



# Card Personalization Validation Guide For *PayPass* – Mag Stripe

**December 2008**

Changes from the previous edition (October 2008) are:

- The address to which Physical Cards need to be shipped is changing as from January 1, 2009.
- The Contact CPV Service Provider subprocess has been merged into the Sample Submission subprocess. The number of tasks required has been reduced and optimized by allowing more tasks to be performed in parallel with each other.
- The business process diagrams have been updated to concentrate on the choreography between you (the acquirer) and the other entities. The activities performed by other entities are now shown as a black box instead of as abstract tasks/activities.
- Editorial Corrections.

**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 manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

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

MasterCard Worldwide  
Chip Centre of Excellence  
Chaussée de Tervuren 198A  
B-1410 Waterloo  
Belgium.  
[www.mastercard.com](http://www.mastercard.com)

---

<b>1 Introduction.....</b>	<b>1-1</b>
Purpose .....	1-1
Audience .....	1-1
Who is involved with Card Personalization Validation .....	1-1
As an Issuer who has Delegated to a Processor .....	1-2
As an Issuer.....	1-2
As a Processor.....	1-3
CPV Contact Information .....	1-4
Related Information .....	1-4
Business Process Diagram Conventions.....	1-5
<b>2 The CPV Process .....</b>	<b>2-1</b>
Implementation.....	2-1
Overview.....	2-1
For Issuers who Delegate to a Processor .....	2-2
Request Report from Processor.....	2-2
Change Notification Submission .....	2-2
For Issuers and Processors .....	2-2
Issuer or Processor Self-Assessment.....	2-2
Sample Submission .....	2-3
Change Notification Submission .....	2-3
<b>3 Request Report from Processor.....</b>	<b>3-1</b>
Overview.....	3-1
Process .....	3-1
<b>4 Issuer or Processor Self-Assessment .....</b>	<b>4-1</b>
Overview.....	4-1
Process .....	4-1
<b>5 Sample Submission .....</b>	<b>5-1</b>
Overview.....	5-1
Process .....	5-2

## Table of Contents

---

<b>6 Change Notification Submission .....</b>	<b>6-1</b>
Overview .....	6-1
Process .....	6-1
<b>Appendix A Test Issuer Master Key Exchange .....</b>	<b>A-1</b>
A.1 Method 1 — Clear Text Key .....	A-1
A.2 Method 2 — Clear Text Key Components .....	A-2
A.3 Method 3 — Encrypted Key Using a MasterCard-specified Key Encryption Key .....	A-2
A.4 Method 4 — Encrypted Key using Issuer-specified KEK .....	A-3

# 1 Introduction

This chapter provides an introduction to the Card Personalization Validation process for *PayPass* – Mag Stripe technical products.

## Purpose

The objective of Card Personalization Validation (CPV) is to ensure that every Technical Product bearing a MasterCard brand mark offers the correct level of service, acceptance, interoperability, performance, and security to cardholders and acceptance locations.

The Card Personalization Validation (CPV) process for *PayPass* – Mag Stripe ensures that these objectives are met, with particular emphasis on verifying that the *PayPass* – Mag Stripe Technical Product(s) that you plan to issue have the correct contactless application personalization.

## Audience

MasterCard provides this guide for issuers, processors, and their authorized agents. Specifically, the following personnel should find this guide useful:

- Program Managers and Project Managers for issuers implementing new or amending existing *PayPass* – Mag Stripe Technical Products bearing a MasterCard brand mark.
- Program Managers and Project Managers for processors (or personalization bureaus) delegated by an issuer implementing new or amending existing *PayPass* – Mag Stripe Technical Products bearing a MasterCard brand mark.

## Who is involved with Card Personalization Validation

You can be involved with Card Personalization Validation for *PayPass* – Mag Stripe in three different ways:

- As an issuer who has delegated to a processor
- As an issuer
- As a processor (or personalization bureau) acting on behalf of an issuer

## **As an Issuer who has Delegated to a Processor**

If you are an issuer who has delegated to a processor, you are not directly involved with the testing aspect of Card Personalization Validation as your processor has to obtain the necessary approval.

However, you are responsible for ensuring that Technical Products issued by your processor have passed Card Personalization Validation. It is therefore necessary for you to ensure that your processor has obtained the necessary approval and that it is still valid. When there is a change in the Specifications the approval is invalid and your processor must obtain a new approval.

## **As an Issuer**

You must do Card Personalization Validation when you make any changes to your card, such as:

- You are issuing a new Technical Product. Figure 1.1 shows how Card Personalization Validation fits into the sequence of processes when issuing a new *PayPass* – Mag Stripe Technical Product.
- You have an existing Technical Product and want to amend any of the personalization characteristics (excluding cardholder related data and expiration dates). For example, changing the BIN whilst maintaining all other personalization parameters, or due to changes in *PayPass Personalization Data Specification* or as the result of an *Operational Bulletin*.
- You have an existing Technical Product and want to change the Vendor Product.

Depending upon the nature of the change, you do a self-assessment to determine whether you need to submit a sample for testing or to simply send in a change notification (which may result in you being requested to submit a sample for testing).

