactions.

If online PIN has been identified as the cardholder verification method for the transaction, the PIN is verified as part of the online authorization request.

### **End of Transaction**

A *PayPass - M/Chip* terminal ends the interaction with the card once the results of the first **GENERATE AC** command are received by the terminal. A *PayPass - Mag Stripe* terminal ends the interaction with the card once the results of the **COMPUTE CRYPTOGRAPHIC CHECKSUM** command are received by the terminal. This is not the end of the *PayPass* transaction.

The *PayPass* terminal completes the transaction based on:

- An offline approval or decline response from the card for *PayPass - M/Chip* transactions.

OR

- An online authorization response (approve or decline) when requested

When the printing of a receipt is supported by the point of sale, for *PayPass* transactions less than or equal to the chargeback protection amount, a receipt must be available if requested by the cardholder. A receipt must be provided for transactions above the chargeback protection amount if the terminal is capable of producing a receipt.

Neither issuer authentication nor script processing is completed during a *PayPass - M/Chip* transaction.

## **Other Transaction Types and Environments**

There are additional transaction types and environments in which *PayPass* cards may or may not be used.

### **Purchase with Cash Back**

Purchase with Cash Back is not supported on Maestro *PayPass*.

The *PayPass* interface may be used for MasterCard Purchase with Cash Back transactions as per the existing product rules. Cardholder verification is always required for Purchase with Cash Back transactions.

### **Unique and Special Transactions**

MasterCard *PayPass* must not be used for Unique Transactions, as defined in the *MasterCard Rules*.

Maestro *PayPass* must not be used for Special Transactions, as defined in the Maestro rules.

### **Cardholder Activated Terminals**

MasterCard defines several types of cardholder activated terminals (CATs). *PayPass* may be used at CAT Level 1, 2, 3 and 4 terminals (see the *Chargeback Guide* for full definitions).

## PayPass Introduction

### Other Transaction Types and Environments

---

As CAT Level 1 terminals require PIN based cardholder verification, only *PayPass* cards that support online PIN or On Device Cardholder Verification may be used at these terminals.

---

## Chapter 3 Issuer Requirements

*This chapter includes information on requirements for the issuer.*

---

General Requirements .....	3-1
Card Requirements .....	3-1
Card Delivery .....	3-13
Issuer Host Requirements .....	3-13
Clearing Requirements .....	3-15
Chargeback and Exception Processing .....	3-16



## General Requirements

### PayPass Enrollment

For issuers wishing to participate in the *PayPass* program, completion of the *PayPass* Program Enrollment Form is mandatory. Once enrolled, issuers receive access to the relevant technical documents.

---

<b>R</b>	<b>ALL</b>	All customers who wish to issue <i>PayPass</i> must enroll in the <i>PayPass</i> program.
----------	------------	---

---

## Card Requirements

Various requirements and best practices exist for the *PayPass* card.

### Approvals and Testing

All *PayPass* cards issued are required by MasterCard to have MasterCard vendor product approval. It is the issuer's responsibility to confirm all products have received this approval. A full *PayPass* card Letter of Approval is only granted to a card when it has successfully completed all of the following:

- Interface and Application Testing
- Compliance Assessment and Security Testing
- Card Quality Management

When ordering cards from a card manufacturer, the issuer must ensure that the card manufacturer has a current *PayPass* Letter of Approval for the product being purchased. The Letter of Approval is valid for the duration of the time the cards are held in stock prior to being issued.

All *PayPass* products must have a valid *PayPass* Letter of Approval at the time the product is issued.

---

<b>R</b>	<b>ALL</b>	Issuers must ensure that all <i>PayPass</i> cards are covered by a valid Letter of Approval at the time they are issued.
----------	------------	--

---

### Branding, Appearance and Physical Requirements

For the brand standards and design elements required for *PayPass* cards, please refer to the *MasterCard PayPass Branding Standards* and the *Maestro PayPass Branding Standards*. Issuers must obtain approval from MasterCard Card Design Management for their *PayPass* card design, even if a similar design has already been approved for use on a non-*PayPass* card.

*PayPass* cards look similar to standard cards, with the exception of the *PayPass* logo. MasterCard recommends the logo be placed on the front of the card.

---

<b>R</b>	<b>ALL</b>	Cards must comply with the <i>PayPass</i> branding requirements.
----------	------------	--

---

#### PayPass Cards

If *PayPass - M/Chip* is implemented on an ISO 7816 compliant plastic card then the card must support both magnetic stripe and an EMV contact chip.

---

<b>R</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> Cards must be hybrid cards supporting both magnetic stripe and contact chip.
----------	------------	--

---

A MasterCard *PayPass* card that supports chip on the contact interface normally also supports *PayPass - M/Chip*.

---

<b>BP</b>	<b>MC</b>	A chip capable MasterCard branded <i>PayPass</i> card should support <i>PayPass - M/Chip</i> .
-----------	-----------	--

---

#### Non-card Devices

*PayPass* functionality can be present in form factors other than traditional payment cards. Examples of different forms are:

- Mobile phones
- Key fobs
- Watches

All *PayPass* non-card devices conduct *PayPass* transactions in the same way as *PayPass* cards. They may support special functionality, such as On Device Cardholder Verification.

When *PayPass - M/Chip* cards use offline risk management features, an interaction with the card is required to manage the offline risk management counters. This cannot be performed in a normal *PayPass* payment transaction since response data from the issuer is not returned to the card. This interaction may be achieved:

- By performing a transaction through the contact interface of a hybrid card
- By over-the-air messages, for example to a mobile phone
- Through the contactless interface in a special terminal designed for this purpose, if supported by the cardholder device.

*PayPass* cards which support offline transactions, including all Maestro cards, must be able to support the management of the offline risk management counters. *PayPass - M/Chip* non-card devices that cannot support the management of the offline risk management counters must be configured as online only.

All *PayPass* non-card device programs must be approved by MasterCard.

The MasterCard *PayPass* device given to the cardholder must be linked to a MasterCard card account assigned to that same cardholder accessed by a standard MasterCard card. This card does not have to be a *PayPass* card. The expiration date of the *PayPass* device must not be later than the card that it is linked to. If the MasterCard card is cancelled, the issuer must simultaneously cancel the companion *PayPass* device. It is not necessary for the *PayPass* device to display an account number.

Devices other than mobile phones should accommodate a signature panel where possible. Those devices that cannot accommodate a signature panel should contain a customization area or unique identification number. A minimal space on small form factors is sufficient to provide cardholders with an opportunity to customize the device with their initials or another mark to identify it as belonging to them.

<b>R</b>	<b>ALL</b>	All <i>PayPass</i> non-card device programs must be approved in advance by MasterCard.
<b>R</b>	<b>MC</b>	A MasterCard branded <i>PayPass</i> device must be linked to an account with a standard MasterCard card. This card does not need to support <i>PayPass</i> .
<b>R</b>	<b>MC</b>	The expiration date of the <i>PayPass</i> device must not be later than the card to which it is linked.
<b>R</b>	<b>MC</b>	The <i>PayPass</i> device must be cancelled if the linked MasterCard card is cancelled.
<b>BP</b>	<b>MC</b>	The <i>PayPass</i> device, other than a mobile phone, should accommodate a signature panel.
<b>R</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> non-card devices that do not provide a mechanism to reset offline risk management counters must be configured as online only.
<b>R</b>	<b>MS</b>	Maestro <i>PayPass</i> must only be supported on a dual interface card or other device that supports over-the-air communication to manage the offline risk management counters.

### Card Application

*PayPass - M/Chip* must be implemented using approved applications. Examples are:

- *PayPass - M/Chip 4*
- *M/Chip Advance*
- *PayPass - M/Chip Flex*
- Mobile MasterCard *PayPass - M/Chip 4*

---

**R ALL** All *PayPass - M/Chip* cards must use approved applications.

---

### Support of *PayPass - M/Chip* and *PayPass - Mag Stripe*

A *PayPass* card using the MasterCard brand:

- Must support *PayPass - Mag Stripe* transactions
- May support *PayPass - M/Chip* transactions

---

**R MC** A MasterCard *PayPass* card must support *PayPass - Mag Stripe* transactions.

---

A *PayPass* card using the Maestro brand:

- Must support *PayPass - M/Chip* transactions
- Must not support *PayPass - Mag Stripe* transactions for Maestro

---

**R MS** A Maestro *PayPass* card must support *PayPass - M/Chip* transactions.

---

**R MS** A Maestro *PayPass* card must not support *PayPass - Mag Stripe* transactions.

---

*PayPass* technology may not currently be used on MasterCard Fleet or MultiCard products as data positions required by *PayPass* are already used in the product personalization requirements of these products.

---

**R MC** MasterCard Fleet or MultiCard products including *PayPass* must not be issued.

---

### Online and Offline Capability

*PayPass - Mag Stripe* transactions are normally authorized online. The card has no input into the decision to seek authorization.

In *PayPass - M/Chip* cards the transaction counters and decision making capability of the chip are used to control risk. To support fast transactions, it is recommended that *PayPass - M/Chip* cards be configured to support offline transaction approval. Maestro *PayPass* cards must not be configured as online only.

As some terminals operate exclusively online, *PayPass - M/Chip* cards should be configured to support online transaction approval.

To meet special market requirements MasterCard may approve cards that are exclusively online or exclusively offline; however, issuers should be aware that these cards do not work in some terminals.

---

**R MS** Maestro *PayPass* cards must not be configured as online only.

---

**BP ALL** *PayPass - M/Chip* cards should be configured to support offline transaction approval. They should not be configured to be exclusively online.

---

**BP ALL** *PayPass - M/Chip* cards should be configured to support online transaction approval. They should not be configured to be exclusively offline.

