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
2200 MasterCard Boulevard
O’Fallon MO  63368-7263
USA

1-636-722-6100

www.mastercard.com
Chapter 3  Appropriate Approval Processes

3.1 Trusted Service Managers (TSMs) ................................................................. 3-1
   3.1.1 Purpose .................................................................................................. 3-1
   3.1.2 Requirement Level ................................................................. 3-1
   3.1.3 Procedure ....................................................................................... 3-1
   3.1.4 Contacts ........................................................................................ 3-1

3.2 User Interface Applications ............................................................................. 3-1
   3.2.1 Purpose .................................................................................................. 3-1
   3.2.2 Requirement Level ............................................................................. 3-2
   3.2.3 Procedure ........................................................................................ 3-2
   3.2.4 Contacts ........................................................................................ 3-2

3.3 Assembly Options .......................................................................................... 3-2
   3.3.1 Single Wire Protocol (SWP) Assemblies ............................................. 3-2
      3.3.1.1 SWP UICC Approval ................................................................. 3-2
      3.3.1.2 SWP Handset Approval .......................................................... 3-3
   3.3.2 Mobile Devices with Embedded Secure Elements ............................ 3-3
      3.3.2.1 Purpose ....................................................................................... 3-4
      3.3.2.2 Requirement Level ................................................................. 3-4
      3.3.2.3 Procedure ............................................................................. 3-4
      3.3.2.4 Contacts ................................................................................ 3-4
   3.3.3 Mobile MasterCard PayPass Tag Products ....................................... 3-5
      3.3.3.1 Purpose ....................................................................................... 3-5
      3.3.3.2 Requirement Level ................................................................. 3-5
      3.3.3.3 Procedure ............................................................................. 3-5
      3.3.3.4 Contacts ................................................................................ 3-5
   3.3.4 Removable Combined Contactless/Secure Element Solutions .......... 3-6
      3.3.4.1 Radio Frequency Identification (RFID) Solutions ......................... 3-6
      3.3.4.2 NFC Solutions ........................................................................ 3-7
Annex A  Process Guide Applicability Table

A.1 Purpose................................................................................................................................A-1

A.2 Table.....................................................................................................................................A-1
Using this Manual

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

Scope .........................................................................................................................................1
Audience ...................................................................................................................................1
Reader Guidance......................................................................................................................1
Abbreviations and Acronyms.................................................................................................2
Related Information..................................................................................................................3
Terminology .............................................................................................................................4
Revision History.......................................................................................................................7
Scope

This document describes all processes that must have been completed in order for any Mobile MasterCard PayPass implementation to be approved.

Audience

Due to the various different implementations of Mobile MasterCard PayPass, and the fact that depending on the architecture used, the market where it is being implemented, and the relationships between the parties involved in setting up an implementation, the intended audience of this document is broad and includes:

- Trusted Service Managers (TSMs)
- Secure Element Providers
- Processors
- Mobile Handset Manufacturers
- User Interface/Wallet Application Providers
- Mobile Network Operators

It is the responsibility of the Issuer to ensure that Mobile MasterCard PayPass is only issued to implementations that are fully approved—i.e. all components of that implementation have been tested and approved in combination.

Reader Guidance

This document describes at a high level the testing, approval and all related processes for all Mobile MasterCard PayPass implementations.

References are made throughout this document to other more specific guide documents that relate to the type of product, service or architecture.
# Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAST</td>
<td>Compliance Assessment and Security Testing</td>
</tr>
<tr>
<td>EP</td>
<td>Evaluation Plan</td>
</tr>
<tr>
<td>IC</td>
<td>Integrated Circuit</td>
</tr>
<tr>
<td>ICCN</td>
<td>Integrated Circuit Certificate Number</td>
</tr>
<tr>
<td>J2ME</td>
<td>Java 2 Platform, Micro Edition</td>
</tr>
<tr>
<td>LoA</td>
<td>Letter of Approval</td>
</tr>
<tr>
<td>MNO</td>
<td>Mobile Network Operator</td>
</tr>
<tr>
<td>MPCN</td>
<td>Mobile Payment Certificate Number</td>
</tr>
<tr>
<td>mPIN</td>
<td>mobile Personal Identification Number</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communications</td>
</tr>
<tr>
<td>OTA</td>
<td>Over The Air</td>
</tr>
<tr>
<td>RF</td>
<td>Radio Frequency</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identity Module</td>
</tr>
<tr>
<td>SWP</td>
<td>Single Wire Protocol</td>
</tr>
<tr>
<td>TSM</td>
<td>Trusted Service Manager</td>
</tr>
<tr>
<td>UI</td>
<td>User Interface</td>
</tr>
<tr>
<td>UICC</td>
<td>Universal Integrated Circuit Card</td>
</tr>
<tr>
<td>USIM</td>
<td>Universal Subscriber Identity Module</td>
</tr>
</tbody>
</table>
Related Information

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

Note MasterCard reserves the right to release new versions of documents referenced by this process. Partners should therefore check for the latest documentation versions and the impact of any amendments they contain before starting the partner testing process.