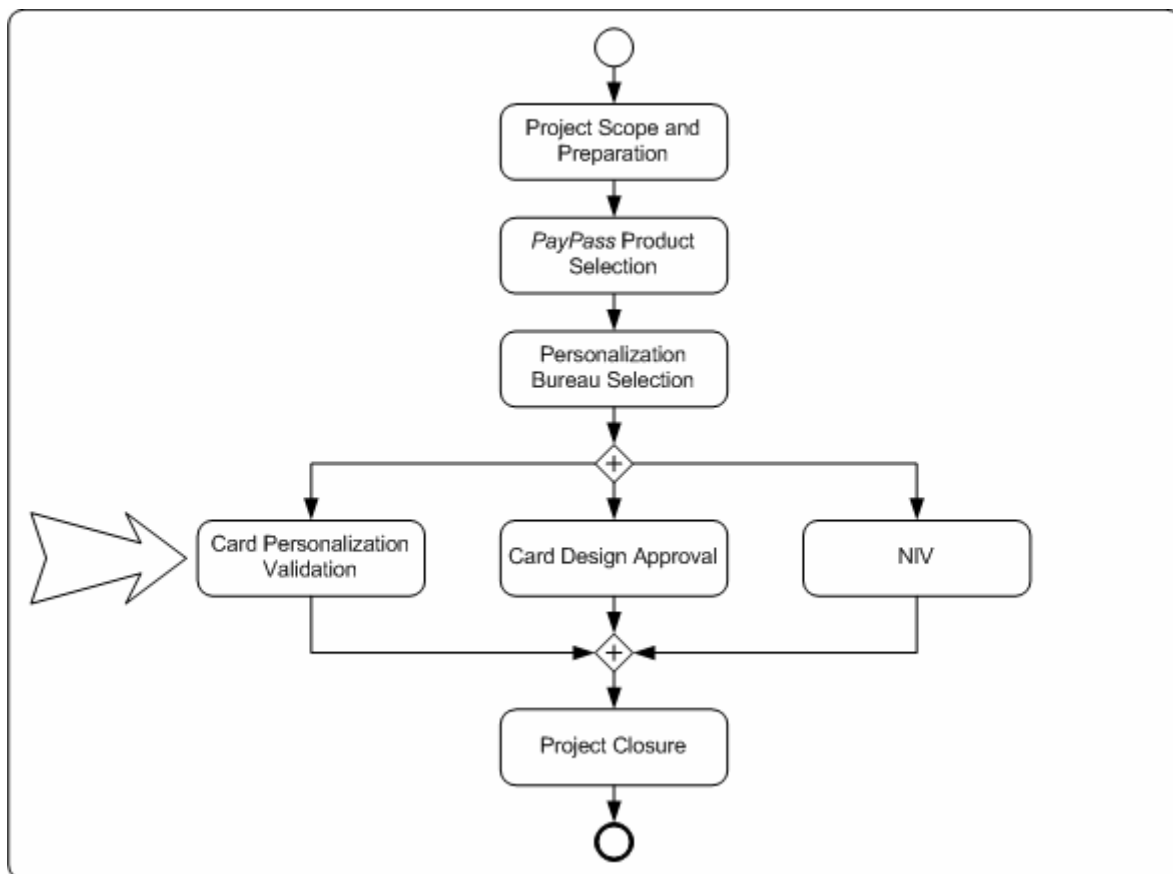
It is assumed that you have already chosen:

- The Technical Product
- The Personalization Bureau

It is also assumed that in choosing the above you have ensured that the vendors are appropriately licensed and the Vendor Products approved by MasterCard.

Certified vendors are listed in the Certified Vendors (for Card Production Services of any MasterCard, Maestro, or Cirrus Branded Card) document that is regularly published as an attachment to the Global Security Bulletin, available on MasterCard OnLine®.

A copy of the *PayPass* Vendor Product Letter of Approval for each approved product is published on [www.paypass.com](http://www.paypass.com).

Figure 1.1—Sequence of Processes when Issuing a New *PayPass* – Mag Stripe Technical Product

### As a Processor

As a processor, you need to do Card Personalization Validation under the same criteria and in the same manner as if you were an issuer, as detailed above.

You can also leverage CPV for a Technical Product to all your issuers without the need to reobtain CPV for each issuer program: if you have an existing *PayPass* Mag Stripe based Technical Product that has CPV, you can offer it to all your issuers provided that personalization parameters, with the exception of cardholder related data, are identical to that for which CPV was granted, and that it supports the *PayPass* personalization command set.

## CPV Contact Information

MasterCard Worldwide  
CPV Team  
Chip Center of Excellence  
Chaussée de Tervuren 198A  
B-1410 Waterloo  
Belgium

[chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com)

**From January 1, 2009, the Physical Cards should be shipped by secure courier to:**

FIME Asia Test Centre  
Suite 807-808, 8th Floor, No. 2, Lane 150, Sec. 5, Sinyi Road  
Sinyi District, Taipei  
TAIWAN 110

[chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com)