---

### Service Codes

A value for the service code may be found several times on a *PayPass - M/Chip* card. For example:

- on the magnetic stripe of the card in both Track 1 and Track 2
- Track 1 Data (tag '56') and Track 2 Data (tag '9F6B') accessed via the *PayPass* interface
- Track 2 Equivalent Data (tag '57') accessed via the *PayPass* interface
- Track 2 Equivalent Data (tag '57') accessed via the contact interface

Although not recommended, *PayPass* issuers may choose to use service code values in the *PayPass* application differently than the magnetic stripe of the same card. It is recommended that cards be personalized to use the same service code appropriate for the product each time the service code is used.

If the issuer does use a different service code value on the *PayPass* interface, the value may be acted on by some terminals. In particular, terminals that process the service code may reject international cards that have a service code value starting with '5' (National use only).

---

**BP ALL** Issuers should use the value of the service code appropriate for the product each time the service code is used.

---

### **Purchase with Cash Back**

Maestro cards must not support Purchase with Cash Back on the *PayPass* interface.

Debit MasterCard cards may support Purchase with Cash Back on the *PayPass* interface.

Purchase with Cash Back on the *PayPass* interface is only supported for MasterCard credit cards in European markets.

Purchase with Cash Back transactions always require cardholder verification, regardless of the amount.

---

<b>R</b>	<b>MS</b>	Maestro cards must not be configured to support Purchase with Cash Back through the <i>PayPass</i> interface.
<b>R</b>	<b>MC</b>	MasterCard credit cards issued outside the Europe region must not be configured to support Purchase with Cash Back through the <i>PayPass</i> interface.

---

### **Application Selection**

*PayPass* terminals normally perform application selection using the PPSE on the card. All *PayPass* cards must contain a PPSE.

Issuers must use the Application Priority Indicator to show the preferred sequence of choice of all *PayPass* applications on the card. Issuers must set a priority for each application. Cardholder confirmation must not be requested.

The AID value used for *PayPass* is the same AID used for the contact interface. There are no specific AIDs for *PayPass*.

Supported AIDs are:

- MasterCard 'A0000000041010'
- Maestro 'A0000000043060'

Identification of *PayPass* cards use the product AID without any extension, as shown above. PIX extensions may be used by issuers and are considered as a successful match by the terminal when partial AID matching is supported. However, it is recommended not to use PIX extensions, as some legacy *PayPass* terminals do not support partial AID matching.

If the same account is accessed by the contact and contactless interface, the AID used on each interface might be different; the contact AID may contain a PIX extension, but the contactless AID excludes this PIX extension.

The Application Label (tag '50') must be present in a *PayPass* card. This may appear on any receipts.

The Application Label on a MasterCard card must be **MasterCard, MASTERCARD, Debit MasterCard or DEBIT MASTERCARD**.

The Application Label on a Maestro card must be **Maestro or MAESTRO**.

Issuers may personalize the Application Preferred Name (tag '9F12') and Issuer Code Table Index (tag '9F11'). The Application Preferred Name may be used on receipts instead of the Application Label if the terminal supports the code table indicated.

<b>R</b>	<b>ALL</b>	All <i>PayPass</i> cards must contain a PPSE.
<b>R</b>	<b>ALL</b>	Issuers must set a unique value for the Application Priority Indicator in each <i>PayPass</i> application on the card.
<b>R</b>	<b>ALL</b>	Issuers must not set the Cardholder Confirmation bit in the Application Priority Indicator.
<b>R</b>	<b>ALL</b>	Issuers must use the appropriate Application Label.
<b>BP</b>	<b>ALL</b>	PIX extensions should not be used in the AID for <i>PayPass</i> .

### Card Authentication

MasterCard requires the use of Dynamic CVC3 by all *PayPass - Mag Stripe* cards. This includes *PayPass - M/Chip* cards that perform *PayPass - Mag Stripe* transactions.

For *PayPass - M/Chip* online transactions the ARQC should be validated to prevent counterfeit fraud.

For MasterCard *PayPass - M/Chip*:

- Cards issued in the Europe region must support CDA and must not support SDA
- Cards issued outside of the Europe region that do not support CDA must operate as online only. Cards must not support SDA

MasterCard recommends that the issuer support CDA.

All Maestro *PayPass* cards must support CDA and must not support SDA for Maestro *PayPass - M/Chip*.

*PayPass* does not support DDA as this requires the *PayPass* card to be in communication with the terminal for a longer period than other offline CAM options.

<b>R</b>	<b>MS</b>	Maestro <i>PayPass - M/Chip</i> cards must support CDA and must not support SDA.
<b>R</b>	<b>MC</b>	New MasterCard <i>PayPass - M/Chip</i> cards must not support SDA.

## Issuer Requirements

### Card Requirements

---

<b>R</b>	<b>MC</b>	New MasterCard <i>PayPass - M/Chip</i> cards issued in the Europe region must support CDA.
<b>R</b>	<b>MC</b>	New MasterCard <i>PayPass - M/Chip</i> cards issued outside of the Europe region must support CDA or be configured as online only and not support any offline CAM.
<b>BP</b>	<b>MC</b>	Issuers outside the Europe region are strongly recommended to use CDA on MasterCard <i>PayPass - M/Chip</i> cards.
<b>R</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> cards must not support DDA on the <i>PayPass</i> interface.
<b>R</b>	<b>MC</b>	MasterCard <i>PayPass - M/Chip</i> cards must use a Dynamic CVC3 for <i>PayPass - Mag Stripe</i> transactions.
<b>BP</b>	<b>ALL</b>	Issuers are strongly recommended to validate the ARQC for online <i>PayPass - M/Chip</i> transactions.

The payment system public keys for *PayPass - M/Chip* have the same values and expiry dates, as those used for MasterCard contact transactions. It is recommended to use the same Issuer Key pair for transactions on the contact and contactless interface of a *PayPass - M/Chip* card; therefore, the same Issuer Public Key certificate may be used.

It is recommended to use the same ICC Key pair for transactions on the contact and contactless interface of a *PayPass - M/Chip* card. The ICC Public Key Certificate cannot be shared between the contact and contactless interface even if the same keys are used since some of the data elements signed in the certificate are different.

---

<b>BP</b>	<b>ALL</b>	Issuers should use the same Issuer and ICC Public Keys across both the contact and contactless interface.
-----------	------------	---

---

### Cardholder Verification

A signature or PIN is not required for a *PayPass* transaction less than or equal to the chargeback protection amount. In this situation, no setting of the Service Code for *PayPass - Mag Stripe*, or CVM List for *PayPass - M/Chip*, requires the acquirer to obtain cardholder verification.

For transactions greater than the chargeback protection amount, cardholder verification is normally requested. If transactions are completed with no cardholder verification above the chargeback protection amount then the acquirer may be liable for disputed transactions.

**For *PayPass - Mag Stripe* transactions**, the cardholder verification method is determined by the terminal in a similar manner to swiped magnetic stripe transactions. The terminal is not required to refer to the Service Code, which appears in multiple data elements. If the device supports On Device Cardholder Verification, this is communicated to the terminal as part of the transaction.

**For PayPass - M/Chip transactions**, the CVM is determined by the *PayPass* reader application in the terminal based on the terminal capabilities and CVM List or other data in the card.

MasterCard *PayPass - M/Chip* cards:

- Must support signature
- Must support online PIN
- Must support No CVM
- May support On Device Cardholder Verification

The issuer may elect for either signature or online PIN to be preferred and personalize the CVM List accordingly. On Device Cardholder Verification is performed above the chargeback protection amount if supported by the device and the terminal.

Maestro *PayPass* cards:

- Must support No CVM
- Must not support signature, online PIN, or On Device Cardholder Verification

If issued in a **soft limit** market, Maestro *PayPass - M/Chip* cards:

- Must support No CVM and online PIN
- Must not support signature
- May support On Device Cardholder Verification

Offline PIN is not supported for *PayPass - M/Chip* transactions. Offline PIN may be supported on the same card but only for contact EMV transactions. Issuers must not include offline PIN options in the CVM List read through the *PayPass* interface.

<b>R</b>	<b>MS</b>	Maestro <i>PayPass - M/Chip</i> cards must support No CVM for <i>PayPass</i> transactions.
<b>R</b>	<b>MS</b>	Maestro <i>PayPass</i> cards issued in <b>soft limit</b> markets must support online PIN for <i>PayPass</i> transactions.
<b>R</b>	<b>MC</b>	MasterCard <i>PayPass - M/Chip</i> cards must support No CVM, online PIN and signature.
<b>R</b>	<b>All</b>	<i>PayPass - M/Chip</i> cards must not support either offline plain text PIN or offline enciphered PIN in the CVM List read through the <i>PayPass</i> interface.

### Magnetic Stripe Based PVV

It may not be possible or easy to change some of the data on a *PayPass* card. Any existing magnetic stripe processes that rely on rewriting data to the magnetic stripe after the card has been issued needs to be evaluated. In particular this may affect magnetic stripe based PVV solutions for online PIN verification if PIN change is supported.

---

<b>BP ALL</b>	Magnetic stripe based PVV methods should not be used for online PIN verification if PIN change is supported.
---------------	--

---

### Managing the Contactless Controls

The issuer should manage the offline counters and parameters for the contactless interface during the authorization response to a contact chip transaction. They cannot be managed during a *PayPass* transaction as the Issuer Authentication Data from the authorization response is never delivered to the card.

The *PayPass - M/Chip* application may trigger an online authorization request at the next contact transaction to enable management of the offline counters.

### Personalization Requirements

The *PayPass* personalization requirements are detailed in the *PayPass Personalization Data Specifications* and the *M/Chip Card Personalization Standard Profiles (including PayPass)*.

MasterCard requires that the personalization of each card configuration be approved using the CPV service before cards are issued.

MasterCard prohibits encoding the cardholder name in the data read through the contactless interface to prevent unauthorized disclosure. It is recommended to use a space character followed by the surname separator “/” in the Track 1 Data.