Note Document references are to generic PayPass documentation, which although not designed with mobile implementations in mind, will suffice for the development of early mobile implementations of PayPass. Any mobile specific documentation that is published in future will take precedence over generic PayPass documentation.

<table>
<thead>
<tr>
<th>Subject</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAST</td>
<td>Compliance Assessment and Security Testing Program</td>
</tr>
<tr>
<td>EMV</td>
<td>EMV Integrated Circuit Card Specifications for Payment Systems</td>
</tr>
<tr>
<td></td>
<td>Book 1 Application Independent ICC to Terminal Interface Requirements, Version 4.2</td>
</tr>
<tr>
<td></td>
<td>Book 2 Security and Key Management.</td>
</tr>
<tr>
<td></td>
<td>Book 3 Application Specification</td>
</tr>
<tr>
<td></td>
<td>Book 4 Cardholder, Attendant, and Acquirer Interface Requirements</td>
</tr>
<tr>
<td>EMV Contactless Protocol</td>
<td>EMV Contactless Communication Protocol Specification</td>
</tr>
<tr>
<td>MasterCard PayPass Branding</td>
<td>MasterCard PayPass Branding Standards</td>
</tr>
<tr>
<td>Standards</td>
<td></td>
</tr>
<tr>
<td>PayPass on Mobile Requirements</td>
<td>MobilCard PayPass – Requirements</td>
</tr>
<tr>
<td>Mobile MasterCard PayPass User</td>
<td>MobileCard PayPass User Interface Application – Requirements</td>
</tr>
<tr>
<td>Interface Application Requirements</td>
<td></td>
</tr>
<tr>
<td>Mobile MasterCard PayPass TSM</td>
<td>MobilCard PayPass TSM Service – Functional Requirements</td>
</tr>
<tr>
<td>Service Functional Requirements</td>
<td></td>
</tr>
</tbody>
</table>
## Terminology

This section explains a number of key terms and concepts used in this manual.

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assembly</td>
<td>A combination of components that, when brought together, can perform the basic function of making a contactless payment and can therefore be tested for functional compliance with Mobile MasterCard PayPass requirements. This does not include any OTA component. Typically this includes the mobile device, the Secure Element, the contactless processor, the contactless antenna and the necessary software to perform payment transactions.</td>
</tr>
<tr>
<td>CAST</td>
<td>The process that tests whether the chip, operating system and application(s) meet the security requirements as documented in [CAST].</td>
</tr>
<tr>
<td>Compliance Assessment and Security Testing Certification</td>
<td>Acknowledgement by MasterCard that the chip, operating system and application(s) meet the CAST requirements.</td>
</tr>
<tr>
<td>Compliance Certificate</td>
<td>The final formal confirmation from MasterCard to a TSM that the TSM’s solution under evaluation has successfully completed the entire approval process.</td>
</tr>
<tr>
<td>Component</td>
<td>Any product, part or combination of parts used in a Mobile MasterCard PayPass implementation (e.g. Mobile Device or payment application)</td>
</tr>
<tr>
<td>Formal Tests</td>
<td>Generic term used to refer to the set of testing sub-processes that have a defined start (sample requirements etc) and end point (test assessment, test report etc).</td>
</tr>
<tr>
<td>Letter of Approval (LoA)</td>
<td>Acknowledgement by MasterCard that a product or service demonstrated compliance to all relevant requirements.</td>
</tr>
<tr>
<td>Mobile Device</td>
<td>Any mobile phone, smartphone or handheld PDA or communications device.</td>
</tr>
<tr>
<td>Mobile Device Manufacturer</td>
<td>The manufacturer of the mobile device.</td>
</tr>
<tr>
<td>Mobile Partner Program</td>
<td>MasterCard’s Mobile Department within Innovative Platforms, runs a program for all companies that are involved in or wish to be involved in mobile payment initiatives including implementations of Mobile MasterCard PayPass, either at an issuer level or at a supplier level. The program is supported by a website (within MasterCard Online <a href="http://www.mastercard-mobilepartner.com">www.mastercard-mobilepartner.com</a>) which acts as a communication and reference tool for all registered partners.</td>
</tr>
</tbody>
</table>
## Terminology