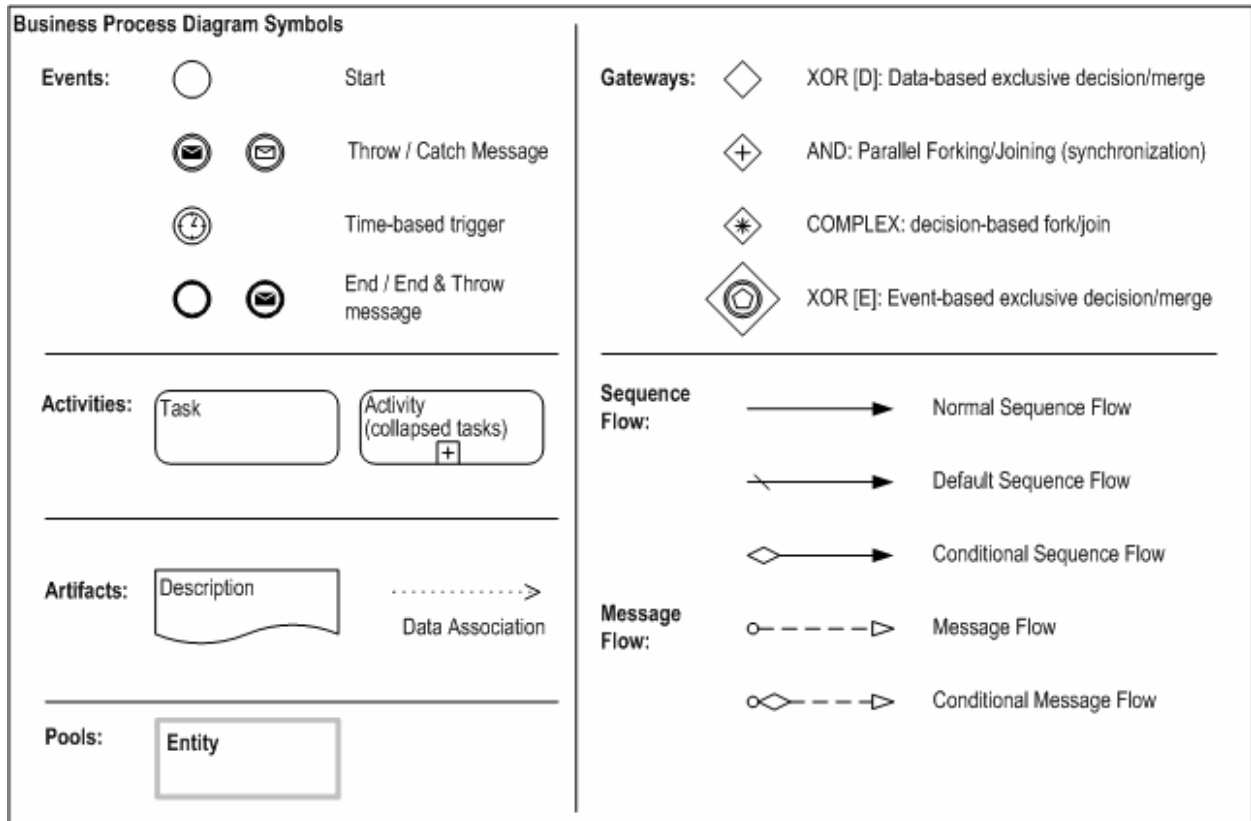
## Related Information

The following documents and resources provide information related to the subjects discussed in this manual:

- *PayPass Personalization Data Specification*
- *MasterCard PayPass – Mag Stripe Issuer Implementation Requirements Guide*
- *M/Chip Qualified Test Tools*

## Business Process Diagram Conventions

The business process diagrams in this guide use the following symbols:



- A pool is used to contain activities within an organization.
- An activity can be atomic (is a task) or compound (contain multiple activities).
- An activity is started (or triggered) by a Start Event, a Time-based Trigger, or a sequence or message flow from another activity.
- Sequence flow lines (with solid lines and arrowheads) connect one activity to another, to a gateway or to an end event.
- Gateways signal a split in a process flow or a merger of multiple process flows.
- Message flow lines (with dashed lines and open arrowheads) connect activities across pools (usually via an artifact).
- A process contains activities interconnected by means of flow lines.



## 2 The CPV Process

This chapter provides an overview of the Card Personalization Validation for *PayPass* Mag Stripe process and a summary of its subprocesses

### Implementation

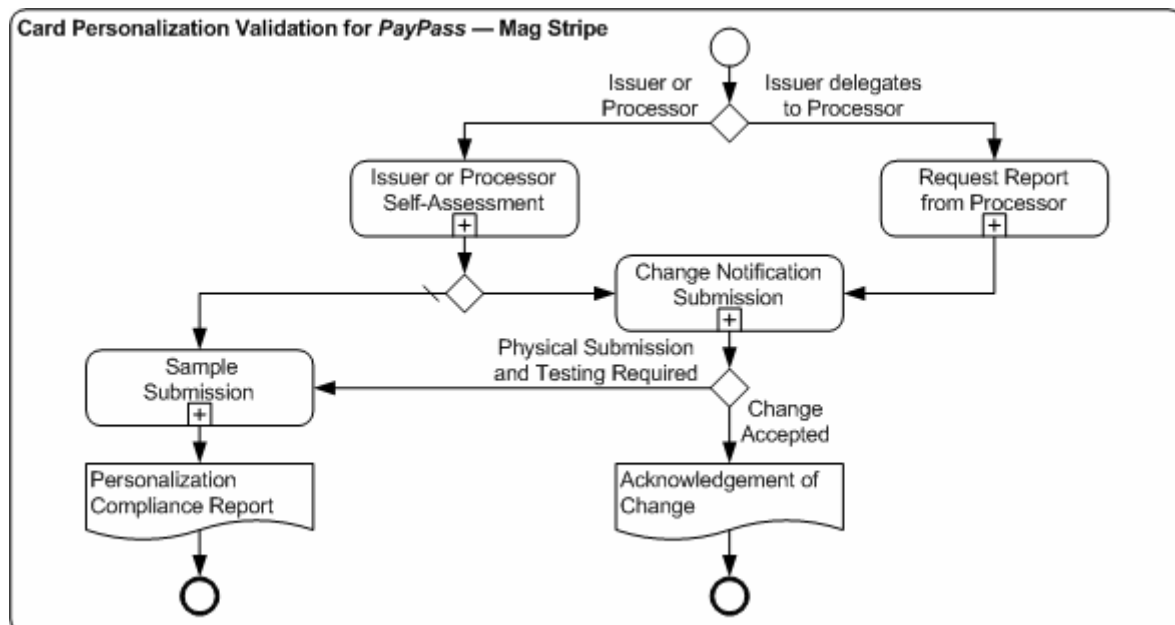
The CPV Process is a collaboration process involving the following entities:

- You, in the rôle of an Issuer or a Processor
- A CPV Service Provider
- MasterCard

### Overview

Figure 2.1 shows the process and the sequence flow between its subprocesses.

