Mobile MasterCard PayPass TSM Approval Guide

Dec 2014 - Version 2.0

Proprietary Rights

Trademarks

MasterCard
Global Digital Technology Center
The Gateway East
152 Beach Road #35-00 S(189721)
Singapore
www.mastercard.com

1 Using this Manual

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

1.1 Scope

This document describes all the processes that must be completed in order for any Trusted Service Manager (TSM), and any specific services they provide for use in issuing Mobile MasterCard *PayPass* implementations, to be fully approved for commercial deployment with MasterCard issuing banks. For the avoidance of doubt the generic term Mobile MasterCard *PayPass* is used throughout this document to describe all variants of *PayPass* implementations on mobile devices or involving mobile devices as a carrier device for the payment device.

1.2 Audience

The primary audience for this document is organizations that function as the Trusted Service Manager for a Mobile MasterCard *PayPass* implementation. However, there are additional entities that play a role in successful implementation of Mobile MasterCard *PayPass* capability that may also find this document useful to understand who the individual stake holders are, the roles that they fulfill and the procedures MasterCard has implemented to ensure the overall implementation functions as expected...

These include:

- Mobile Network Operators
- Mobile Handset Manufacturers
- Component Vendors (who provide NFC components to handset manufacturers)
- SIM card manufacturers (who would be manufacturing SIM cards for use in the handsets)
- Payment Application Developers
- User Interface Application Developers
- Issuers

Issuers that offer *PayPass* transaction capability via a mobile device to their account holders must ensure that all components utilized for the Mobile

PayPass implementation are fully approved and compliant with MasterCard requirements.

It is generally expected that TSMs will ensure this on behalf of the banks that they provide their services to.

It is also expected that TSMs will initiate the Approval of their solution themselves.

1.3 Reader Guidance

This document describes the evaluations and associated administrative processes that apply for TSMs and their solutions if they are to be used in implementations of Mobile MasterCard *PayPass*.

1.4 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

Acronym	Meaning
HSM	Hardware Security Module
GVCP	Global Vendor Certification Program
MNO	Mobile Network Operator
OTA	Over The Air
SE	Secure Element
SCMS	Smart Card Management System
SIM	Subscriber Identity Module
TSM	Trusted Service Manager
UI	User Interface
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

1.5 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.

Title	Description
Security Requirements for Mobile Payment Provisioning – July 07	Security Requirements for Mobile Payment Provisioning
Mobile MasterCard *PayPass* TSM Functional Requirements v2-0	Functional requirements for all TSM solutions

1.6 Terminology

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

Term	Meaning
Approval	The umbrella term for all testing and/or evaluation and/or review processes and outputs thereof relating to products or services or components thereof that are used in implementations of Mobile MasterCard *PayPass*.
Assessment Summary	Acknowledgement by MasterCard that specified components of the submitted product or service were compliant with the corresponding requirements at the time of testing; this does not constitute a full Approval, it is merely an interim step and may be used as input to the Approval Review.
Audit	Any formal inspection or examination of a system, process, or functional entity, carried out by an auditor, using a defined set of criteria.
Auditors	A security specialist accredited by MasterCard to evaluate TSM compliance with physical and logical security requirements defined by the Global Vendor Certification Program (GVCP) in [Security Requirements for Mobile Payment Provisioning].
Bureau	In relation to these requirements, the term 'bureau' is used to refer to an organization that personalizes plastic cards, but which can provide additional services as appropriate for mobile provisioning.
Compliance Certificate	The final formal confirmation from MasterCard to a TSM that the TSM's solution under evaluation has successfully completed the entire approval process.
Certification	The generic term for the outcome of the process of evaluating a TSM and confirming its compliance with all relevant MasterCard requirements.
Component	Any product, part or combination of parts used in a Mobile MasterCard *PayPass* implementation (e.g. Mobile Device or payment application)