<table>
<thead>
<tr>
<th>Term</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>On-device Personalization Application</td>
<td>Software that provides interaction between the PayPass application within the Secure Element and the mobile network for over-the-air personalization. It also enables downloading of the PayPass application over-the-air to the Secure Element. May be implemented in a number of ways, for example a Java MIDlet and is also referred to as a Trusted Service Agent (TSA).</td>
</tr>
<tr>
<td>OTA</td>
<td>Over-The-Air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile handset or any component within the mobile handset via the mobile network.</td>
</tr>
<tr>
<td>Over-the-air (OTA) personalization</td>
<td>Personalization (see definition below) carried out in such a way that the mobile handset Secure Element to be personalized is connected to the associated personalization data servers via a wide-area network, such as a mobile network or the Internet.</td>
</tr>
<tr>
<td>Payment Application</td>
<td>The software implemented within the secure memory domain of a Mobile MasterCard PayPass implementation (e.g. on the secure UICC card) covering the requirements of the PayPass or Mobile MasterCard PayPass Specification.</td>
</tr>
<tr>
<td>Payment Application Provider</td>
<td>A legal entity that has signed a PayPass Specification License Agreement, is entitled to use PayPass brands and supply PayPass applications and whose name will be stated on the MasterCard Mobile MasterCard PayPass Implementation -Letter of Approval.</td>
</tr>
<tr>
<td>Mobile MasterCard PayPass Testing and Approvals Process</td>
<td>Execution of a defined set of tests and evaluations on submitted product samples, or services claimed representative for that product or service, against requirements identified in [EMV Contactless Protocol], for PayPass–Mag Stripe in [PAYPASS MAG STRIPE], for PayPass–M/Chip in [PAYPASS M/CHIP] and for PayPass M/Chip Flex in [PAYPASS M/CHIP FLEX]. The process defined by this document.</td>
</tr>
<tr>
<td>Mobile MasterCard PayPass Evaluation Plan</td>
<td>Test plan defining which describes the actions required by the submitting entity or entities during the formal test process. It also shows the personalization profile requirements and number of samples to be submitted for formal testing.</td>
</tr>
<tr>
<td>SE Provider</td>
<td>A legal entity that provides any form of Secure Element for use in a Mobile MasterCard PayPass implementation, and whose name will be stated on the MasterCard PayPass Implementation -Letter of Approval.</td>
</tr>
<tr>
<td>Term</td>
<td>Meaning</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sub-component</td>
<td>Any constituent part of a component product or service used in a Mobile MasterCard PayPass implementation (such as a contactless antenna used in a contactless device such as a mobile phone).</td>
</tr>
<tr>
<td>Test Report</td>
<td>Summary of test results, issued by a Testing Laboratory as a result of Formal Testing.</td>
</tr>
<tr>
<td>Testing Laboratory</td>
<td>A facility accredited by MasterCard International to perform tests on PayPass and Mobile MasterCard PayPass components.</td>
</tr>
<tr>
<td>User Interface/Wallet</td>
<td>A legal entity that has signed a relevant PayPass License Agreement, is entitled to use PayPass brands and supply PayPass UI/Wallet applications and whose name will be stated on the MasterCard Mobile MasterCard PayPass Implementation - Letter of Approval.</td>
</tr>
<tr>
<td>Application Provider</td>
<td>An application that typically runs on the non-secure memory of a mobile device and facilitates user interaction with the Payment Application or Applications running within the Secure Element (features may include mPIN entry, transaction history review and OTA functionality).</td>
</tr>
</tbody>
</table>
Revision History

MasterCard periodically will issue revisions to this document as and when any enhancements, new developments, corrections or any other changes are required.

Each revision includes a summary of changes which is added to the revision history below, describing what has changed and how. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appear at the right of each revision marker.

MasterCard may publish revisions to this document in a MasterCard bulletin, another MasterCard publication, or on MasterCard OnLine, within the Mobile Partner Program section: www.mastercard-mobilepartner.com.

A subsequent revision is effective as of the date indicated in that publication or on MasterCard OnLine and replaces any previous edition.

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>History</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>Nov 08</td>
<td>Final version of formal testing and approvals processes for Mobile MasterCard PayPass implementations based on generic PayPass implementation specifications.</td>
<td>First formal process for mobile implementations of PayPass.</td>
</tr>
<tr>
<td>1.1</td>
<td>Jan 09</td>
<td>Updated terminology</td>
<td>No change to the process</td>
</tr>
<tr>
<td>2.0</td>
<td>Dec 09</td>
<td>New high-level version of guide to cover all product and service types as well as all known architecture variants</td>
<td>New stand-alone processes for TSM Approvals, UI Approvals, SWP UICC and SWP Handset Approvals as well as guidance on all other types of Assembly.</td>
</tr>
</tbody>
</table>
Introduction

This document gives a high level overview of the approval processes for all types of Mobile MasterCard PayPass implementation.

This document replaces the previous Mobile MasterCard PayPass Testing and Approval Guide which described a common process for all architecture types. This version refers to other process guide documents for the different architecture types or component parts of Mobile MasterCard PayPass implementations.

This chapter provides the reader with some background to the approach.

1.1 Background ..................................................................................................................... 1-1
1.2 Who Needs to Use this Process? .................................................................................. 1-1
1.3 When is this Process Used? ........................................................................................... 1-2
1.4 How is this Process Used? ............................................................................................ 1-2
1.1 Background

MasterCard has developed a comprehensive test and validation process for Mobile MasterCard PayPass implementations which is closely based on the existing PayPass Vendor Product Approval Process, Personalization Bureau Accreditation Process and Branding Approval Process for cards and devices. This enables world-wide interoperability as well as quality, reliability and security assurance at acceptable levels of time and cost.