Figure 2.1—Card Personalization Validation (for *PayPass* – Mag Stripe) Process Flow



## For Issuers who Delegate to a Processor

For issuers who delegate to a processor, the Card Personalization Validation (CPV) process for *PayPass* – Mag Stripe products comprises two subprocesses:

- Request Report from Processor
- Change Notification Submission

### Request Report from Processor

In this subprocess you must obtain confirmation from the processor that they have successfully completed Card Personalization Validation. This confirmation should be a *PayPass Personalization Compliance Report* and any associated *PayPass – Mag Stripe Change Notification Forms* with its acknowledgement from MasterCard against the report.

This subprocess is detailed in chapter 3.

### Change Notification Submission

In this subprocess you provide a change list from an existing technical product and request an assessment from MasterCard to use the changed technical product.

This subprocess is detailed in chapter 6.

As you have delegated to a Processor, the normal outcome is that your change notification will be accepted.

## For Issuers and Processors

For an issuer or processor, the Card Personalization Validation (CPV) process for *PayPass* – Mag Stripe products comprises three subprocesses:

- Issuer or Processor Self-Assessment
- Sample Submission
- Change Notification Submission

### Issuer or Processor Self-Assessment

In this subprocess you evaluate the *PayPass* – Mag Stripe Technical Product that you want to issue and elect to either submit samples for testing (Sample Submission) or to submit a change notice for assessment (Change Notification Submission).

This subprocess is detailed in chapter 4.

After doing this subprocess, you do either of the following two subprocesses, based upon the results of your assessment.

### Sample Submission

In this subprocess you personalize a sample card, make a Card Image of it, then send both to a CPV Service Provider who test it for conformance with the appropriate personalization specifications. A *PayPass Personalization Compliance Report* is issued based on the CPV Testing that is performed.

This subprocess is detailed in chapter 5.

### Change Notification Submission

In this subprocess you provide a change list from an existing technical product and request an assessment from a CPV Service Provider to use the changed technical product.

This subprocess is detailed in chapter 6.

**NOTE:**

**As a result of the Change Notification Submission, you may still be required to do Sample Submission before the result of the Card Personalization Validation can be given.**



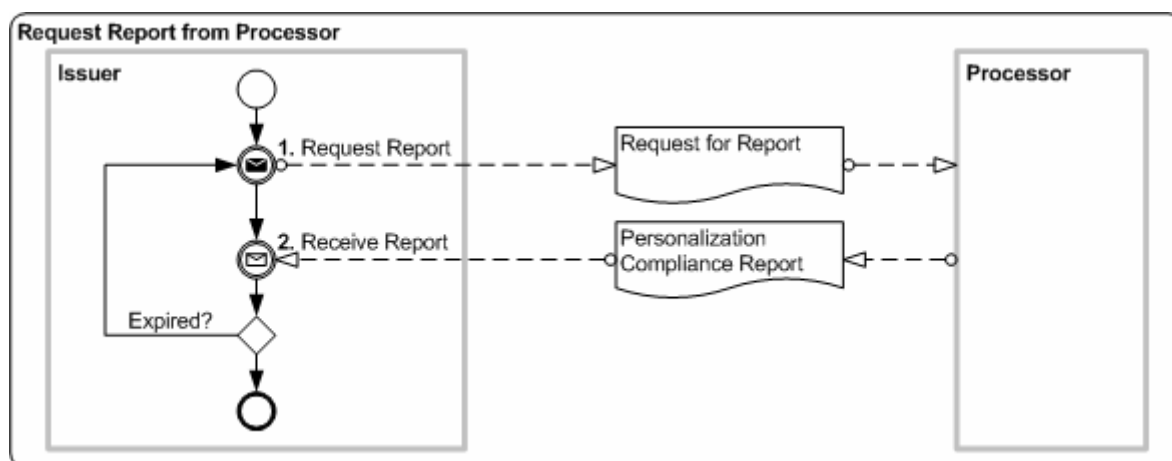
## 3 Request Report from Processor

This chapter details the subprocess where an issuer who has delegated to a processor requests confirmation from the processor to ensure that Card Personalization Validation has been done. This confirmation is the supply of an appropriate *PayPass Personalization Compliance Report* and any associated *PayPass – Mag Stripe Change Notification Forms* with its acknowledgement from MasterCard against the report.

### Overview

Figure 3.1 shows the request report from processor subprocess flow.

Figure 3.1—Request Report from Processor Subprocess Flow



### Process

1. Send a request to your processor to confirm that they successfully completed Card Personalization Validation for the Technical Products that they issue or plan to issue on your behalf.
2. Receive the confirmation, which should be a *PayPass Personalization Compliance Report* and any associated *PayPass – Mag Stripe Change Notification Forms* with its acknowledgement from MasterCard against the report.

Ensure that the report is still valid (because approval could be invalid due to changes such as those made to the *PayPass Personalization Data*

## Request Report from Processor Process

---

*Specification* under which the original validation was granted). If it is expired, go back to step 1 to request a valid report.