Term	Meaning
Evaluation	Generic term used to refer to the set of testing processes that have a defined start (request for supporting documents etc) and end point (evaluation assessment, report etc).
Evaluation Plan	Test plan which describes the scope of evaluations and actions required by the submitting entity or entities during the formal test process. It also describes requirements for submission of supporting documents that are needed during evaluation and the demo scenarios that will be assessed.
Evaluation Report	Document summarizing the results of a formal Evaluation
Facility	The physical premises at which the TSM operates its business.
Global Vendor Certification Program	A MasterCard program covering assessment of the physical security of a manufacturing site and logical security of production data network environment, hardware, and software. This program is used to maintain and improve your security infrastructure and to prevent attacks to MasterCard products, components, and related network and company image.
Handset	A type of mobile device, specifically a mobile phone handset.
Issuer	A financial institution that is licensed to issue MasterCard payment solutions (such as cards or *PayPass* devices)
Mobile Device	A portable electronic device with contactless and wide area communication capabilities. Mobile devices include mobile phones and other consumer electronic devices such as suitably equipped Personal Digital Assistant (PDA)
Mobile MasterCard *PayPass* Testing and Approval Process	The collective term for all tests and evaluations that must be completed by vendors of any component used in Mobile MasterCard *PayPass* implementations.

Term	Meaning
Mobile Partner Program	The Mobile department within MasterCard Worldwide runs a program for all companies that are involved in, or wish to be involved in, any mobile payment related initiative (including, but not limited to, Mobile MasterCard *PayPass*), either at an issuer level or at a supplier level. The program is supported by a website (within MasterCard Online: www.mastercard-mobilepartner.com) which acts as a communication tool and resource centre for all partners.
Mobile Provisioning	The provisioning of applications to a Mobile Device by means of a wireless connection. In the context of TSMs this term is typically used to describe the provisioning of Payment Applications to a Mobile Device, which may also include the provisioning of On-Device Personalization Applications to facilitate the personalization of such Payment Applications.
On-device Personalization Application	A software program that runs in a Mobile Device to provide interaction between the *PayPass* application within the Secure Element and the mobile network for over-the-air personalization. It also enables download of the *PayPass* application over-the-air to the Secure Element.
OTA	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.
OTA Personalization	Personalization (see definition below) of a Payment Application on a Secure Element within a Mobile Payment Device using a wireless data transfer such as the mobile network.
OTA Provisioning	The transfer of Payment Applications Over The Air onto a Secure Element on a Mobile Payment Device.
Payment Application	Generic term for any application which runs in a secure environment on a payment device (such as an ID-1 card or a Secure UICC) and which facilitates the payment transaction taking place with a payment terminal.

Term	Meaning
Payment Application Provider	A legal entity that has signed the applicable license agreements entitling it to obtain technical specifications against which a Payment Application can be developed and which also entitle it to apply for formal approval and commercialize such a Payment Application.
Payment Device	Any device that (once personalized) is capable of executing a payment transaction.
Personalization	Installation of cardholder-specific data into the Secure Element of a Payment Device. May take place Over The Air, via the contactless interface or via a contact interface during or after production.
Personalization Bureau	A facility responsible for writing payment system, issuer, and account holder specific data to a payment card or alternate form factor. This facility is acting on behalf of a licensed issuer and is authorized by MasterCard to perform this activity for MasterCard branded products...
Provisioning	Installation of a Payment Application into the Secure Element on or in a Mobile Device
Provisioning data	The set of issuer- and subscriber-specific data needed to personalize a Payment Device. In the context of mobile payments, this may include application keys, application configuration parameters, and other provisioning data.
Secure Element	A secure, tamper-resistant, storage and execution environment holding payment applications and payment assets such as keys.
Secure Element Issuer	A legal entity that provides any form of Secure Element for use in a Mobile MasterCard *PayPass* implementation.
Security Accreditation	Formal acknowledgement by MasterCard that a TSM and its specified solution for use in Mobile MasterCard *PayPass* implementations and all of its components demonstrated compliance to MasterCard's Security Requirements.
Subscriber	The person to whom a mobile payment device is issued and subsequently personalized, and who possesses and uses that device as the registered user.

Term	Meaning
Trusted Service Manager	An entity that provisions, personalizes or manages Payment Applications on Mobile Devices on behalf of MasterCard issuers. A TSM may perform any or all of these roles including the data preparation, data management, and key management functions.
TSM Certification	The generic term for the outcome of the process of evaluating a TSM and confirming its compliance with all relevant MasterCard requirements.
TSM Platform	An application suite that typically comprises of functional modules including payment application personalization & lifecycle management, SE lifecycle management, SE security key management, inter-system messaging communication & notification, NFC service eligibility control, remote administration management and monitoring & reporting services.
TSM Supplier	An entity that supplies the TSM platform to the TSM Vendor. A TSM supplier and TSM vendor can be the same entity.
TSM System	An application server which is configured from a TSM Platform to operate TSM roles in an NFC ecosystem. It connects to one or more external entities within the same ecosystem for inter-TSM messaging and notification purposes. There can be more than 1 TSM system in a TSM vendor's facility.
TSM Vendor	An entity that owned the facility where the TSM system is hosted. A TSM vendor is responsible for all matters pertaining to TSM approval process.