This document gives a high level overview of all processes that must have been completed by product or service vendors in order for any implementation of Mobile MasterCard PayPass to be approved.

Completing this process allows all parties involved in the supply chain to demonstrate conformity to MasterCard’s security, PayPass, and Mobile MasterCard PayPass requirements. The official confirmation from MasterCard will come in the form of a Letter of Approval to the vendor of a specific service or product.

1.2 Who Needs to Use this Process?

Ultimately the issuer must ensure that all processes have been completed in order to issue Mobile MasterCard PayPass.

This document is designed for a broad audience as Mobile MasterCard PayPass implementations may vary greatly both in terms of architecture and also in terms of which entities are responsible for components or indeed entire implementations for testing and approval.

This document will guide each vendor through the process that applies to them based on the service or product they are providing and which architecture they plan to support. References will be made throughout this document to other more detailed process guide documentation.

Key audience members are therefore:

- Secure Element manufacturers (such as UICC card manufacturers)
- Payment Application developers
- Mobile Device manufacturers
- UI/Wallet Application developers
- Trusted Service Managers
- Mobile Network Operators

Issuers will also be given access to this document for reference if requested.
1.3 When is this Process Used?

- Whenever a new component product or service designed for use in Mobile MasterCard PayPass implementation is about to be issued or commercialized for the first time.
- Or a new Mobile MasterCard PayPass assembly is about to be issued or commercialized for the first time,
- Or if any changes are made to a product, service or assembly or if a Letter of Approval or Compliance Certificate is about to expire.

This may be a completely new set of components being combined in an assembly for the first time (in which case all testing can be carried out in one process), or it could simply involve the use of one (or more) new component(s) such as a new Mobile Device or a new Payment Application (in which case any previously published test results may—depending on circumstances—be re-used and combined with an overall evaluation of the assembly—through a Technical Assessment Review—thus saving time and costs in gaining the approval).

1.4 How is this Process Used?

The process relating to tests and evaluations is driven by the suppliers of components or services that they wish to provide for use in a Mobile MasterCard PayPass implementation.

The process relating to the choice of components for an assembly may be MNO or Issuer driven, but Issuers must always ensure that they only issue or deploy Mobile MasterCard PayPass if all components have been formally assessed for compliance and have the necessary approval(s).

It is the responsibility of the vendor (component or service provider) to initiate the actions required to achieve Approval and for their product or service to be made available for additional or delta testing if requested by an issuer or by MasterCard.

It is also the responsibility of the vendor to contact MasterCard to ascertain if their product requires CAST evaluation, and to organize this if required by MasterCard.

To manage the process, it is recommended that any vendor or group of vendors jointly appoint a project manager as the point of contact with MasterCard and Testing Laboratories.

The main contact for any questions related to this process is mobilepartner@mastercard.com.
2 Mobile MasterCard PayPass Component Approval Requirements

This chapter gives an overview of the different types of component products and services (and their sub-components) that typically make up implementations of Mobile MasterCard PayPass.

2.1 Summary of Component Products and Services

2.2 The User Interface Application

2.3 The Trusted Service Manager
   2.3.1 The TSM Datacentre
   2.3.2 The TSM On-device Personalization Application

2.4 The Assembly
   2.4.1 The Secure Element
      2.4.1.1 The IC
      2.4.1.2 The Operating System
      2.4.1.3 The Payment Application
   2.4.2 The Mobile Device
      2.4.2.1 The Contactless Module
2.1 Summary of Component Products and Services

The different types of component products and services (and their sub-components) that typically make up implementations of Mobile MasterCard PayPass are:

The User Interface Application

The Trusted Service Manager

- A TSM may also make use of a personalization application (also known as TSM agent or proxy application) that resides on the Mobile Device or Secure Element

The Assembly comprising

- The Secure Element comprising
  - The Integrated Circuit - IC (which must be certified as being secure and will therefore need to have a valid EMVCo Certificate and appropriate reference; ICCN).
  - The Operating System (which must also be certified as being secure on the specified IC, and which will therefore need to undergo the MasterCard Compliance Assessment and Security Testing (CAST) evaluation process covering the entire software layer on the given IC).
  - The Payment Application (which must also be certified as being secure on the specified Operating System and IC, and which will therefore need to be included in the MasterCard CAST evaluation process covering the software layer on the given IC).