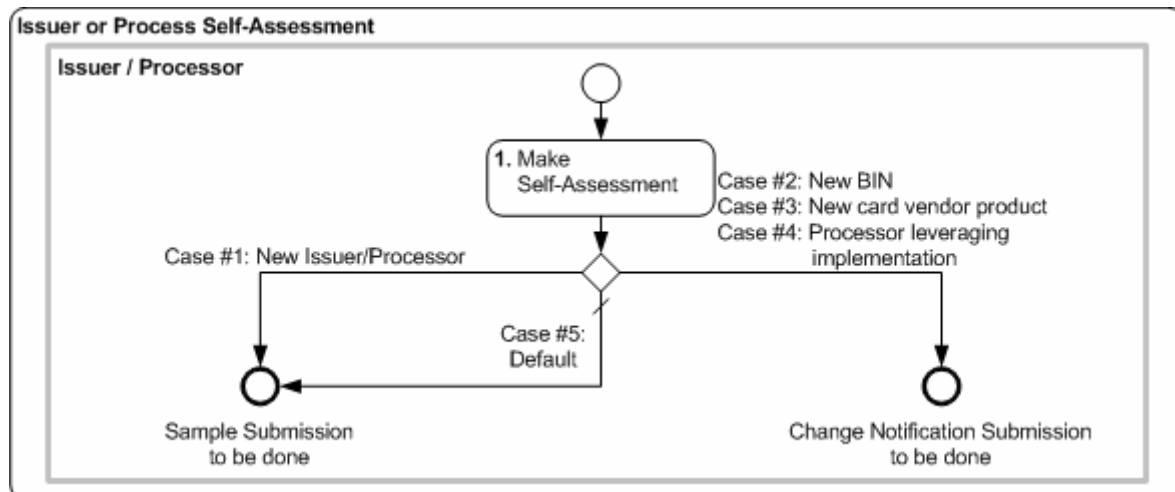
## 4 Issuer or Processor Self-Assessment

This chapter details the subprocess where you evaluate the *PayPass* – Mag Stripe Technical Product that you want to issue or amend and elect to either submit samples for testing or to submit a change notification for assessment.

### Overview

Figure 4.1 shows the assessment subprocess flow.

Figure 4.1—Issuer or Processor Self-Assessment Subprocess Flow



### Process

You must choose whether to do Sample Submission or Change Notification Submission. You need to evaluate the following choices, in the order they are presented, to determine what you need to do:

- If you are an issuer or processor who has not previously done Card Personalization Validation, you must elect to do Sample Submission.
- If you are creating a new Technical Product by changing the BIN of an existing approved Technical Product, and furthermore will not be changing any of the personalization parameters (except for cardholder related data and the expiration date), you must elect to do Change Notification Submission.

- If a new card vendor product is introduced to the existing deployment providing and the following three conditions are true:
  - a. the parameters are the same
  - b. the personalization process uses the MasterCard personalization command set defined for *PayPass* MagStripe as specified in *PayPass Personalization Data Specification*.
  - c. the card vendor product is type approvedthen you must elect to do Change Notification Submission.
- If you are a Processor then you can provide your implementation to other issuer programs provided that:
  - a. the personalization parameters (except for cardholder related data and the expiration date) are the same
  - b. can provide a valid compliance report for that productthen you must elect to do Change Notification Submission.
- In all other circumstances, you must elect to do Sample Submission.