1.7 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 the Mobile Partner Program website and replaces any previous edition.

Version	Date	History	Impact
1.0	Nov 09	First complete version	
2.0	Dec 14	Second complete version	Updated TSM Approval Guide incorporating clarifications regarding process and applicability of processes.

2 Introduction

This chapter provides the reader with an overview of the Evaluation and Accreditation Processes for Trusted Service Managers (TSM) who wishes to commercialize solutions to be used when implementing Mobile MasterCard *PayPass*.

2.1 Background

MasterCard has developed a comprehensive test and validation process for all products and services (components) of Mobile MasterCard *PayPass* implementations. The process is closely based on the existing validation processes for *PayPass* card devices and other vendors involved in the supply chain (such as Personalization Bureaus). This enables world-wide interoperability as well as quality, security and reliability assurance at acceptable levels of time and cost.

This document describes all processes that must be completed in order for any TSM to be approved for support of a Mobile MasterCard *PayPass* program.

Completing this process allows the parties involved in the personalization, mobile provisioning and where applicable other life-cycle management parts of the supply chain to demonstrate conformity to:

- [*Mobile MasterCard PayPass TSM Functional Requirements*]
- [*Security Requirements for Mobile Payment Provisioning*]

A TSM that successfully completes all of the applicable tests and evaluations will receive a formal Compliance Certificate from MasterCard.

The TSM Approved List is published on a monthly basis on the Mobile Partner Program web site [www.mastercard-mobilepartner.com].

2.2 Who needs to Use this Process?

Issuers have an obligation to ensure that all components of a Mobile MasterCard *PayPass* implementation (including the TSM), have been fully evaluated and are approved. In most cases it is likely that issuers will rely on TSMs to correctly manage the provisioning and personalization process so that personalization requests where at least one component is not approved are refused.

This document is designed primarily for TSMs, but is also relevant to a broader audience (including Mobile Network Operators (MNOs), Application Developers, Secure Element Issuers, Mobile Handset Manufacturers and Issuers), as these other members of the Mobile MasterCard *PayPass* value chain will need to be aware of the role performed by the TSM, its purpose and the importance thereof.

This document will guide the TSM through the process by defining formal sub-processes and each step that they will need to follow.

2.3 When is this Process Used?

This process is used:

- When a new TSM wishes to provide OTA provisioning services for MasterCard issuers
- Annually on the anniversary of the initial Certification
- If any changes are made to an existing approved TSM.

Examples of changes to existing approved TSMs include:

- Changes to the logical architecture of the TSM solution.
- Changes to the physical site of an approved TSM's facilities.
- New project implementation
- New integration
- New additional geographical TSM sites.

2.4 How is this Process Used?

This process describes the key activities which must be successfully completed in order for a TSM to become a MasterCard certified TSM.

To manage the process, it is recommended that the submitting entity appoints a project manager as the point of contact with MasterCard and the Laboratories and/or Auditors.

It is the responsibility of the TSM to initiate the actions required to achieve Certification or renewal of an existing Certification.

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

Compliance certificates will be issued to the TSM or submitting entity upon successful completion of the process by MasterCard.

The main contact for any questions related to this process is mobilepartner@mastercard.com

2.5 Licensing Requirement

Vendors wishing to receive Mobile MasterCard *PayPass* specifications and ultimately support a TSM system for approval must sign the appropriate MasterCard *PayPass* License Agreement.

Vendors managing an on-behalf service for Secure Element Issuers to load, install, extradite and delete the Mobile MasterCard PayPass application must sign the appropriate MasterCard *PayPass* License Agreement.