- The Mobile Device

- The Contactless Module which performs both the digital and analog processing comprising
  - The contactless and analog signal processing component or module (this may be integrated with the Secure Element, or alternatively may take the form of a separate integrated circuit integrated into the Mobile Device depending on the architecture).
  - The Proximity Antenna (this may be integrated into the Mobile Device or alternatively may be integrated with a removable Secure Element which includes the Contactless Chip or Modem)

Figure 2.1 below shows a generic schematic of the various components that make up an implementation of Mobile MasterCard PayPass.
2.2 The User Interface Application

The User Interface Application or Wallet Application is an optional component and can be programmed in different formats depending on the device type and preference such as:

- J2ME
- Symbian
- Smart Card Webserver
- Native (to handset platform)
- And others

Although this is an optional component, almost all implementations will make use of such an application in one format or another, with functionality varying from basic
account default setting to more advanced mPIN entry, transaction history checking and online account management features.

The requirement for such applications to be reviewed and approved by MasterCard only applies to User Interface Applications that interface with the MasterCard Payment Application and/or that make use of any MasterCard brand identifiers.

Note User Interface Applications that do not interface with any MasterCard Payment Applications on Secure Elements and that do not make use of any MasterCard brand identifiers are exempt from any MasterCard approval requirements.

2.3 The Trusted Service Manager

The Trusted Service Manager (TSM) is the entity which enables the personalization and provisioning of payment applications and account credentials onto a mobile payment device. In many cases this will utilize an OTA mechanism.

The roles that a TSM typically performs may include:

- Personalization profile preparation (on behalf of issuers)
- Payment Application provisioning
- Payment Application personalization
- Secure Element or secure memory domain management (on behalf of issuers)
- Key management

Due to the nature of these roles and how they are implemented on mobile devices, a TSM solution often involves both a server side implementation in combination with a local mobile client – the On-device Personalization Application (also known as the TSM client or agent).

2.3.1 The TSM Datacentre

The TSM Datacentre and its purpose are typically concerned with functions such as the following:

- Receiving issuer data
- Preparation of issuer data for personalization
- Encryption of personalization data for provisioning
- Provisioning of payment applications to mobile devices
As these functions are very similar in nature to the functions being performed by a Personalization Bureau in the payment card environment, the following equivalent set of security requirements apply: [MasterCard Security Requirements for Mobile Payment Provisioning].

In order to ensure a TSM Service complies with these requirements, a process of accreditation has been set up that is based very much on the process of accreditation for Personalization Bureaus which involves both a logical and physical audit.

2.3.2 The TSM On-device Personalization Application

Many TSM solutions also make use of an On-Device Personalization Application (also referred to as TSM “Client” or “Agent”) which runs locally on the Mobile Device and enables the secure encrypted provisioning of payment applications and personalization from the server directly onto the Secure Element or secure memory domain.

Such an application is also subject to review depending on its scope and MasterCard may require a functional evaluation to be performed in order to ensure the solution is reliable and meets MasterCard’s usability requirements.

2.4 The Assembly

The Assembly is defined as being the “payment device” comprising all the necessary components that enable a contactless transaction to take place when the device is placed in the payment reader’s field. It is made up of several components, and depending on the architecture, can range from being a single integrated device, to a combination of separate component products which are developed and commercialized by multiple different vendors. The individual component parts (or component products, depending on the architecture), and their respective approval requirements are listed below.

2.4.1 The Secure Element

The Secure Element is the dedicated secure Integrated Circuit (IC), or secure memory domain within an IC, where the Payment Application and all payment related assets are stored, and where the payment transaction processing takes place.

2.4.1.1 The IC

In all contactless payment implementations the payment assets and Payment Application must be stored and processed on an integrated circuit or IC. MasterCard requires all such ICs to be secure and has developed a thorough evaluation process to ensure conformance with the security requirements as defined by CAST which has now been adopted by EMVCo as an industry-wide standardized approach.
Note An IC must have a valid EMVCo Certificate and accompanying reference number; ICCN.

2.4.1.2 The Operating System

In order for the Payment Application to function correctly, and in order to provide suitable logical security measures, vendors typically develop optimized Operating Systems for their Secure Elements which are installed on the IC.

Any such Operating System must also be assessed for its security compliance level. At the time of publication of this document no such process exists within EMVCo, so MasterCard’s own CAST process is applicable to Operating System reviews and certifications.

Note The Software on an IC (which is made up of the Operating System and the Payment Application together) must have a MasterCard CAST Certificate.

2.4.1.3 The Payment Application

In order to perform a payment transaction via a contactless interface a Payment Application is needed. There are two forms of MasterCard applications depending on the market in question:

- MasterCard PayPass - Mag Stripe
- MasterCard PayPass - M/Chip

There are a number of specifications for these applications depending on the required functionality and preferred configuration options. The latest specifications can be obtained from the Mobile Partner Program (www.mastercard-mobilepartner.com).

These applications are typically programmed in Java for Java Cards, but may take any other form so long as they comply with the Mobile MasterCard PayPass Technical Specifications and MasterCard Security Requirements.