Third Party Data may be used by a terminal for proprietary processing. Issuers that intend to participate in a scheme utilizing this data object must request a Unique Identifier from MasterCard.

---

<b>R ALL</b>	CPV must be successfully completed for all <i>PayPass</i> cards issued.
<b>R ALL</b>	The name of the cardholder must not be readable over the <i>PayPass</i> interface.
<b>R ALL</b>	If Third Party Data is included in the <i>PayPass</i> card, and is intended to be used to carry proprietary data, then the issuer must contact MasterCard at <a href="mailto:specifications@paypass.com">specifications@paypass.com</a> to obtain the Unique Identifier.
<b>BP ALL</b>	Issuers should use " /" for the cardholder name in the data read through the <i>PayPass</i> interface.
<b>BP ALL</b>	The <i>PayPass</i> card should be personalized with Third Party Data containing the Device Type.

---

Data objects may be personalized in the card organized in the pre-defined file structure detailed in the *PayPass Personalization Data Specifications* to allow efficient data capture by the *PayPass* terminal resulting in a faster transaction.

---

**R ALL** If data objects are not organized according to the rules specified for the pre-defined file structure, then the pre-defined values for the AFL must not be used.

---

### PayPass — M/Chip Personalization Requirements

Some data elements are unique for the contactless interface and some are shared with the contact interface.

For *PayPass* the issuer may operate in full chip grade, semi-grade or magnetic stripe grade on the contact profile.

Chip grade issuers, semi-grade issuers and magnetic stripe grade issuers that have the capability to distinguish between chip-read and magnetic stripe-read transactions must use a different value for Chip CVC on the contactless interface to the CVC1 encoded on the magnetic stripe. This prevents compromised *PayPass* data being used to fraudulently create valid counterfeit magnetic stripe cards.

Maestro cards that do not have a CVC1 encoded on the magnetic stripe do not need to include a Chip CVC.

However to protect against the risk of counterfeiting, it should not be possible to reproduce the Track 2 on the magnetic stripe from the *PayPass* data in the chip. This means that some aspect of the magnetic stripe data should be unique to the stripe, unpredictable and validated during the authorization.

---

**R ALL** Chip grade issuers, semi-grade issuers and magnetic stripe grade issuers that have the capability to distinguish between chip-read and magnetic stripe-read transactions must support a Chip CVC in Track 2 Equivalent Data on the contactless interface that is different to the CVC1 if present.

---

**R ALL** The genuine CVC1, as found on the physical magnetic stripe, must not appear in any data element that can be read through the contactless interface (except as allowed above).

---

**BP MS** Issuers of Maestro *PayPass* cards that do not have a Chip CVC in Track 2 Equivalent Data should ensure that the Track 2 data found on the magnetic stripe cannot be reproduced from the *PayPass* data on the chip. Some aspect of the magnetic stripe data should be unique to the magnetic stripe, unpredictable and validated during the authorization.

---

Issuers may choose to use an Application PAN on the contactless interface which is different to the PAN present on the magnetic stripe or that appears on the face of the card.

To protect critical data used in the transaction, if the card supports offline card authentication then the data elements shown in the table below must be stored in records that are signed.

## Issuer Requirements

### Card Requirements

---

Data Element	Tag
Application Currency Code <sup>1</sup>	'9F42'
Application Expiration Date	'5F24'
Application Effective Date <sup>2</sup>	'5F25'
Application PAN Sequence Number	'5F34'
Application Primary Account Number	'5A'
Application Usage Control	'9F07'
CDOL1	'8C'
CDOL2	'8D'
CVM List	'8E'
Issuer Action Code - Default	'9F0D'
Issuer Action Code - Denial	'9F0E'
Issuer Action Code - Online	'9F0F'
Issuer Country Code	'5F28'
SDA Tag List	'9F4A'

---

**R ALL** The data elements shown in the table above, if present, must all be stored in records that are signed.

---

### ***PayPass* - Mag Stripe Personalization Requirements**

The first and only record of the file in SFI 1 must include the data objects necessary to perform the *PayPass* -Mag Stripe transactions.

The last digit of both Track 1 and Track 2 must not be used by the issuer as this is used by the terminal to indicate the number of digits of the unpredictable number (nUN).

The positions where the *PayPass* reader stores the ATC, UN, and CVC3 in the discretionary data in Track 1 Data and Track 2 Data, should be filled with zeroes. This is a requirement if *PayPass* On Behalf CVC validation services are used.

- 
1. If present and the CVM List contains condition code value of '06', '07', '08', or '09'
  2. If present

---

<b>R</b>	<b>MC</b>	Record 1 of SFI 1 must contain the data to perform a <i>PayPass</i> - Mag Stripe transaction. Record 1 must be the only record included in SFI 1.
<b>R</b>	<b>MC</b>	The last digit of both Track 1 and Track 2 must not be used by the issuer.
<b>R</b>	<b>MC</b>	Placeholders for dynamic data which is inserted by the terminal in either Track 1 or Track 2 must be zero filled if <i>PayPass</i> -on behalf CVC validation services are used.

---

## Card Delivery

*PayPass* data can be read by any reader that can power the contactless chip and send the correct commands.

Therefore, it is feasible that card data could be captured while the card is in transit to the cardholder. Issuers should consider appropriate control methods to reduce the risks and impact of card or data interception. This might be by using a special envelope to shield card reading or by disabling the contactless interface until the card has been activated by the cardholder.

---

<b>BP</b>	<b>ALL</b>	Issuers should disable the contactless interface until the card has been activated by the cardholder.
-----------	------------	---

---

## Issuer Host Requirements

Issuer host must meet requirements to accommodate authorization messages and decisions.

### Authorization Messages

*PayPass* issuers must ensure host systems are capable of correctly receiving and processing authorization messages containing specific values for the data element (DE) 22 (POS Entry Mode) and DE 61 (POS Data) that identify *PayPass* transactions.

- DE 22 (POS Entry Mode), subelement 1, value **07** is used for a *PayPass* - *M/Chip* transaction. A value of **91** is used for a *PayPass* - Mag Stripe transaction even if performed at a *PayPass* - *M/Chip* terminal.
- DE 61 (POS Data), subelement 11, value **3** is used for any *PayPass* transaction at a *PayPass* - *M/Chip* terminal, the terminal may also be *PayPass* - Mag Stripe capable, and a value of **4** is used for any *PayPass* transaction at a *PayPass* - Mag Stripe only terminal.

---

<b>R</b>	<b>ALL</b>	Issuers must support on their network interface and host system <i>PayPass</i> transactions as described above.
----------	------------	---

---

### Authorization Decisions

Authorization requests are approved against the account balance or open to buy position in the usual way. In addition, issuers should check the authenticity of the *PayPass* card by validating the Dynamic CVC3 or ARQC received.

The issuer should take into account that the TVR included in the authorization request of a *PayPass - M/Chip* transaction does not always reflect the real outcome of the terminal tests performed. An example of this is when card authentication may have been completed after the **GENERATE AC** command was issued to the card or after the TVR was signed.

<b>BP</b>	<b>ALL</b>	Issuers should always perform online CAM by checking that the ARQC contained in a <i>PayPass - M/Chip</i> online authorization request is correct.
<b>R</b>	<b>ALL</b>	An authorization or clearing request may legitimately contain a TC in DE 55. Issuers must not routinely decline transactions in this situation.
<b>R</b>	<b>ALL</b>	The transaction amount and the transaction date may be different in DE 55 when compared other fields in the authorization message. The issuer must not routinely decline transactions in this situation.
<b>R</b>	<b>MC</b>	Issuers must always perform online CAM by checking that the CVC3 contained in a <i>PayPass - Mag Stripe</i> online authorization request is correct.
<b>BP</b>	<b>MC</b>	Issuers should monitor the ATC to help detect fraud.
<b>BP</b>	<b>MC</b>	Issuers must be able to process <i>PayPass - Mag Stripe</i> transactions if either Track 1 Data or Track 2 Data is present in the authorization message.

### Authorization Responses

A referral response must not be given to a *PayPass* authorization request.

Since the consumer remains in control of the *PayPass* card throughout the transaction, the opportunity for merchants to pick up these cards is limited. Issuers should not use a capture card authorization response to *PayPass* transactions.

**For *PayPass - M/Chip* authorization responses**, the issuer should not generate Issuer Authentication Data, because the *PayPass* terminal is not able to pass it to the *PayPass* card.

**For *PayPass - M/Chip* authorization responses**, the issuer should not include issuer scripts because the *PayPass* terminal is not able to pass them to the *PayPass* card.

<b>R</b>	<b>ALL</b>	Issuers must not use a referral <b>01</b> authorization response code.
<b>BP</b>	<b>ALL</b>	Issuers should not use a capture card <b>04</b> authorization response code.

---

<b>BP</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> issuers should not generate Issuer Authentication Data for authorization responses.
<b>BP</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> issuers should not send scripts with authorization responses.
<b>R</b>	<b>ALL</b>	Issuers that use a PAN mapping service must return the genuine PAN in the authorization response message, even if an alternative PAN was used in the authorization request.

---

### Refunds

MasterCard *PayPass* issuers must be able to support the processing of a refund transaction initiated via the *PayPass* contactless interface.

---

<b>R</b>	<b>MC</b>	Issuers must be able to process refunds initiated via the contactless interface.
----------	-----------	--

---

## Clearing Requirements

*PayPass* transactions are identified in clearing messages.

### Clearing Messages

*PayPass* issuers must ensure host systems are capable of correctly receiving and processing existing subfields within the clearing message containing specific values of the data input capability and the data input profile, DE 22 (POS Entry Code).

DE 22, subfield 1 identifies the terminal capabilities and must contain:

- the value of **M** for a transaction at a *PayPass - M/Chip* terminal. The terminal may also be *PayPass - Mag Stripe* capable.
- the value of **A** for a transaction at a *PayPass - Mag Stripe* terminal.