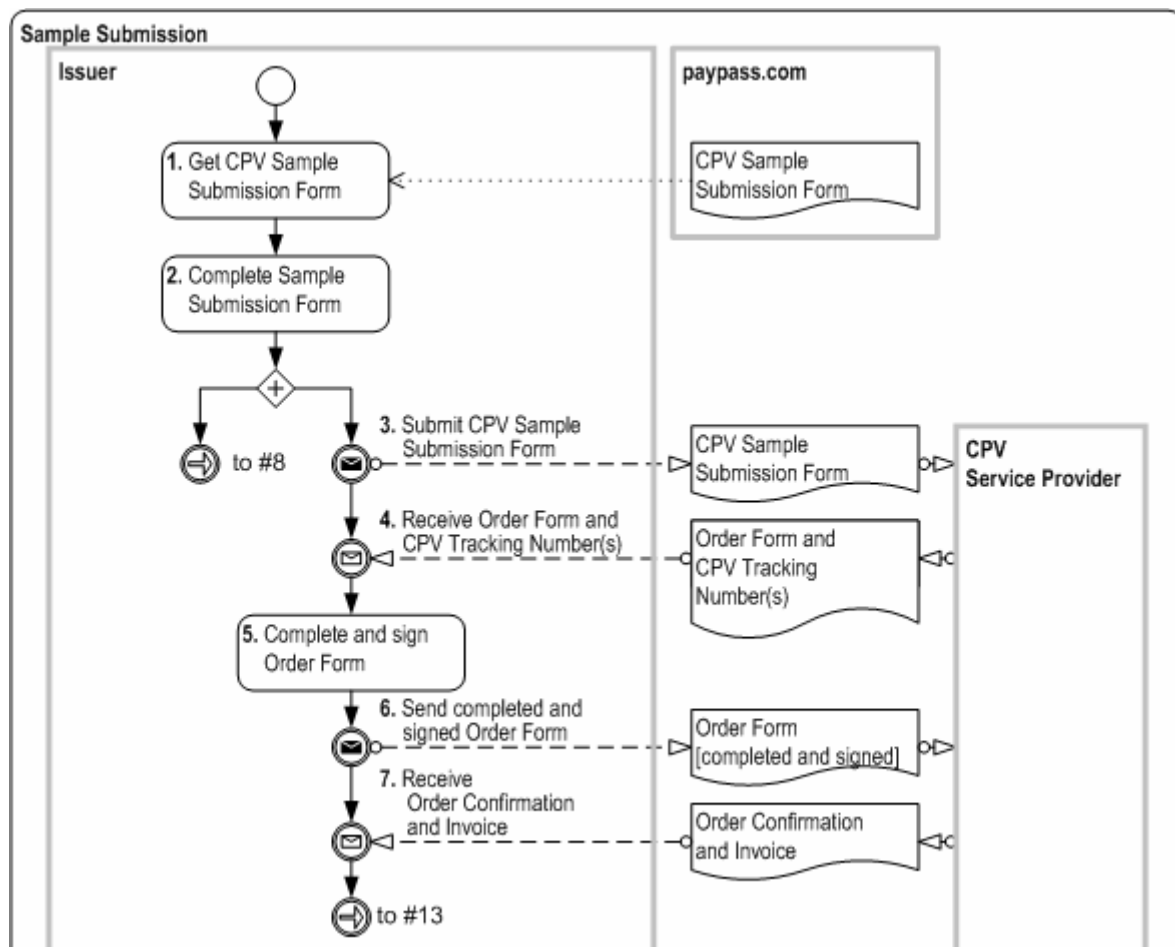
# 5 Sample Submission

This chapter details the subprocess where you personalize a Technical Product and generate a Card Image from it which you send to MasterCard who tests it for conformance with the appropriate personalization specifications. If successful you will also be requested to send the original Technical Product to MasterCard. You will receive a *PayPass Personalization Compliance Report* as a formal record of the result of the CPV Test, whether successful or not.

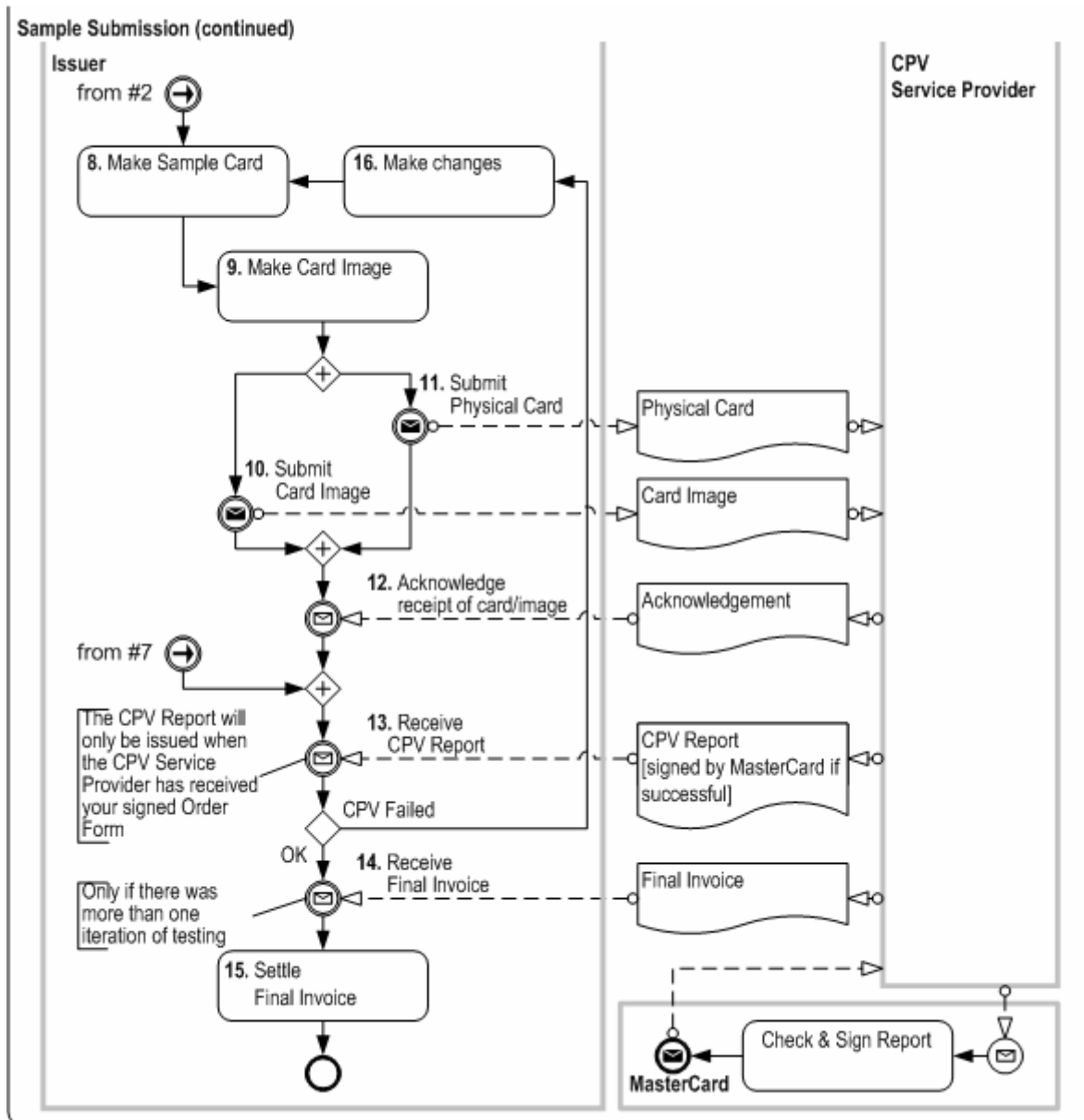
## Overview

Figure 5.1 shows the Sample Submission subprocess flow.

Figure 5.1—Sample Submission Subprocess Flow



## Sample Submission Process



## Process

1. Get the *PayPass – Mag Stripe CPV Sample Submission Form* which you can find via <http://www.paypass.com/documentation.html>.
2. Complete the *PayPass – Mag Stripe CPV Sample Submission Form*.