Vendors who do not yet have a relevant license agreement in place should contact the Mobile Partner Program by email:

mobilepartner@mastercard.com

3 Certification Process

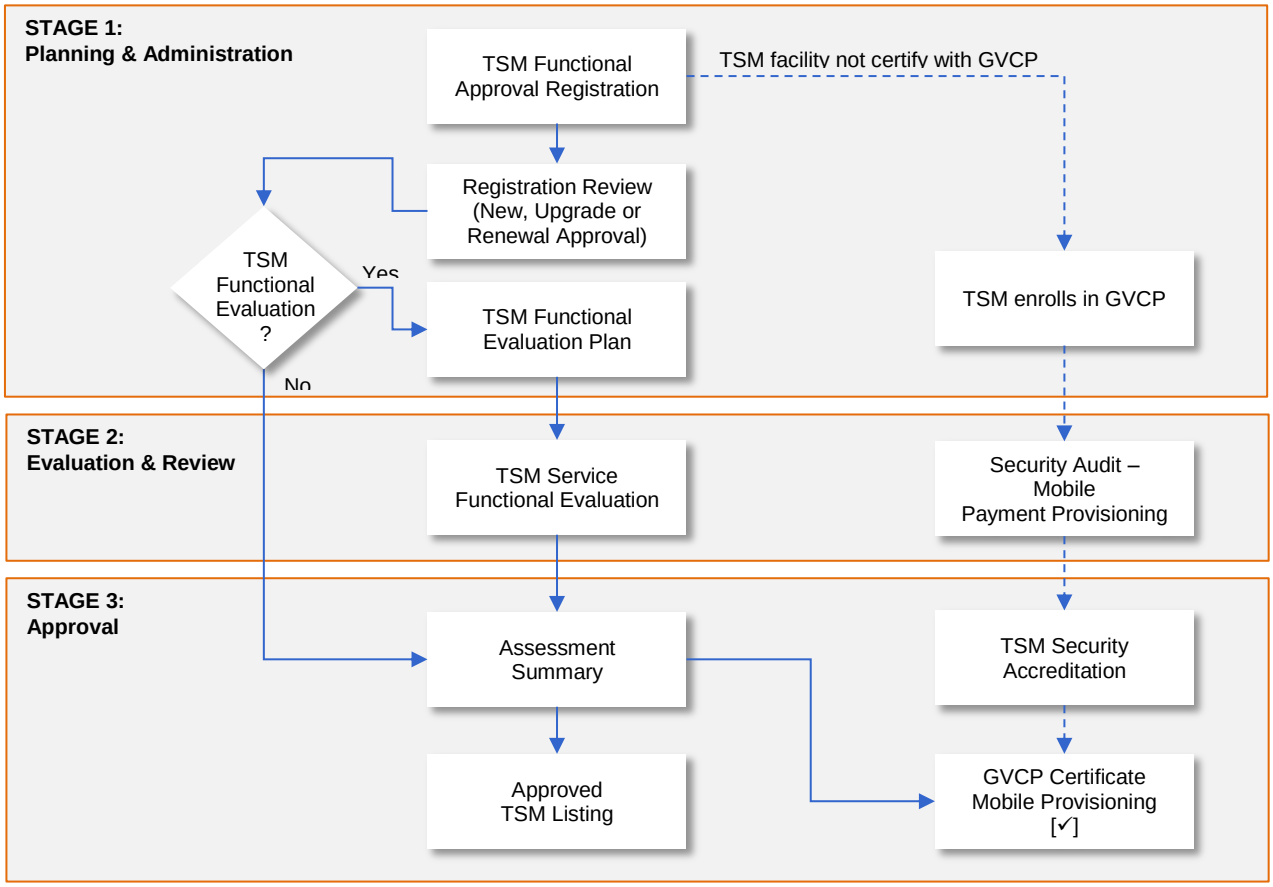
This chapter gives a high level overview of the three key stages in the Certification Process.

3.1 Overview

The TSM Certification Process can be broken down into three key stages as shown in the diagram below. This chapter provides a high level overview of each of the key stages, and chapters 4 – 6 provide more detailed descriptions of each specific step in the process.

Figure 3.1 identifies the individual processes and their relationships.

Figure 3.1—Mobile MasterCard *PayPass* TSM Certification Process Overview



3.2 Key Stage 1: Planning & Administration Phase

The first step of Key Stage 1 is the Registration Process during which the TSM vendor will register their product or service and a specific geographic site where processing will take place, by completing a Registration Form designed to capture information about the TSM system, the key point of contact and the product/service and the site (including all relevant components and features).