DE 22, subfield 7 identifies the card data input profile for this transaction and must contain:

- the value **M** for a *PayPass - M/Chip* transaction.
- the value **A** for a *PayPass - Mag Stripe* transaction.

---

<b>R</b>	<b>ALL</b>	Issuers must support <i>PayPass</i> transactions as described above on their clearing interface and host system.
----------	------------	--

---

## Chargeback and Exception Processing

Issuers may not make a retrieval request for a transaction identified as a *PayPass* transaction that is less than the chargeback protection amount, except in certain transit situations.

No new chargeback reason codes have been introduced to support *PayPass*. Updates to the existing reason codes are documented in the *Chargeback Guide* or in the *Maestro Global Product Rules*.

---

## Chapter 4 Acquirer Requirements

*This chapter includes information on requirements for the acquirer.*

---

General Requirements .....	4-1
Terminals .....	4-2
Offline Card Authentication .....	4-10
Cardholder Verification .....	4-11
Terminal Risk Management.....	4-14
Terminal Action Codes (TACs).....	4-14
Authorization Responses.....	4-14
Receipts .....	4-15
Subsequent Contact Transactions.....	4-15
Terminated Transactions .....	4-16
Cardholder Activated Terminals.....	4-16
Automated Teller Machines .....	4-17
Acquirer Network Requirements.....	4-18
Authorization Requirements.....	4-19
Clearing Requirements.....	4-19
Exception Processing.....	4-20
On-behalf Services .....	4-21



## General Requirements

Overall general requirements for acquirers and merchants include *PayPass* enrollment and acceptance.

### PayPass Enrollment

Acquirers implementing *PayPass* acceptance must enroll in the MasterCard *PayPass* program. Acquirers must be enrolled and receive approval from MasterCard to acquire *PayPass* transactions.

Program enrollment allows acquirers access to all required specifications and to receive MasterCard related services and products.

---

<b>R</b>	<b>ALL</b>	Members that want to acquire <i>PayPass</i> transactions must enroll in the <i>PayPass</i> program.
----------	------------	---

---

### PayPass Acceptance

*PayPass* acceptance means that all cardholder devices are valid for acceptance at terminals, not just *PayPass* cards.

A *PayPass* terminal that accepts MasterCard:

- Must accept *PayPass* - Mag Stripe transactions
- May support *PayPass* - *M/Chip* transactions

A *PayPass* terminal that accepts Maestro:

- Must not accept Maestro in *PayPass* - Mag Stripe mode. The terminal may support *PayPass* - Mag Stripe for MasterCard.
- Must support *PayPass* - *M/Chip* transactions

*PayPass* - *M/Chip* must be used if supported by the card and terminal. Attempted *PayPass* - *M/Chip* transactions must not fallback to *PayPass* - Mag Stripe. Terminals cannot change processing mode during a transaction once it is determined.

---

<b>R</b>	<b>MC</b>	A MasterCard <i>PayPass</i> terminal must support <i>PayPass</i> - Mag Stripe.
----------	-----------	--

---

<b>R</b>	<b>MS</b>	A Maestro <i>PayPass</i> terminal must support <i>PayPass</i> - <i>M/Chip</i> .
----------	-----------	---

---

<b>R</b>	<b>MS</b>	A Maestro <i>PayPass</i> terminal must not support <i>PayPass</i> - Mag Stripe.
----------	-----------	---

---

*PayPass* - Mag Stripe merchant locations normally also support magnetic stripe contact acceptance.

*PayPass* - *M/Chip* enabled merchant locations normally also support contact EMV and magnetic stripe acceptance. If the terminal supports contact chip technology, then products supported for *PayPass* must also be supported for contact chip transactions.

## Acquirer Requirements

### Terminals

---

A terminal that supports magnetic stripe and EMV chip contact transactions (hybrid terminal) that also supports *PayPass* should support *PayPass - M/Chip*.

---

<b>BP</b>	<b>ALL</b>	A hybrid terminal that also supports <i>PayPass</i> should support <i>PayPass - M/Chip</i> .
-----------	------------	--

---

<b>BP</b>	<b>ALL</b>	A <i>PayPass</i> terminal should also support contact transactions.
-----------	------------	---

---

<b>R</b>	<b>ALL</b>	A hybrid terminal must support on the chip contact interface every product supported on the contactless interface.
----------	------------	--

---

Locations that accept contactless only transactions are permitted in agreement with MasterCard and are used for specific merchant category codes on an individual country basis.

An updated list of countries and merchant categories that are allowed to accept *PayPass* only is maintained in the *Chargeback Guide* following notification in a *Europe Region Operations Bulletin*.

## Terminals

Acquirers and merchants must only use approved *PayPass* terminals.

### Approvals and Testing

Products which are not *PayPass* approved need to obtain approval before deployment. Subsequent changes to terminal software could affect compliance with *PayPass* Terminal Vendor testing and must be discussed with MasterCard.

---

<b>R</b>	<b>ALL</b>	Acquirers must only deploy terminals that have successfully completed the MasterCard <i>PayPass</i> vendor product approval process. Approvals are only given to properly licensed vendors.
----------	------------	---

---

### Terminal Branding

*PayPass* terminals must meet the MasterCard branding requirements. *PayPass* terminals use common interfaces to provide a consistent consumer and merchant experience. Please see the *PayPass - Mag Stripe Acquirer Implementation Requirements* and *PayPass - M/Chip Acquirer Implementation Requirements*.

In order to give the cardholder clear information as to where to tap the *PayPass* device on the *PayPass* terminal, acquirers must use the *PayPass* landing zone. The landing zone must indicate with the contactless identifier where the cardholder has to tap or hold the MasterCard *PayPass* card.

If space permits, MasterCard *PayPass* and other scheme branding may also be placed on the landing zone as long as branding rules are maintained and the contactless symbol is not obscured in any way. If space on the landing zone does not allow room for scheme branding, then it should be placed elsewhere at the point of interaction. It should not distract the customer from identifying the contactless symbol and the landing zone.

---

<b>R</b>	<b>ALL</b>	<i>PayPass</i> terminals must meet the MasterCard <i>PayPass</i> branding standards.
----------	------------	--

---

### Terminal Design and Ergonomics

Merchants should consider that the placement of the *PayPass* reader is particularly important to the cardholder using the reader. The *PayPass* reader contains the antenna and needs to be conveniently placed and visible. *PayPass* readers may be integrated within a payment terminal or be stand-alone devices.

MasterCard recommends that where appropriate, the *PayPass* reader is included in a PIN Entry/contact card acceptance device keeping the terminal footprint on the merchant site to a minimum.

If a merchant uses a separate Electronic Cash Register (ECR) and *PayPass* POS terminal, the payment amount generated by the ECR should be made automatically available to the *PayPass* terminal when a cardholder chooses to pay with *PayPass*. This integration eliminates the need for dual-amount entry by the clerk which is a key time-saver and also reduces the risk of error.

When the interaction with the card is successfully completed, the reader provides a visible and audible indication of a successful *PayPass* interaction to the cardholder. The visible and audio cues confirm the card can be removed, but not that transaction is approved or completed.

---

<b>BP</b>	<b>ALL</b>	The <i>PayPass</i> reader should be included in the PIN Entry Device to minimize the terminal footprint.
-----------	------------	--

---

<b>BP</b>	<b>ALL</b>	The payment amount should be made automatically available to the <i>PayPass</i> terminal by the electronic cash register. The amount should not have to be entered manually.
-----------	------------	--

---

<b>R</b>	<b>ALL</b>	The terminal must use visual and audible cues to the cardholder that the <i>PayPass</i> interaction has been successful and is complete.
----------	------------	--

---

*PayPass* acceptance devices must be designed to avoid accidental capture of MasterCard *PayPass* payment account information when a consumer intends to transact using the card's magnetic stripe or contact chip, where present.

*PayPass* readers must be designed to prevent the introduction of foreign objects which may degrade unit performance or be used to capture *PayPass* payment application data from a *PayPass* card or device.

## Acquirer Requirements

### Terminals

---

Consideration should be given that in some retail environments:

- The terminal may be subjected to physical abuse by consumers. It is recommended that it be constructed from durable materials and have the facility to be securely attached to a counter or mounting location.
- The terminal may be located in a position where liquid spillage may occur. It is recommended for such environments that the terminal be sealed to prevent liquids from causing damage to the internal components.

### Visual Card Checks

There is no need to complete visual card checks for *PayPass* transactions. Therefore, the merchant does not have to:

- Check any visual security features, such as the presence of a MasterCard hologram
- Visually check the valid date and the expiration date on the face of the card
- Manually check Warning Bulletins
- Compare the four-digit truncated account number imprinted in the signature panel with the last four digits of the embossed account number on the face of the card
- Compare the embossed account number on the face of the card with the number displayed or printed from the POS terminal
- Compare any photograph on the card with the person presenting the card
- Check that the card is signed (This does not mean that a signature is not required to complete the transaction)

Any automation of the above visual checks by the POS system, such as Swipe and Verify checks, must be capable of being overridden or disabled for the acceptance of *PayPass* transactions.

### Transaction Types

#### Payment

*PayPass* acquirers must support payment transactions.

---

<b>R</b>	<b>ALL</b>	<i>PayPass</i> acquirers must support payment transactions.
----------	------------	---

---

#### Purchase with Cash Back

Terminals may support cash back for MasterCard *PayPass*, according to the product rules. Cardholder verification and online authorization are always required for Purchase with Cash Back transactions.

Terminals must not support cash back for Maestro *PayPass* transactions.

---

<b>R</b>	<b>MS</b>	Purchase with Cash Back transactions must not be completed with Maestro <i>PayPass</i> .
<b>R</b>	<b>MC</b>	Cardholder verification and online authorization must always be performed for Purchase with Cash Back transactions.