These applications must therefore undergo the CAST evaluation in order to be certified as compliant with MasterCard’s security requirements, and must also be tested to ensure they comply with MasterCard’s functional requirements.
Note

A Payment Application running on an Operating System used on an IC must have a MasterCard CAST Certificate and is therefore subject to the same Software CAST Certification as the Operating System it runs on. In short; a Payment Application must be certified on every Operating System and IC that it runs on.

2.4.2 The Mobile Device

The role of the Mobile Device in Mobile MasterCard PayPass implementations can vary depending on the architecture.

For the most basic solutions, where no major contactless or payment related components are integral parts of the handset, most of the testing focuses on removable contactless payment device (such as a removable Secure Element integrated with a Contactless Module).

However due to the nature of Mobile Devices and contactless technology (both of which rely on RF transmissions), and the fact that contactless performance can vary depending on the sub-components that are in proximity of the antenna, additional interference testing is usually required to ensure reliability.

Mobile Devices with integrated payment and contactless components, such as Mobile Devices complete with integrated Secure Elements and Contactless Modules or SWP enabled NFC handsets which only contain an integrated Contactless Module and not the Secure Element, will need to undergo more thorough formal testing as either complete assemblies or component products respectively (see examples of products of this type below).

Figure 2.2—Examples of Mobile Devices with Integrated NFC technology
2.4.2.1 The Contactless Module

The Contactless Module enables the contactless communication between the Payment Application and the terminal. It will typically consist of two key components:

- An integrated circuit to perform the digital and analog signal processing
- An antenna that enables the RF communication with another antenna in a reader

Depending on the architecture, the contactless module may be an integral part of a Mobile Device in which case the necessary tests are carried out on the Mobile Device (as the device under test)—see Figure 2.2.

Alternatively the contactless module may be an integral part of a separate removable product or component that is not part of the Mobile Device but is attached to (see Figure 2.3), or inserted into, a suitable connection point or space within the handset (see Figure 2.4).

Figure 2.3—Example of Externally Attached Mobile MasterCard PayPass Tag

Note Please refer to section 3.3.3 for additional information about this specific product.
Figure 2.4—Example of UICC with Integrated Contactless Chip, Secure Element, and Flexible Antenna

Figure 2.5—Example of UICC connector with integrated Contactless Chip, Secure Element, and Flexible Antenna

Figure 2.6—Example of Stand-alone microSD with Integrated NFC Chip, Antenna and Secure Element
Regardless of the architecture, the contactless module will need to be assessed for its compliance with the specifications in [EMV Contactless Communication Protocol Specification].

Additional tests will also be applied to ensure that the device is compatible with all approved readers in the field and to ensure that there is no interference between the Contactless Module and other RF modules in a mobile device.

Mobile Devices that include NFC functionality will also require additional testing to be carried out in order to ascertain any effect on transaction performance.

Note More detailed descriptions of tests and guidelines on the tests that are applicable to specific architectures and types of implementation can be found in the guide documents and test description documents that are referenced in chapter 3, Appropriate Approval Processes.

Note A full list of applicable tests is always stated in the Evaluation Plan that is issued by MasterCard when a vendor makes a formal submission for approval of a product or service.
Appropriate Approval Processes

The Approval Process for specific components of Mobile MasterCard PayPass implementations will vary depending on the architecture. This chapter gives guidance on which specific processes (and accompanying guide documents) should be referenced for the different solutions.

3.1 Trusted Service Managers (TSMs) ......................................................... 3-1
   3.1.1 Purpose .............................................................. 3-1
   3.1.2 Requirement Level .............................................. 3-1
   3.1.3 Procedure ........................................................ 3-1
   3.1.4 Contacts ......................................................... 3-1

3.2 User Interface Applications ................................................................. 3-1
   3.2.1 Purpose .............................................................. 3-1
   3.2.2 Requirement Level .............................................. 3-2
   3.2.3 Procedure ........................................................ 3-2
   3.2.4 Contacts ......................................................... 3-2

3.3 Assembly Options ............................................................................. 3-2
   3.3.1 Single Wire Protocol (SWP) Assemblies .................. 3-2
      3.3.1.1 SWP UICC Approval .................................... 3-2
      3.3.1.2 SWP Handset Approval .............................. 3-3
   3.3.2 Mobile Devices with Embedded Secure Elements .... 3-3
      3.3.2.1 Purpose ..................................................... 3-4
      3.3.2.2 Requirement Level ...................................... 3-4
      3.3.2.3 Procedure .................................................. 3-4
      3.3.2.4 Contacts ................................................... 3-4
   3.3.3 Mobile MasterCard PayPass Tag Products .............. 3-5
      3.3.3.1 Purpose ..................................................... 3-5
      3.3.3.2 Requirement Level ...................................... 3-5
      3.3.3.3 Procedure .................................................. 3-5
      3.3.3.4 Contacts ................................................... 3-5
   3.3.4 Removable Combined Contactless/Secure Element Solutions ...... 3-6
      3.3.4.1 Radio Frequency Identification (RFID) Solutions .................. 3-6
      3.3.4.2 NFC Solutions ............................................ 3-7
3.1 Trusted Service Managers (TSMs)

3.1.1 Purpose

MasterCard has developed a stand-alone Approval Process for TSMs in the context of Mobile MasterCard PayPass implementations.