Once registration has been completed MasterCard's technical teams will review the information provided and make decisions on what type of evaluations are needed and where these should be carried out. The required evaluations and accompanying instructions to the TSM vendor, regarding the next steps, are formally summarized in the Evaluation Plan which is provided to the TSM vendor.

Any TSM vendor that is not yet enrolled in the Global Vendor Certification Program (GVCP), will need to do so at the earliest available opportunity, as this is a prerequisite for the Security Audit to take place.

3.3 Key Stage 2: Testing and Evaluation Phase

Once the TSM vendor has received the Evaluation Plan the TSM system is able to start formal evaluation. The scope of functional evaluation depends on whether it is a new approval or an upgrade/renewal approval. The evaluations are carried out by MasterCard personnel.

3.4 Key Stage 3: Review & Certification Phase

MasterCard will perform a thorough assessment and review to ascertain the level of conformance with the various requirements.

Each project implementation in a facility will be assessed individually, and if successful, any or all the assessments will be summarized in a formal statement called the Assessment Summary (AS).

The results of the assessment (and where applicable the AS) are then presented to MasterCard's Certification Authority for final review and a Compliance Certificate can then be issued to the TSM system, thus formally confirming compliance of the TSM vendor and its solution with all requirements.

4 Administrative Processes

This chapter outlines the Administrative Processes. There are two different areas of focus for any TSM Certification:

1. Functional evaluation
2. Security evaluation

The administrative processes described in this document cover both areas, while the administrative sub-process specifically covering the security evaluation area will generally be determined during the Registration Process (see section 3.2) and are detailed in the resulting Evaluation Plan (see section 3.3).

4.1 TSM Registration

4.1.1 Purpose

TSM Registration or Upgrade/Renewal Registration is designed to register full details:

- Of new TSM system and the functional scope thereof for formal evaluation.
- Of the TSM geographical location for logical and physical security evaluation.
- Of any change to a TSM system that has already been approved.
- Of the existing TSM site and its most up-to-date service description for the annual renewal (in the case of annual renewals to existing Certifications).

In the case of a renewal or change, it is the TSM vendor's responsibility to ensure all supporting documentation is unexpired, valid and applicable.

The TSM registration for renewal is required when TSM vendor undergoes the GVCP annual renewal certification.

Note **Each physical TSM site or facility will need to be registered separately as Security Audits, Accreditations and Compliance Certificates are site specific. Assessment Summaries relating to the TSM system and its end-to-end configuration might be re-used for multiple sites, provided they all use the same approved TSM platform and offer the same service levels and functionality.**

Note **The Registration Form will need to be completed for every annual renewal of an existing TSM and its service.**

4.1.2 Output

The result of this process is a completed registration form submitted by the TSM.

4.1.3 Requirement Level

The process is mandatory for all Certification requests.

4.1.4 Procedure

The procedure is:

1. The TSM vendor obtains the latest version of the TSM Registration Form from the Mobile Partner Program website [www.mastercard-mobilepartner.com] or from the Mobile Partner Program contact below.
2. The TSM vendor completes all relevant parts of the Mobile MasterCard *PayPass* TSM Registration Form.

Note **MasterCard will instruct the partner which sections of the forms to fill in when the TSM receives the forms.**

For new implementations or renewal requests, any existing relevant formal documentation relating to previous formal test cycles should be submitted. For changed products/components, information describing the change should also be submitted.

3. The documentation is e-mailed to the contact below.
4. MasterCard receives the registration documentation to enter into the database.

4.1.5 Contacts

The MasterCard contact for TSM Registration is mobilepartner@mastercard.com.

4.2 TSM Registration Review and Evaluation Plan

4.2.1 Purpose

This process is comprised of two stages:

1. Registration Review
2. Evaluation Planning

Once the completed registration form has been received the information will be reviewed by MasterCard to:

- Check that all relevant license agreements are in place and valid for the TSM vendor.
- Identify the mandated formal evaluations for the registered TSM roles.

- Provide information to allow the TSM vendor to initiate the ordering process for formal security evaluations at Test Laboratories and Auditors.
- Provide documentation to indicate to Laboratories and Auditors that MasterCard has given the 'green light' to begin formal evaluation.
- Identify a date by which evaluations must be completed.