---

### Refunds

Acquirers must be able to process refund transactions initiated via the *PayPass* interface. A refund must be to the same account as the original transaction.

Cardholder verification is not required for refunds. Authorization is not required for refunds.

Merchant support for *PayPass* refunds is recommended at a minimum of one *PayPass* enabled terminal in a merchant location.

**For *PayPass* - M/Chip transactions**, refunds over the contactless interface must be performed by reading the Track 2 details and then requesting an AAC. The refund is then cleared in the normal way. This prevents card risk management counters from being adversely impacted.

**For *PayPass* - Mag Stripe transactions**, refunds over the contactless interface must be performed by reading Track 2 details via the contactless interface and clearing the refund transaction in the normal way.

---

<b>R</b>	<b>ALL</b>	Acquirers must be able to support refunds via the contactless interface.
<b>R</b>	<b>ALL</b>	If <i>PayPass</i> – M/Chip refunds over the contactless interface are supported by the merchant, the transaction must be terminated by requesting an AAC from the card, if supported by the <i>PayPass</i> reader application.
<b>R</b>	<b>ALL</b>	If <i>PayPass</i> – Mag Stripe refunds over the contactless interface are supported by a merchant, the transaction must be performed by reading Track 2 details from the card.
<b>BP</b>	<b>ALL</b>	If refunds are supported by a merchant, they should be available for <i>PayPass</i> transactions via the contactless interface.

---

### Dynamic Currency Conversion

Dynamic Currency Conversion is not supported for *PayPass* transactions.

### Gratuities

If gratuities are to be included in the *PayPass* transaction then the cardholder should be offered the opportunity to add the gratuity amount before the *PayPass* transaction commences.

#### Online and Offline Capability

The terminal is normally online capable unless it is a CAT Level 3 terminal that is offline only. Other exceptions may be allowed by MasterCard such as Maestro acceptance on a bus.

Since some *PayPass - M/Chip* cards may be configured to work as offline only, MasterCard recommends that terminals not be online only.

---

<b>BP</b>	<b>ALL</b>	<i>PayPass</i> terminals should be online capable unless CAT Level 3 terminals or other exceptions approved by MasterCard.
-----------	------------	--

---

<b>BP</b>	<b>ALL</b>	<i>PayPass</i> terminals should not be online only for <i>PayPass - M/Chip</i> .
-----------	------------	--

---

#### PayPass Limits

In the technical specifications, three limits are used by terminals in processing *PayPass* transactions. The same limit may have different values for different products. The limits must be configurable for each AID accepted at the terminal.

The Terminal Contactless Transaction Limit is a maximum transaction amount above which a contactless transaction must not be performed.

Transactions less than or equal to the Terminal CVM Required Limit do not require cardholder verification and, unless specifically requested by the cardholder, do not require a printed receipt. This means the facility to produce receipts must be available unless some special circumstances apply. For *PayPass* transactions above the Terminal CVM Required Limit, normal cardholder verification and receipt printing procedures apply.

The Terminal Contactless Floor Limit is a transaction amount above which online issuer authorization is required.<sup>1</sup>

#### Terminal Contactless Transaction Limit

When more than one *PayPass* application is identified on a card, an application for which the Terminal Contactless Transaction Limit is exceeded must not be used to complete a transaction. The transaction may be performed if other applications are identified permitting the transaction amount or if the terminal should prompt for a contact transaction to be performed.

There is no maximum transaction amount for MasterCard *PayPass* set in the MasterCard rules. There is no maximum transaction amount for Maestro *PayPass* set in **soft limit** markets.

---

<b>BP</b>	<b>ALL</b>	Terminals should prompt cardholders and/or merchants to use an alternative technology to perform the transaction if the Terminal Contactless Transaction Limit is exceeded for all <i>PayPass</i> applications on the card.
-----------	------------	---

---

---

1. Acquirers should be aware that the transaction limits discussed here are managed and supported differently in the different version of the *PayPass - M/Chip* reader.

### Terminal CVM Required Limit

Transactions less than or equal to the Terminal CVM Required Limit do not require cardholder verification.

Transactions greater than the Terminal CVM Required Limit require cardholder verification if the acquirer wants to avoid potential chargeback liability. If a merchant accepts these transactions with no cardholder verification, then the merchant may be liable for disputed transactions.

**For MasterCard PayPass**, the limits published in the *Chargeback Guide* are defined as chargeback protection amounts. These amounts are equivalent to the Terminal CVM Required Limit.

**For Maestro PayPass - M/Chip**, the terminal must support only No CVM as the CVM method for transactions less than or equal to the Terminal CVM Required Limit.

Terminals in markets that allow Maestro *PayPass* transactions above the Terminal CVM Required Limit must not support No CVM for Maestro above this limit. Otherwise, cards from **hard limit** markets, which do not support online PIN in the CVM List (*PayPass*), would be accepted for transactions above the ceiling limit with no cardholder verification.

---

<b>R</b>	<b>MS</b>	A Maestro <i>PayPass - M/Chip</i> terminal must support No CVM as the CVM method for transactions less than or equal to the Terminal CVM Required Limit.
<hr/>		
<b>R</b>	<b>MS</b>	Terminals in markets that allow Maestro <i>PayPass</i> transactions above the Terminal CVM Required Limit must not support No CVM for Maestro above this limit.

---

### Terminal Contactless Floor Limit

**For PayPass - M/Chip** transactions less than or equal to the Terminal Contactless Floor Limit may be authorized offline. Transactions greater than this limit should be authorized online by the issuer to provide the acquirer protection against authorization related chargebacks. Online issuer authorization may be required for transactions less than or equal to this limit, if this is the outcome of the terminal and card risk management.

**For PayPass - Mag Stripe** transactions, online issuer authorization is normally obtained for all transactions.

Generally, there are no special floor limits applicable to *PayPass* transactions. The same limits apply for contact transactions. In certain markets, *PayPass* specific floor limits have been defined, refer to the Quick Reference Booklet to view details of all current floor limits. However, terminal implementations should be able to maintain and use this limit independently for each interface.

---

<b>BP</b>	<b>ALL</b>	Transactions greater than the Terminal Contactless Floor Limit should be authorized online by the issuer.
-----------	------------	---

---

#### Maestro PayPass Limits

For Maestro *PayPass*, in any market, one of the following criteria would apply:

- The Terminal Contactless Transaction Limit and Terminal CVM Required Limit have the same value. Collectively they are referred to as the ceiling limit and their value is defined in the *Maestro Global Rules*. All Maestro *PayPass* transactions are completed with no cardholder verification. This is defined as a **hard limit** market.
- There is no maximum transaction amount. Transactions may be completed above the Terminal CVM Required Limit. A merchant must obtain cardholder verification to protect against chargebacks. This is defined as a **soft limit** market.

Details of the exception markets which allow transactions above the ceiling limit are announced in the applicable *Europe Region Operations Bulletin*.

#### PayPass Mode Selection

The cardholder decides whether to use *PayPass* or an alternative interface on the card. The terminal does not drive this decision.

If the cardholder chooses to use *PayPass*, and both the card and terminal support *PayPass - M/Chip*, then this mode must be used to complete the transaction.

---

<b>R</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> must be used if both the card and terminal support it.
----------	------------	--

---

#### Data Usage

*PayPass* acquirers must only use data read from the contactless interface for *PayPass* transactions. Data obtained from the contactless interface must not be used for another transaction type.

---

<b>R</b>	<b>ALL</b>	Data read from the <i>PayPass</i> interface may only be used for <i>PayPass</i> transactions.
----------	------------	---

---

#### Track Data Consistency

For *PayPass - Mag Stripe* transactions, some POS systems collect Track 1 data, truncate it, and process it as Track 2. *PayPass* Track 1 and Track 2 data may be different. For this reason, merchants and acquirers must make sure that Track 1 data is processed as Track 1 and Track 2 data is processed as Track 2. If data from one track is presented as the other, this may cause the transaction to be rejected by the card issuer as the Dynamic CVC3 cannot verify correctly.

Track 2 Equivalent Data is mandatory for *PayPass - M/Chip* transactions. It must be transmitted to the issuer in every authorization message.

---

<b>R</b>	<b>ALL</b>	Merchants and acquirers must make sure that Track 1 Data is processed as Track 1 and Track 2 Data is processed as Track 2.
<b>R</b>	<b>ALL</b>	Track 2 Equivalent Data must be used in the authorization request for <i>PayPass - M/Chip</i> transactions.

---

### Service Codes

MasterCard *PayPass* issuers may choose to use service code values in the *PayPass* data different from those typically used for magnetic stripe cards. A service code read during the *PayPass* transaction that indicates the presence of a chip card does not mean that the terminal must prompt for a contact transaction. A service code read during the *PayPass* transaction indicating that PIN is required does not mean that PIN is required for a *PayPass* transaction below the chargeback protection amount.

---

<b>R</b>	<b>ALL</b>	Terminals must not prompt for a contact transaction just because the service code read during the <i>PayPass</i> transaction indicates a chip is present on the card.
<b>R</b>	<b>ALL</b>	Terminals must not prompt for PIN for transactions less than or equal to the chargeback protection amount just because the service code read during the <i>PayPass</i> transaction indicates that a PIN is required.

---

### Cardholder Name

*PayPass* cards must not include the cardholder name in the data read through the contactless interface. POS systems that normally obtain and make use of the cardholder name from Track 1 data obtained from a magnetic stripe read must be able to accommodate this difference.

---

<b>R</b>	<b>ALL</b>	Terminals that process Track 1 data must be able to handle the data without a fully populated cardholder name.
----------	------------	--

---

### Application Selection

Terminals must maintain an independent list of AIDs accepted by the terminal for *PayPass*, compared to the contact interface.

The highest priority available payment application is selected automatically by the *PayPass* terminal. *PayPass* terminals must support application selection without cardholder assistance as defined in *EMV Book 1, Section 12.4, Step 5*. If priorities have not been set in the card, then the first available application must be selected.