Please refer to [Mobile MasterCard PayPass TSM Approval Guide] for information on the process.

3.1.2 Requirement Level

The process is mandatory for all TSMs that are providing a hosted service for MasterCard issuing banks.

3.1.3 Procedure


3.1.4 Contacts

The MasterCard contact for queries regarding the TSM Approval Process is:

mobilepartner@mastercard.com

Note

For TSM solutions that utilize a User Interface or Wallet Application for the Personalization Process as well as typical UI functionality, the UI/Wallet Approval Guide referred to below will also apply.

3.2 User Interface Applications

3.2.1 Purpose

MasterCard has developed a stand-alone Approval Process for User Interface Applications in the context of Mobile MasterCard PayPass implementations.

Please refer to [Mobile MasterCard PayPass UI/Wallet Approval Guide] for information on the process.
3.2.2 Requirement Level

The process is mandatory for all UI/Wallet Applications that interact with MasterCard Payment Applications and/or that carry any MasterCard brand identifiers.

3.2.3 Procedure


3.2.4 Contacts

The MasterCard contact for queries regarding the UI/Wallet Approval Process is:

mobilepartner@mastercard.com

3.3 Assembly Options

3.3.1 Single Wire Protocol (SWP) Assemblies

SWP Assemblies are made up of two components that can be approved as stand-alone products:

- SWP Universal Integrated Circuit Card (UICC) (including Payment Application)
- SWP enabled Near Field Communications (NFC) Handset

Both of these products have their own approval process as detailed below.

3.3.1.1 SWP UICC Approval

Purpose

MasterCard has developed a stand-alone Approval Process for SWP enabled UICC card products including Payment Application (in the context of Mobile MasterCard PayPass implementations).

Please refer to [Mobile MasterCard PayPass SWP UICC Approval Guide] for information on the process.

Requirement Level

The process is mandatory for all SWP UICC and Payment Application combinations that are to be used in the context of Mobile MasterCard PayPass implementations.
Procedure


Contacts

The MasterCard contact for queries regarding the Mobile MasterCard PayPass SWP UICC Approval Process is:

mobilepartner@mastercard.com

### 3.3.1.2 SWP Handset Approval

**Purpose**

MasterCard has developed a stand-alone Approval Process for SWP enabled NFC handsets (or mobile devices), in the context of Mobile MasterCard PayPass implementations.

Please refer to [Mobile MasterCard PayPass SWP Handset Approval Guide] for information on the process.

**Requirement Level**

The process is mandatory for all SWP enabled NFC handsets that are to be used in the context of Mobile MasterCard PayPass implementations.

**Procedure**


**Contacts**

The MasterCard contact for queries regarding the Mobile MasterCard PayPass SWP Handset Approval Process is:

mobilepartner@mastercard.com

### 3.3.2 Mobile Devices with Embedded Secure Elements

Mobile devices with embedded Secure Elements are evaluated in the same way as card products or other sealed system payment devices.
Note: It is important to note however that every Payment Application running on a particular NFC enabled mobile device will need to be evaluated on that platform and each evaluation of a complete Assembly of this type will result in a separate Letter of Approval. The smallest common denominator in approvals of this type of product is always the Payment Application.

3.3.2.1 Purpose

MasterCard has developed a stand-alone Approval Process for NFC enabled mobile devices with embedded Secure Elements, which is based very closely on the existing approval process for card products.

Please refer to [PayPass Vendor Product Approval Process Guide (Cards and Devices)] for information on the process.

Note: Due to the differences between mobile devices and payment devices that are only designed with payment functionality in mind (such as traditional ID-1 PayPass enabled card products) there will be some additional testing required beyond the tests that are typically required for products such as ID-1 PayPass cards. All applicable tests are always specified to the vendor in a formal document by MasterCard called the Evaluation Plan. The list of applicable tests is always based on the information gathered during the registration process.

3.3.2.2 Requirement Level

The process is mandatory for all NFC enabled Mobile Devices that are to be used in implementations of Mobile MasterCard PayPass.

3.3.2.3 Procedure


3.3.2.4 Contacts

The initial MasterCard contact for queries regarding the Approval Process for NFC enabled Mobile Devices with embedded Secure Elements is:

mobilepartner@mastercard.com
3.3.3 Mobile MasterCard PayPass Tag Products

As Mobile MasterCard PayPass Tag products are in effect no more than cut-down versions of ID-1 PayPass card products, they will follow the same approval process, and therefore the same process guide document applies.

However as Mobile MasterCard PayPass Tag devices are designed primarily for use on mobile devices they must also undergo certain testing in combination with a selection of common mobile devices (each of which is chosen based on its physical and Radio Frequency (RF) characteristics).