4.2.2 Output

The results of the review will result in the Evaluation Plan which will contain relevant details as listed above as well as a set of clear instructions to the TSM vendor describing how to proceed with the evaluations.

This is an internal MasterCard process and is applied to all submissions.

MasterCard will contact the submitting entity if any further details are required as input to this process, or to notify of changes to the evaluation process or plan.

4.2.3 Requirement Level

The process is mandatory for all Certification requests.

4.2.4 Procedure

The procedure is:

1. MasterCard reviews the information in the TSM Registration Form
2. MasterCard issues an Evaluation Plan and sends it to the contact name given in the Registration Form

4.2.5 Contacts

The MasterCard contact for queries relating to the Evaluation Plan is mobilepartner@mastercard.com.

4.3 GVCP Application

4.3.1 Purpose

In order for a TSM vendor to start any processes relating to the security evaluation, it must be enrolled in the Global Vendor Certification Program (GVCP).

TSM's that are not enrolled in the GVCP at the time of registering their solution for Certification will be instructed to do so at their earliest opportunity in the Evaluation Plan.

4.3.2 Output

The outcome of GVCP Application will be enrollment of the TSM vendor in the GVCP, which will in turn enable the TSM vendor to be audited by the accredited auditors and to receive Accreditation and ultimately Certification.

4.3.3 Requirement Level

The process is mandatory for all TSM's that are not enrolled in the GVCP at the time of registering for Certification.

4.3.4 Procedure

The procedure is:

1. The TSM vendor receives the instruction to enroll in the GVCP as part of the Evaluation Plan (where applicable).
2. The TSM vendor contacts the GVCP Helpdesk to initiate enrollment
3. Further instructions will be given by the GVCP Helpdesk

4.3.5 Contacts

The MasterCard contact for queries relating to GVCP Application is gvcp-helpdesk@mastercard.com

5 Evaluation Processes

This chapter outlines the Tests and Evaluations Processes.

5.1 TSM Functional Evaluation

5.1.1 Purpose

The TSM Functional Evaluation process is designed to ensure that any TSM system offering that is designed to interact with any part of a Mobile MasterCard *PayPass* implementation conforms to MasterCard's functional expectations as defined in:

- [*Mobile MasterCard PayPass TSM Functional Requirements*]

This may include:

- A filled-in of an evaluation script of the TSM platform which the TSM System is based on if a new or upgraded TSM platform is used.
- A review of technical documentation submitted by the TSM vendor describing the end-to-end solution.
- An end-to-end evaluation by MasterCard on a staging environment (which may be pre-commercialization, but must utilize all systems that will be used when launched to market – such as servers, OTA gateways etc.).

This process does not take into account the security requirement of a TSM system.

A Functional Evaluation of the TSM system can be required as a result of the Registration Review

5.1.2 Output

The output of this process is a TSM Functional Evaluation Report, if the TSM platform is evaluated.

5.1.3 Requirement Level

When required by MasterCard.

5.1.4 Procedure

The procedure is:

1. Following completion of the TSM Registration process the vendor will have received a TSM Evaluation Plan giving clear instructions on what type of supporting documentation should be sent to whom for evaluation.

2. The partner provides the requested documentation to MasterCard as specified in the Evaluation Plan.
3. MasterCard performs the evaluations and generates a TSM Platform Functional Evaluation Report (if a new or upgraded platform is used).
4. The TSM System Functional Evaluation Report is used as input to the Accreditation Review.

5.1.5 Contacts

All queries relating to the TSM System Functional Evaluation Process shall be sent to mobilepartner@mastercard.com

5.2 TSM Security Audit

5.2.1 Purpose

This process tests the compliance of a TSM system to MasterCard's security requirements for TSM system as defined in:

- [*Security Requirements for Mobile Payment Provisioning*]

It is an audit that is performed by a MasterCard approved auditor to assess the physical and logical security of the TSM system, including the provider's facilities and all relevant applications designed for use in a Mobile MasterCard *PayPass* implementation.

Note **Where the functionality supplied by the TSM extends beyond the scope as defined in [*Security Requirements for Mobile Payment Provisioning*] there may be additional requirements for PCI compliance.**

5.2.2 Output

The process results in a report relating to the TSM system and its service or solution. The report will be issued by a MasterCard approved auditor.