Cardholder confirmation must not be supported by the terminal for *PayPass* transactions.

## Acquirer Requirements

### Offline Card Authentication

---

---

<b>R</b>	<b>ALL</b>	Terminals must support application selection without cardholder assistance.
----------	------------	---

---

<b>R</b>	<b>ALL</b>	Terminals must not support cardholder confirmation.
----------	------------	---

---

The AID value used for *PayPass* is the same AID used for the contact interface. There are no specific AIDs for *PayPass*.

Supported AIDs are:

- MasterCard 'A0000000041010'
- Maestro 'A0000000043060'

An application on the card can be selected by the terminal if the ADF is identical to, or begins with, an AID supported by the terminal. PIX extensions may be used by issuers but identification of *PayPass* cards uses the product AID irrespective of any extension. Terminals must support partial name matching for application selection.

---

<b>R</b>	<b>ALL</b>	Terminals must support partial name matching during application selection.
----------	------------	--

---

## Offline Card Authentication

For *PayPass - M/Chip*:

- Online only *PayPass* terminals do not need to support offline card authentication methods (CAM).
- Offline capable *PayPass - M/Chip* terminals must support offline CAM.

---

<b>R</b>	<b>ALL</b>	All offline capable <i>PayPass - M/Chip</i> terminals must support CDA.
----------	------------	---

---

*PayPass* does not support DDA.

The payment system public keys for *PayPass - M/Chip* are the same values and may be shared with those used for MasterCard contact transactions. Terminals must contain all current keys and must be able to store up to six CA Public Keys per RID.

The terminal must associate each key with the following key-related information that is used with the key.

- Certification Authority Public Key Check Sum (if required)
- Certification Authority Public Key Exponent
- Certification Authority Public Key Index
- Certification Authority Public Key Modulus

MasterCard test public keys must not be held in operational terminals.

<b>R</b>	<b>ALL</b>	All offline capable <i>M/Chip</i> terminals must hold all the active and current MasterCard public keys.
<b>R</b>	<b>ALL</b>	Terminals must only accept keys that the terminal can authenticate as originating from the genuine acquirer.
<b>R</b>	<b>ALL</b>	Acquirers must be able to verify that all the appropriate keys are loaded into all terminals that generate transactions which they acquire.
<b>R</b>	<b>ALL</b>	Terminals must not hold test public keys which might be used for live transactions.

## Cardholder Verification

Cardholder verification is not required for a *PayPass* transaction less than or equal to the chargeback protection amount.

To enjoy chargeback protection, the *PayPass* transaction must be properly identified in authorization and clearing records.

For transactions greater than the chargeback protection amount, a CVM is required. If transactions are completed without cardholder verification and are above the chargeback protection amount, then the acquirer may be liable for disputed transactions. Maestro terminals in **soft limit** markets that accept transactions above the ceiling limit with cardholder verification must not accept transactions above the ceiling limit with no cardholder verification.

**For *PayPass* - *M/Chip* transactions**, the reader must complete CVM Processing for all transaction amounts, both above and below the Terminal CVM Required Limit. The CVM is determined by the CVM list or other data supplied by the card and the CVM capabilities indicated by the *PayPass* reader application of the terminal. The CVM capabilities may be different above and below the Terminal CVM Required Limit.

MasterCard recommends to process *PayPass* transactions:

- Without cardholder verification if less than or equal to the chargeback protection amount
- With cardholder verification if above the chargeback protection amount

**For MasterCard *PayPass***, if an attended terminal supports transactions greater than the chargeback protection amount, then the terminal:

- Must support signature
- May support online PIN
- May support On Device Cardholder Verification

## Acquirer Requirements

### Cardholder Verification

---

**For Maestro PayPass in soft limit** markets, attended terminals that support transactions above the ceiling limit:

- Must support online PIN
- Should support On Device Cardholder Verification

*PayPass* terminals must not permit PIN Entry Bypass. *PayPass* terminals must not support offline PIN on the *PayPass* interface.

Purchase with Cash Back transactions must be completed with cardholder verification, regardless of the amount. ATM transactions must be verified by online PIN.

---

<b>BP</b>	<b>ALL</b>	<i>PayPass - M/Chip</i> terminals, except CAT Level 1 terminals, should not request cardholder verification for transactions less than or equal to the chargeback protection amount.
<b>BP</b>	<b>MC</b>	All MasterCard <i>PayPass - M/Chip</i> terminals should not support No CVM for transactions greater than the chargeback protection amount.
<b>R</b>	<b>MC</b>	MasterCard <i>PayPass</i> terminals must support signature for transactions greater than the chargeback protection amount.
<b>BP</b>	<b>MC</b>	MasterCard <i>PayPass</i> terminals that support transactions greater than the chargeback protection amount should support online PIN.
<b>BP</b>	<b>MC</b>	MasterCard <i>PayPass</i> terminals should support On Device Cardholder Verification for transactions greater than the chargeback protection amount.
<b>R</b>	<b>MS</b>	Maestro <i>PayPass</i> terminals must support No CVM for transactions less than or equal to the ceiling limit.
<b>R</b>	<b>MS</b>	Maestro <i>PayPass</i> terminals must not support No CVM for transactions greater than the ceiling limit.
<b>R</b>	<b>MS</b>	Maestro <i>PayPass</i> terminals in <b>soft limit</b> markets that support transactions greater than the ceiling limit must support online PIN.
<b>BP</b>	<b>MS</b>	Maestro <i>PayPass</i> terminals in <b>soft limit</b> markets should support On Device Cardholder Verification for transactions greater than the ceiling limit.
<b>R</b>	<b>ALL</b>	<i>PayPass</i> terminals must not perform PIN Entry Bypass.
<b>R</b>	<b>MC</b>	MasterCard <i>PayPass</i> Purchase with Cash Back transactions require cardholder verification, regardless of the amount.
<b>R</b>	<b>ALL</b>	ATM transactions must be verified by online PIN.

---

**For *PayPass - M/Chip* transactions**, the CVM used is identified before Terminal Action Analysis. It is determined by the terminal based on the methods supported by the *PayPass* reader application in the terminal and the CVM List (*PayPass*) and other data personalized in the chip application.

The use of No CVM must be positively identified by the EMV process. It does not mean skip CVM processing.

CAT Level 1 terminals must support and use online PIN for all *PayPass* transactions.

CAT Level 2 and CAT Level 3 terminals must use No CVM for all *PayPass* transactions.

---

<b>R</b>	<b>ALL</b>	CAT Level 1 terminals must support online PIN.
<b>R</b>	<b>ALL</b>	CAT Level 2 and CAT Level 3 terminals must support only No CVM for <i>PayPass</i> transactions.

---

When online PIN is used to verify the cardholder, if the authorization is declined by the issuer because the PIN is incorrect, the transaction should be restarted and the cardholder prompted to re-enter their PIN.

---

<b>BP</b>	<b>ALL</b>	If an online authorization is declined by the issuer because of an incorrect PIN, then a new <i>PayPass</i> transaction should be started.
-----------	------------	--

---

Offline PIN is not supported for *PayPass - M/Chip* transactions. Offline PIN may be supported at the same terminal but only for contact EMV transactions. Terminals must ensure that offline PIN is never selected as the CVM for a *PayPass* transaction.

---

<b>R</b>	<b>ALL</b>	Terminals must not request offline PIN for <i>PayPass</i> transactions.
----------	------------	---

---

**For *PayPass - Mag Stripe* transactions,** the CVM is determined by the terminal.

If the online PIN is incorrect, a new transaction should be started and the cardholder prompted to retry PIN entry.

If a signature is required for cardholder verification, this may be captured on a receipt or electronically. When the *PayPass* cardholder device does not carry the customer signature and signature verification is required, the signature must be verified against either the companion card or some form of formal identification. Formal identification must include a specimen signature and be confirmed as belonging to the same cardholder. If this is not available, the *PayPass* transaction must be cancelled or completed with no cardholder verification at the acquirer's risk.

## Terminal Risk Management

Exception File Checking by the terminal is optional for *PayPass* transactions. It may be done after the communication with the card is finished. The current terminal application version number for *PayPass* is '0002'.

*PayPass* terminals may perform a cumulative floor limit check by adding the last transaction in the terminal log file, if present and if performed by the same card, to the current transaction amount and comparing the total with the Terminal Contactless Floor Limit.

Neither Velocity Checking by the terminal nor Random Transaction Selection is performed for *PayPass* transactions.

---

<b>R</b>	<b>ALL</b>	The terminal application version number for <i>PayPass - M/Chip</i> must be set to '0002'.
----------	------------	--

---

## Terminal Action Codes (TACs)

The mandatory TACs used for *PayPass* transactions are given in the following chapter. The TACs are different depending on the terminal capabilities.

If the terminal supports contact transactions the terminal must maintain the *PayPass* TACs independently.

## Authorization Responses

If a response to an authorization is not received, transactions are approved at the acquirer's risk.

For *PayPass - M/Chip* there is no second terminal or card risk management possible, as there is for contact transactions.

Referrals or Call Me issuer responses are not required to be supported by acquirers for *PayPass*. Referral responses may be declined by the acquirer or merchant.

Retaining the card at an attended terminal is optional as it may be impractical for an attendant to retain a card that is not initially handed over to the merchant during payment.

## Receipts

For transactions less than or equal to the Terminal CVM Required Limit, a *PayPass* merchant, card acceptor, must make a receipt available if requested by the cardholder.

Receipts may be offered at the end of a transaction, rather than the cardholder or merchant needing to confirm if they would like a receipt before continuing.

Above the Terminal CVM Required Limit, a receipt must always be provided if the terminal has that capability.

Any receipt should specifically identify *PayPass* transactions. The input method should be shown as Contactless, CONTACTLESS, *PayPass* or RF for *PayPass* transactions.