This testing is designed to ascertain the extent to which the Tag affects the RF performance of the mobile device and also to which extent the mobile device affects the Analog performance of the Tag.

3.3.3.1 Purpose

MasterCard has developed a stand-alone Approval Process for Mobile MasterCard PayPass Tag products, which is based very closely on the existing approval process for standard ID-1 format card products.

Please refer to [PayPass Vendor Product Approval Process Guide (Cards and Devices)] for information on the process.

**Note**

Please note that additional interference testing (between the Tag product and a selection of mobile devices) is required for all Mobile MasterCard PayPass Tag products. These additional tests will be specified in the Evaluation Plan.

3.3.3.2 Requirement Level

The process is mandatory for Mobile MasterCard PayPass Tag products.

3.3.3.3 Procedure


3.3.3.4 Contacts

The initial MasterCard contact for queries regarding the Approval Process for Mobile MasterCard PayPass Tag devices is:

testing_card@mastercard.com
### 3.3.4 Removable Combined Contactless/Secure Element Solutions

#### 3.3.4.1 Radio Frequency Identification (RFID) Solutions

Solutions which can draw the power they need to perform a transaction from the field of a contactless payment reader can be tested as stand-alone products with additional testing on specific mobile devices to ascertain impact of mobile device on performance.

Certain tests may therefore be carried out once during the stand-alone testing while others will need to be repeated on the selected devices.

**Purpose**

MasterCard applies a stand-alone Approval Process for removable RFID solutions and mobile devices, which is based very closely on the existing approval process for card products.

Please refer to [PayPass Vendor Product Approval Process Guide (Cards and Devices)] for information on the process.

**Note**

Please note that the scope and approach to testing will vary depending on the type of architecture. Testing will typically involve relevant mobile devices. Information gathered during the registration process will determine which tests will be applied and how. All tests will be specified in the Evaluation Plan.

**Requirement Level**

The process is mandatory for all RFID solutions design for use in Mobile Devices.

**Procedure**


**Contacts**

The initial MasterCard contact for queries regarding the Approval Process for NFC enabled Mobile Devices with embedded Secure Elements is:

mobilepartner@mastercard.com
3.3.4.2 NFC Solutions

Solutions which require a mobile device to either provide the power needed for the product to operate or for some other functional purpose (such as a user interface to enable payment transactions to take place) will need to be tested on the mobile devices for which they have been designed.

Depending on the architecture this will have a varying impact on which tests can be carried out once and which ones will need to be repeated on the various mobile devices.

**Purpose**

MasterCard applies a stand-alone Approval Process for removable NFC solutions and mobile devices, which is based very closely on the existing approval process for card products.

Please refer to [PayPass Vendor Product Approval Process Guide (Cards and Devices)] for information on the process.

**Note**

Please note that the scope and approach to testing will vary depending on the type of architecture. Testing will typically involve relevant mobile devices. Information gathered during the registration process will determine which tests will be applied and how. All tests will be specified in the Evaluation Plan.

**Requirement Level**

The process is mandatory for all removable NFC solutions designed for use in Mobile Devices.

**Procedure**


**Contacts**

The initial MasterCard contact for queries regarding the Approval Process for removable NFC solutions for use in Mobile Devices is:

mobilepartner@mastercard.com
### Process Guide Applicability Table

*This is Annex A of the Mobile MasterCard PayPass Testing & Approval Guide.*

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.1 Purpose</td>
<td>A-1</td>
</tr>
<tr>
<td>A.2 Table</td>
<td>A-1</td>
</tr>
</tbody>
</table>
A.1 Purpose

The purpose of this table is to give the reader a quick reference guide as to which document is the most relevant for their type of product or service and whom to contact, and which documents to check in order to achieve the required approval.

A.2 Table

The Following is the Process Guide Applicability Table:

<table>
<thead>
<tr>
<th>Product/Service</th>
<th>Relevant Guide Document</th>
<th>Available from</th>
</tr>
</thead>
<tbody>
<tr>
<td>TSM</td>
<td>Mobile MasterCard PayPass TSM Approval Guide</td>
<td><a href="http://www.mastercard-mobilepartner.com">www.mastercard-mobilepartner.com</a></td>
</tr>
</tbody>
</table>
### Process Guide Applicability Table

<table>
<thead>
<tr>
<th>Product/Service</th>
<th>Relevant Guide Document</th>
<th>Available from</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID000-format dual interface card, with connection to antenna in mobile device (typically C4C8)</td>
<td>PayPass Vendor Product Approval Process Guide (Cards and Devices)</td>
<td><a href="http://www.PayPass.com">www.PayPass.com</a></td>
</tr>
<tr>
<td>Other architectures</td>
<td>Although other solutions may not have been considered yet, the most applicable guide document is: PayPass Vendor Product Approval Process Guide (Cards and Devices)</td>
<td><a href="http://www.PayPass.com">www.PayPass.com</a></td>
</tr>
</tbody>
</table>