On this form you are asked to provide the test Issuer Master Key (IMK) to allow dynamic CVC3 testing to be performed. Refer to [Appendix A, Test Issuer Master Key Exchange](#), for information on how to exchange this information.

**Now start step #3 and step #8 in parallel with each other.**

3. Send the completed *PayPass – Mag Stripe CPV Sample Submission Form* by e-mail to [chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com).

**NOTE:**

**The originating e-mail address of this request for all future correspondence regarding this sample submission.**

4. You will receive an e-mail response that contains
  - an Order Form
  - the CPV Tracking Number, which is a number that you must quote on all further correspondence related to this instance of Card Personalization Validation for your Technical Product(s).
5. Complete and sign the Order Form.
6. Send the completed and signed Order Form to the CPV Service Provider as detailed on the form. A CPV Service Provider is used and you need to establish the Purchase Order to cover the provision of their testing services.

**NOTE:**

**CPV testing cannot take place until the CPV Service Provider has received and confirmed the necessary Purchase Order. Therefore, to avoid future delays, you must send the Purchase Order without delay.**

7. The CPV Service Provider will send you a confirmation of your purchase order and an accompanying invoice to cover one iteration of CPV Testing.

**Proceed to step #13.**

8. Have your personalization bureau personalize a sample of your selected Technical Product to the parameters that you specified in the *PayPass – Mag Stripe CPV Sample Submission Form*.
9. Generate a complete Card Image from the Technical Product.

The Card Image is created using either a Qualified CPV Test Tool (from one in the Validations Tools List in *M/Chip Qualified Test Tools*) or the MasterCard Card Image Extraction Tool (which is available on MasterCard OnLine). For more information on how to make a Card Image, refer to the documentation that accompanies the tool you are using.

The card image must also include data read from the magnetic stripe itself, if present, in addition to the magnetic stripe equivalent data read via a contact or contactless interface (as applicable).
10. Send the Card Image, along with an electronic copy of the *PayPass – Mag Stripe CPV Sample Submission Form* to [chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com).
11. Send the physical sample to the CPV Management address detailed in [CPV Contact Information](#).
12. When the Card Image and the physical sample are received by the CPV Service Provider you will receive an acknowledgement by e-mail of their receipt.

13. The CPV Service Provider will test the Card Image and Physical Sample and you will receive by e-mail a *PayPass Personalization Compliance Report*. This report will be in the form of a PDF document. For a successful CPV Test, the PDF document will be digitally signed by MasterCard.

**Note:**

**The report will not be issued until the CPV Service Provider has received your completed and signed Order Form from step #6.**

There are two possible outcomes of the CPV Testing:

---

**If the Personalization Then...  
Compliance Report  
indicates...**

---

Successful	Proceed to step #14
Failed	Continue to step #16 to make any necessary changes and being another iteration of CPV Testing

---

14. You will receive, from the CPV Service Provider, an invoice for any additional iterations.
15. Settle the invoice.

**This subprocess is now finished.**

16. Make the changes suggested in the report then go back to step #8.

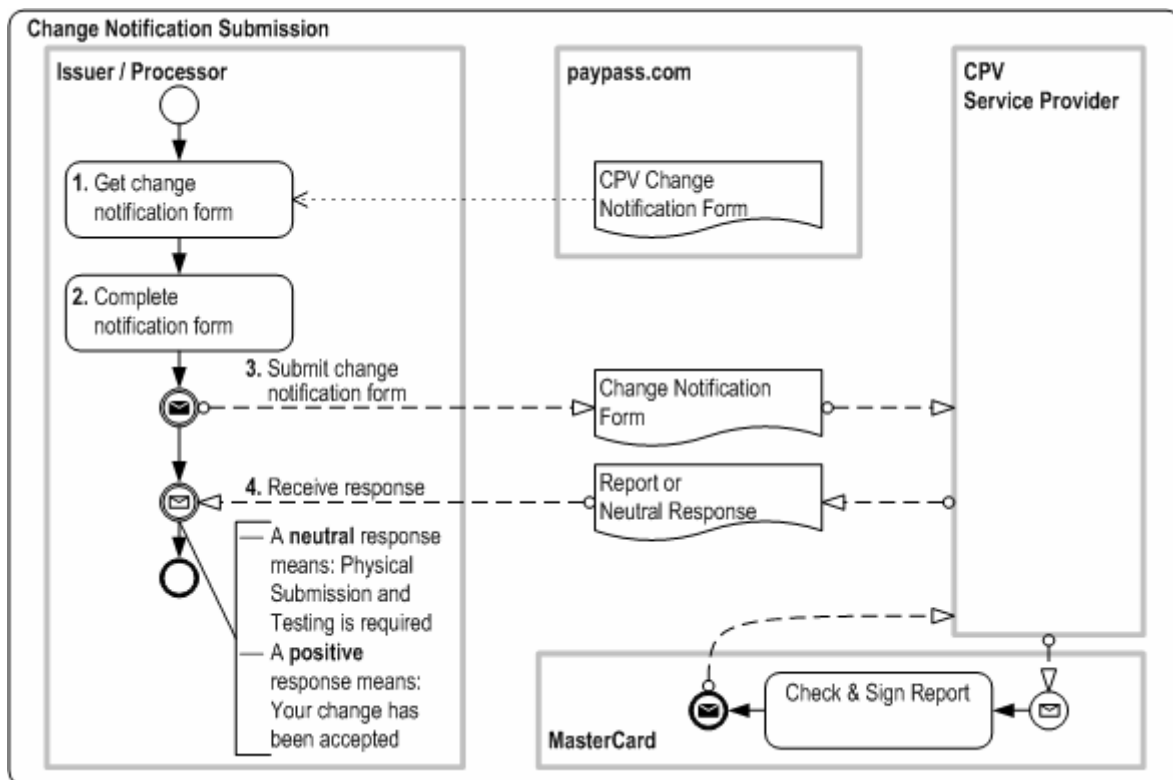
## 6 Change Notification Submission

This chapter details the subprocess where you provide MasterCard with a change list from an existing product and request an assessment from MasterCard to use the changed product.