<b>R</b>	<b>ALL</b>	A receipt must be available for transactions less than the chargeback protection amount on cardholder request.
<b>R</b>	<b>ALL</b>	A receipt must be provided for transactions above the chargeback protection amount if the terminal supports receipt printing.
<b>BP</b>	<b>ALL</b>	Terminals should not routinely produce receipts for transactions less than the chargeback protection amount.

## Subsequent Contact Transactions

If a *PayPass - M/Chip* transaction does not successfully complete for any reason other than a communication error, then the *PayPass* terminal should prompt for a contact transaction to be performed. It should not be assumed that the same card will be declined when used in contact profile.

If a *PayPass* transaction fails, then a new transaction may be attempted using a different card read method supported by both the card and the terminal in the order of preference of:

- Contact EMV
- Magnetic stripe (swipe)

These transactions are authorized according to the current payment product rules for the technology. There are no changes to network messages to identify these transactions as having previously been attempted using the *PayPass* interface. There are no *PayPass* technical fallback transactions.

<b>BP</b>	<b>ALL</b>	<i>PayPass</i> terminals should prompt for a contact transaction when a <i>PayPass</i> transaction is declined by the card, terminal, or issuer, or if it fails to complete for any other reason other than a communication error.
-----------	------------	--

## Terminated Transactions

A terminal may allow a merchant to cancel a transaction:

- For a *PayPass - M/Chip* transaction, before the **GENERATE AC** command is issued

OR

- Before the terminal has requested an online authorization

The terminal should monitor the number of aborted transactions. If the frequency is high it is likely that a fraudster is trying to get a specific value of the Unpredictable Number. The terminal should take appropriate measures to reduce the risks of an attack, introducing wait times after three aborted transactions.

---

**BP ALL** The terminal should take appropriate measures to reduce the risks of an attack using aborted transactions.

---

## Cardholder Activated Terminals

For *PayPass* transactions at Cardholder Activated Terminals:

- For CAT Level 1 terminals the Terminal CVM Required Limit is zero, that is, CVM is always required for a CAT Level 1 transaction. The CVM is always online PIN as offline PIN is not supported for *PayPass* and signature is not possible at an unattended terminal
- For CAT Level 2 and Level 4 terminals the Terminal CVM Required Limit should be set to the chargeback protection amount
- For CAT Level 3 terminals, it is recommended that the Terminal CVM Required Limit and Terminal Contactless Transaction Limit be set to the maximum allowed transaction value for these devices indicated in the *Chargeback Guide*

Unattended terminals may operate at different levels according to the value of the transaction. For example, it is possible to operate as a CAT Level 2 terminal allowing No CVM, up to the chargeback protection amount and to operate as a CAT Level 1 terminal requiring online PIN above the chargeback protection amount.

## Automated Teller Machines

*PayPass* terminals may be deployed to provide contactless interface functionality for ATMs. The overall transaction flow and user interface is determined by the ATM, and is not considered in this document.

The integration of the *PayPass* terminal in the ATM implies certain constraints in its configuration in order to ensure the necessary behavior.

**For *PayPass* - Mag Stripe**, terminals can be used in ATMs without any special configuration or modification.

**For *PayPass* - M/Chip**, the terminal must always request an ARQC from the card. This online-only behavior is ensured by setting the Terminal Contactless Floor Limit to zero.

Since all transactions are performed online, offline card authentication is not necessary. The terminal capabilities can therefore be configured not to support SDA or CDA.

The standard cardholder verification method used in ATM transactions is online PIN. The Terminal Capabilities - CVM Required must indicate support for only online PIN. It must not indicate support for any other CVM. Support for other CVMs such as On Device Cardholder Verification must be deactivated.

In addition, Terminal CVM Required Limit must be set to zero to ensure the terminal capabilities are taken into consideration at every transaction.

---

<b>R</b>	<b>ALL</b>	For use with ATM, the Terminal Contactless Floor Limit in the <i>PayPass</i> – <i>M/Chip</i> terminal must be set to zero.
<b>BP</b>	<b>ALL</b>	For use with ATM, the Terminal Capabilities in the <i>PayPass</i> – <i>M/Chip</i> terminal should be configured not to support any form of offline CAM.
<b>R</b>	<b>ALL</b>	For use with ATM, the Terminal Capabilities – CVM Required in the <i>PayPass</i> – <i>M/Chip</i> terminal must be configured to support only online PIN as a CVM. Support for all other forms of CVM must be de-activated.
<b>R</b>	<b>ALL</b>	For use with ATM, the Terminal CVM Required Limit in the <i>PayPass</i> – <i>M/Chip</i> terminal must be set to zero.

---

## Acquirer Network Requirements

Acquirers and merchants must support changes to transaction messages, intervening systems and networks indicating that a *PayPass* transaction has occurred.

### Data Elements

Acquirer databases must also identify the terminal as being *PayPass* capable. This impacts DE 61 and DE 22 in authorization messages and DE 22 in clearing messages. Other data elements contain the same data values as for existing transactions.

*PayPass* transactions from *PayPass - M/Chip* terminals are either:

- *PayPass - M/Chip* transactions with the same data elements as current chip transactions

OR

- *PayPass - Mag Stripe* transactions with the same data elements as current magnetic stripe transactions

*PayPass* transactions from *PayPass - Mag Stripe* terminals are always *PayPass - Mag Stripe* transactions with the same data elements as current magnetic stripe transactions.

Acquirers who deploy *PayPass - M/Chip* terminals must be Full Grade acquirers. Partial Grade acquirers must migrate to Full Grade chip acquiring and carry all of the minimum data set required. Full Grade acquirers provide DE 55 in the authorization request messages.

For *PayPass - M/Chip* transactions, it is not required to deliver issuer authorization response chip data, including Issuer Scripts, to the terminal in the authorization response. If the data is returned to the terminal then the terminal does not process the data. The terminal is not required to retain the data.

### Authorization Performance

The benefits of MasterCard *PayPass* are maximized when used with high-speed authorization lines.

### Authorization Responses

Referrals are not required to be supported by acquirers for *Paypass* transactions. Any referral response received may be treated as a decline.

### Service Codes

MasterCard *PayPass* issuers may choose to use service code values in the *PayPass* application different from those typically used for magnetic stripe cards. For this reason acquirers need to ensure that all processing systems support all service codes.

## Authorization Requirements

Specific values in existing subfields within the authorization message specify the terminal capability, DE 61, and the profile of operation, DE 22.

### Authorization Messages

*PayPass* transactions require new values in these data elements in authorization messages:

- DE 22, subelement 1, value of **07** is used for a contactless *M/Chip* transaction and a value of **91** is used for a contactless magnetic stripe transaction, even if performed at a *PayPass - M/Chip* terminal.
- DE 61, subelement 11, value of **3** is used for any transaction at a contactless *M/Chip* terminal, the terminal may also be contactless magnetic stripe capable, and a value of **4** is used for any transaction at a contactless magnetic stripe terminal.

Terminals and other parts of the acquirer system must be able to determine when transaction data has been obtained using the *PayPass* interface in order to properly process and identify the transaction to the issuer.

Acquirers should capture the Device Type indicator where present on a *PayPass* device and send this to the issuer in DE 48, subelement 23. The Device Type indicator may be included in the Third Party Data.

Acquirers must support full-grade EMV for all *PayPass - M/Chip* implementations. Partial grade acquiring is not permitted. For *PayPass - M/Chip* transactions, DE 55 is mandatory in authorization messages.

Requirements for acquirer generated reversals for online authorizations are for current processing.

---

<b>R</b>	<b>ALL</b>	Acquirers must process on their network interface and host system <i>PayPass</i> transactions as described above.
<b>R</b>	<b>ALL</b>	Acquirers must be full grade.
<b>BP</b>	<b>ALL</b>	Acquirers should include the Device Type indicator, where present, in the authorization message.

---

## Clearing Requirements

### Clearing Messages

Specific values in existing subfields within the clearing message specify the data input capability and the data input profile, DE 22. *PayPass* transactions require new values in these subfields.

DE 22, subfield 1 identifies the terminal capabilities and must contain:

## Acquirer Requirements

### Exception Processing

---

- the value of **M** for a transaction at a *PayPass - M/Chip* terminal, the terminal may also be *PayPass Mag-Stripe* capable
- the value of **A** for a transaction at a *PayPass Mag-Stripe* terminal

DE 22, subfield 7 identifies the card data input profile for this transaction and must contain:

- the value of **M** for a *PayPass - M/Chip* transaction
- the value of **A** for a *PayPass - Mag Stripe* transaction

For *PayPass - M/Chip* transactions, DE 55 is mandatory in clearing.

No aggregation or truncation of *PayPass* transactions is permitted, except in certain transit situations.

---

**R ALL** Acquirers must process on their clearing interface and host system *PayPass* transactions as described above.

---

## Exception Processing

Acquirers do not need to fulfill a retrieval request for a transaction identified as a *PayPass* transaction that is equal to or less than the chargeback protection amount, except in certain transit situations.

No new chargeback reason codes have been introduced to support *PayPass*. Updates to the existing reason codes are documented in the *Chargeback Guide* or in the Maestro Global Product Rules.

A properly identified *PayPass* transaction, that is less than or equal to the applicable chargeback protection amount, is protected against chargebacks using the following message reason codes.

---

Message Reason Code	Description
4801	Requested Transaction Data Not Received
4802	Requested/Required Information Illegible or Missing
4837	No Cardholder Authorization

---

For message reason code **4837 - No Cardholder Authorization** the transaction must be properly authorized, offline by a chip or online by the issuer, for protection against chargeback.

## On-behalf Services

MasterCard offers the *PayPass* Mapping Service—an optional service that helps issuers process different *PayPass* account numbers by translating them into primary account numbers that can be processed with minimal impact.

---

<b>R</b>	<b>ALL</b>	Acquirer host systems must be able to process <i>PayPass</i> transactions that make use of the MasterCard <i>PayPass</i> Mapping Service. Refer to the <i>PayPass On-behalf Services Guide</i> for more information.
----------	------------	--

---



---

## Chapter 5 Data Requirements

*This chapter defines data requirements for PayPass.*

---

Terminal Action Codes .....	5-1
Offline Only Terminals .....	5-3
Payment Scheme Specific Data Objects .....	5-5
Third Party Data .....	5-5
Application Capabilities Information .....	5-6



## Terminal Action Codes

Chip terminals must use the TAC settings defined in this document for *PayPass* transactions.

As *PayPass* terminals never perform the 2nd **GENERATE AC** command, the IAC - Default and TAC - Default is never applicable at online capable terminals. For *PayPass* transactions, if an online authorization is incomplete, then the transaction is declined.

The IAC - Default and TAC - Default are used at offline only terminals.

Required and recommended values of IACs are provided in the *PayPass - M/Chip Personalization Data Specifications* manual.

### MasterCard and Maestro PayPass Terminal Action Codes for Online Capable Terminals

Byte/Bit	Meaning	Denial	Online	Default
Byte 1 8	Offline Data Authentication was not performed	0	1	1
7	Offline SDA failed	0	1	1
6	ICC data missing	0	1	1
5	ICC on Hot Card File	0	1	1
4	Offline DDA failed	0	1	1
3	Combined DDA/AC Generation failed	0	1	1
2-1	RFU	0	0	0
Byte 2 8	ICC & Terminal have different App Version Numbers	0	0	0
7	Expired application	0	1	1
6	Application not yet effective	0	0	0
5	Service not allowed for card product	0	1	1
4	New Card	0	0	0
3-1	RFU	0	0	0
Byte 3 8	Cardholder verification failed (see exception below)	0	1	1
7	Unrecognized CVM	0	0	0
6	PIN try limit exceeded	0	0	0

## Data Requirements

### Terminal Action Codes

5	PIN req but PIN pad not present/not working	0	1	1
4	PIN req, PIN pad present but PIN not entered	0	1	1
3	Online PIN entered	0	1	1
2-1	RFU	0	0	0
Byte 4 8	Transaction exceeds floor limit	0	1	1
7	LCOL exceeded	0	0	0
6	UCOL exceeded	0	0	0
5	Randomly selected for online processing	0	0	0
4	Merchant forced transaction online	0	1	1
3-1	RFU	0	0	0
Byte 5 8	Default TDOL used	0	0	0
7	Issuer Authentication Unsuccessful	0	0	0
6	Script failed before final cryptogram	0	0	0
5	Script failed after final cryptogram	0	0	0
4-1	RFU	0	0	0

- Terminal Action Code - Denial: '0000000000'
- Terminal Action Code - Online: 'FC509C8800'
- Terminal Action Code - Default: 'FC509C8800'

For MasterCard *PayPass* on online capable terminals that do not support online PIN verification, the settings in the following table must be used.

Byte/Bit	Meaning	Denial	Online	Default
Byte 3 6	PIN try limit exceeded	0	0	0
Byte 3 5	PIN req but PIN pad not present/not working	0	0	0
Byte 3 4	PIN req, PIN pad present but PIN not entered	0	0	0
Byte 3 3	Online PIN entered	0	0	0

- Terminal Action Code - Denial: '0000000000'
- Terminal Action Code - Online: 'FC50808800'
- Terminal Action Code - Default: 'FC50808800'

In Maestro *PayPass* **soft limit** implementations the following setting must be used :

Byte/Bit	Meaning	Denial	Online	Default
Byte 3 8	Cardholder verification failed	1	0	0

- Terminal Action Code - Denial: '0000800000'
- Terminal Action Code - Online: 'FC500C8800'
- Terminal Action Code - Default: 'FC500C8800'

## Offline Only Terminals

### MasterCard and Maestro PayPass Terminal Action Codes for Offline Only Terminals

Byte/Bit	Meaning	Denial	Online	Default
Byte 1 8	Offline Data Authentication was not performed	1	0	0
7	Offline SDA failed	1	0	0
6	ICC data missing	1	0	0
5	ICC on Hot Card File	1	0	0
4	Offline DDA failed	1	0	0
3	Combined DDA/AC Generation failed	1	0	0
2-1	RFU	0	0	0
Byte 2 8	ICC & Terminal have different App Version Nos	0	0	0
7	Expired application	1	0	0
6	Application not yet effective	0	0	0
5	Service not allowed for card product	1	0	0
4	New Card	0	0	0
3-1	RFU	0	0	0
Byte 3 8	Cardholder verification failed	1	0	0

**Data Requirements**  
**Offline Only Terminals**

---

7	Unrecognized CVM	0	0	0
6	PIN try limit exceeded	0	0	0
5	PIN req but PIN pad not present/not working	0	0	0
4	PIN req, PIN pad present but PIN not entered	0	0	0
3	Online PIN entered	0	0	0
2-1	RFU	0	0	0
Byte 4 8	Transaction exceeds floor limit	1	0	0
7	LCOL exceeded	0	0	0
6	UCOL exceeded	0	0	0
5	Randomly selected for online processing	0	0	0
4	Merchant forced transaction online	0	0	0
3-1	RFU	0	0	0
Byte 5 8	Default TDOL used	0	0	0
7	Issuer Authentication Unsuccessful	0	0	0
6	Script failed before final cryptogram	0	0	0
5	Script failed after final cryptogram	0	0	0
4-1	RFU	0	0	0

- Terminal Action Code - Denial: 'FC50808000'
- Terminal Action Code - Online: '0000000000'
- Terminal Action Code - Default: '0000000000'

## Payment Scheme Specific Data Objects

This section lists MasterCard defined data objects used between the card and the terminal for *PayPass* transactions.

### Third Party Data

<b>Tag</b>	'9F6E'
<b>Length</b>	5–32
<b>Format</b>	b
<b>Descriptions</b>	<p>The Third Party Data contains proprietary information from a third party and is coded as shown below. If present in the <i>PayPass</i> Card, the Third Party Data is returned in a file read using the <b>READ RECORD</b> command or in the File Control Information Template.</p> <p>The Device Type subfield is present when the most significant bit of byte 1 of the Unique Identifier is set to 0b. In this case, the maximum length of the Proprietary Data field is 26 bytes.</p> <p>Third Party Data may be used to communicate the device type to the terminal, even when there is no Unique ID or Proprietary Data being used. In this case a static, default value of '0000' for the Unique ID is used.</p>

### Third Party Data Format

Data Field	Length	Format
Country Code	2	Country Code according to [ISO 3166-1]
Unique Identifier	2	b (value assigned by MasterCard)
Device Type	0 or 2	b
Proprietary Data	1–28	b

Device Types are assigned as follows:

Device Type	Value
Card	0
Mobile phone or smart phone	1
Key fob	2
Watch	3
Mobile tag	4

## Data Requirements

### Payment Scheme Specific Data Objects

---

Wristband	5
Mobile phone case or sleeve	6
RFU	

## Application Capabilities Information

<b>Tag</b>	'9F5D'
<b>Length</b>	3
<b>Format</b>	b
<b>Descriptions</b>	The Application Capabilities Information is an optional data object included in the File Control Information Template of the <i>PayPass</i> Card. It lists a number of card features beyond regular payment and is coded as defined below.

Byte	Bit	Description
Byte 1	b8-5	Version number 0000: VERSION 0 Other values: RFU
	b4-1	Data Storage Version Number 0000: DATA STORAGE NOT SUPPORTED 0001: VERSION 1 0010: VERSION 2 Other values: RFU
Byte 2	b8-3	RFU
	b2	Support for balance reading
	b1	CDA Indicator 0: CDA SUPPORTED AS IN EMV 1: CDA SUPPORTED OVER TC, ARQC AND AAC

**Data Requirements**  
**Payment Scheme Specific Data Objects**

---

Byte 3	b8-1	SDS Scheme Indicator
		00000000: Undefined SDS configuration
		00000001: All 10 tags 32 bytes
		00000010: All 10 tags 48 bytes
		00000011: All 10 tags 64 bytes
		00000100: All 10 tags 96 bytes
		00000101: All 10 tags 128 bytes
		00000110: All 10 tags 160 bytes
		00000111: All 10 tags 192 bytes
		00001000: All SDS tags 32 bytes except '9F78' which is 64 bytes
		Other values: RFU



---

## **Appendix A Abbreviations**

*Provides a listing of abbreviations used throughout the manual.*

---

Abbreviations.....	A-1
--------------------	-----



## Abbreviations

Abbreviation	Description
AAC	Application Authentication Cryptogram
ADF	Application Definition File
AFL	Application File Locator
AID	Application Identifier
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
ATM	Automated Teller Machine
CA	Certification Authority
CAM	Card Authentication Method
CAT	Cardholder Activated Terminal
CDA	Combined DDA/AC Generation
CDOL	Card Risk Management Data Object List
CPV	Card Personalization Validation
CVC	Card Verification Code
CVC1	Card Verification Code (used for magnetic stripe transactions)
CVC3	Card Verification Code (used for <i>PayPass</i> )
CVM	Cardholder Verification Method
DDA	Dynamic Data Authentication
DE	Data Element
EMV	Europay MasterCard Visa
IAC	Issuer Action Code
ICC	Integrated Circuit Card
ISO	International Organization for Standardization
nUN	Number of digits of the Unpredictable Number
PIN	Personal Identification Number
PIX	Proprietary Application Identifier
POS	Point of Sale
PPSE	Proximity Payment System Environment

## Abbreviations

### Abbreviations

---

PVV	PIN Verification Value
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
SDA	Static Data Authentication
SDS	Standalone Data Storage
SFI	Short File Identifier
TAC	Terminal Action Codes
TC	Transaction Cryptogram
TVR	Terminal Verification Results
UN	Unpredictable Number