### Overview

Figure 6.1 shows the Change Notification Submission flow.

Figure 6.1—Change Notification Submission Subprocess Flow



### Process

1. Get the *PayPass – Mag Stripe CPV Change Notification Form* which you can find at <http://www.paypass.com/documentation.html>.
2. Complete the information requested in the form.

3. Send the completed form by e-mail to [chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com).

**NOTE:**

**The originating e-mail address of this request is used for all future correspondence regarding this change notification submission.**

4. The CPV Team will assess your submission and send you a response by e-mail which will be either.
  - A positive assessment and you will be given a CPV Reference Number to uniquely refer to this Change Notification Submission for the Technical Product in any future correspondence.
  - A neutral assessment and you will be requested to do a Sample Submission to evaluate the changes that you propose before a definitive response can be provided.

# Appendix A Test Issuer Master Key Exchange

This appendix provides guidance on how you can exchange the TEST Issuer Master Key (IMK) that you use to personalize the sample cards that you use during the Card Personalization Validation process with the CPV Service Provider. There are four methods that you can use to exchange the IMK, and you need to use one of them.

This information is communicated to the CPV Team by completing the *PayPass – Mag Stripe CPV Sample Submission Form* information and sending it by email to [chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com).

If your own policies require it, you may encrypt files containing keys or key components before they are sent to CPV team. This may be done using PGP-compatible encryption software and the relevant PGP public key certificate (which is available on request by e-mail to [chip\\_personalization@mastercard.com](mailto:chip_personalization@mastercard.com)).

If you have a policy which prohibits sending this information by e-mail, then you may send it by secure post to the address detailed in [CPV Contact Information](#).

**NOTE:**

**Only TEST keys should be sent to CPV team. Issuers participating in the MasterCard on-behalf processing services that require the exchange of PRODUCTION keys must send these production keys using MasterCard standard OBKM (On-Behalf Key Management) procedures.**

## A.1 Method 1 — Clear Text Key

In this method, you provide the test Issuer Master Key as a clear text key. This is the preferred method.

To detect transmission errors, it is highly recommended that, if possible, you also provide the Key Check Value (KCV) corresponding to the test Issuer Master Key.

**NOTE:**

**The KCV corresponding to a 3DES key (or key component) is made of six hexadecimal characters representing the 24 leftmost bits from the result of 3DES encryption with that key (or that key component) of a 64-bit block filled with all binary zeroes.**

## A.2 Method 2 — Clear Text Key Components

In this method, you provide three clear text key components, which, when combined by means of exclusive-OR (XOR) operations, result in the test IMK clear text value.

This method should only be used when you are unable to use the Clear Text Key method (Method 1).

To detect transmission errors, it is highly recommended that, if possible, you also provide the Key Check Value (KCV) corresponding to each Clear Text Key component as well as a fourth KCV corresponding to the test Issuer Master Key.

## A.3 Method 3 — Encrypted Key Using a MasterCard-specified Key Encryption Key

In this method, you provide the test Issuer Master Key which has been encrypted using the MasterCard-specified Key Encryption Key (KEK) detailed below. The encryption algorithm to use is Triple DES in ECB (Electronic Code Book) mode. The Key Encryption Key is also known as the Zone Master Key (ZMK).

This method should only be used when you are unable to use either the Clear Text Key method (Method 1) or the Clear Text Key Components method (Method 2).

To detect transmission errors, it is highly recommended that, if possible, you also provide the Key Check Value (KCV) corresponding to the test Issuer Master Key.

MasterCard-specified KEK as a clear text key:

<b>Name</b>	<b>Value</b>
KEK clear text value	<b>C4C8 5152 B640 98A8 0B08 DA5E 64EF 15E9</b>
KEK KCV	<b>1D6A5D</b>

If your HSM (Hardware Security System) requires loading of a MasterCard-specified KEK as three clear text XOR components, you may use the following values<sup>1</sup>:

<b>Name</b>	<b>Value</b>
Component 1	<b>C4C8 5152 B640 98A8 0B08 DA5E 64EF 15E9</b>
Component 1 KCV	<b>1D6A5D</b>
Component 2	<b>1010 2323 3232 4545 5454 6767 7676 8989</b>
Component 2 KCV	<b>33F9CB</b>
Component 3	<b>1010 2323 3232 4545 5454 6767 7676 8989</b>
Component 3 KCV	<b>33F9CB</b>

## **A.4 Method 4 — Encrypted Key using Issuer-specified KEK**

In this method, you provide the test Issuer Master Key encrypted using your own KEK that must be a Triple DES double length key (128 bits, including parity bits). The encryption algorithm to use is Triple DES in ECB (Electronic Code Book) mode. You need to provide the KEK itself either as a Clear Text Key or as three Clear Text Key Components.

This method should only be used when you are unable to use the Clear Text Key method (Method 1), or the Clear Text Key Components method (Method 2), or the Encrypted Key Using a MasterCard-specified Key Encryption Key method (Method 3).

To detect transmission errors, it is highly recommended that, if possible, you also provide the Key Check Value (KCV) corresponding to the test Issuer Master Key, and to the KEK or KEK components.

---

<sup>1</sup> Using components 2 and 3 with identical values causes the first component to become the final key.