Successful completion of the audit will enable the TSM to become accredited by MasterCard for the provisioning of services relating to Mobile MasterCard *PayPass* implementations (such as Over the Air (OTA) provisioning and personalization services).

If the report concludes that a service does not conform to requirements, the submitting entity or entities will be informed and asked what steps they intend to take to correct any nonconformance.

Note **Please check for the latest versions of specifications and reference documentation prior to the audit.**

5.2.3 Requirement Level

The process is mandatory for all Certification requests.

5.2.4 Procedure

The procedure is:

1. The vendor must be a Global Vendor Certification Program (GVCP) member before an audit can take place. If the vendor is not yet a GVCP member, appropriate instructions will be included in the Evaluation Plan.
2. Detailed instructions on the audit process will be given by the GVCP when the vendor contacts the GVCP to initiate this process.
3. The vendor will follow these instructions to arrange for the audit to take place.
4. Audit reports are compiled by the auditors and will be sent to the vendor.
5. MasterCard's GVCP will need to review the audit report and any corrective action plans that may result from the audit and will use these as input to the accreditation.

Note **MasterCard's GVCP will give detailed instructions to the vendor as to which steps need to be completed as part of the GVCP membership, the audit process and any fees that may apply.**

5.2.5 Contacts

The MasterCard contact for GVCP queries and the audit process is:
gvcp-helpdesk@mastercard.com

6 Final Review and Certification Processes

This chapter outlines the Final Review and Accreditation Processes.

6.1 Functional Evaluation Assessment

6.1.1 Purpose

This process is an internal MasterCard process and is a technical review of all the evaluation results for a registered system. It is designed to ensure that the system demonstrates sufficient conformance to MasterCard's functional requirements when tested.

6.1.2 Output

The output of this process is a TSM System Functional Evaluation Assessment Summary (or simply Assessment Summary - AS).

6.1.3 Procedure

The procedure is:

1. MasterCard will review the evaluation report.
2. If the results of the evaluation are positive this will result in a TSM System Functional Evaluation Assessment Summary which is used as input to the Certification Review.

6.1.4 Contacts

All queries relating to the TSM System Functional Evaluation Process shall be sent to mobilepartner@mastercard.com

6.2 Security Audit Review

6.2.1 Purpose

The purpose of this process is for MasterCard's GVCP to review the results of the audit report which will have been carried out based on MasterCard's Security Requirements for OTA Provisioning.

6.2.2 Output

The output of this process is a TSM Security Accreditation.

6.2.3 Procedure

The procedure is:

1. MasterCard receives the Security Audit report and any corrective action plan from the TSM
2. MasterCard reviews the audit report from the accredited auditors and any corrective action plan from the TSM.
3. If the outcome of the review is positive, the TSM will be accredited by MasterCard.
4. If the outcome of the review is negative, the TSM will be requested to put in place necessary corrective actions to provide proof of the completion thereof when this has been done.

6.2.4 Contacts

All queries relating to the Security Audit Review process shall be sent to gvcp-helpdesk@mastercard.com

6.3 TSM Certification

6.3.1 Purpose

The purpose of this process is to issue a formal statement of compliance to the TSM confirming that all aspects of the TSM and its service conform to all applicable MasterCard requirements.

This formal statement of compliance is known as the Compliance Certificate and can be used by the vendor to prove to its customers that it has met MasterCard's requirements and can be used in the context of Mobile MasterCard *PayPass* issuance.

6.3.2 Output

The output of this process is TSM Compliance Certificate.

6.3.3 Requirement Level

This is mandatory for TSMs wishing to provide their system to MasterCard issuing institutions for use in Mobile MasterCard *PayPass* implementations.

6.3.4 Procedure

The procedure is:

1. MasterCard's certification authority reviews the results of the TSM System Functional Evaluation Assessment Summary and the TSM Security Audit Review.
2. If the results of all applicable assessments are positive MasterCard will issue the Compliance Certificate to the vendor.

Compliance Certificates may be made available to MasterCard's Mobile Partner Program Members on www.mastercard-mobilepartner.com for reference.

6.3.5 Contacts

All queries relating to the TSM Certification shall be sent to mobilepartner@mastercard.com.

Appendix A Checklist

This annex contains a checklist to help you verify that you have completed each required step in the approval process.

A.1 Checklist

In order to assist TSMs with the approval process, the following check-list has been drawn up. The key stages in the process are listed here so that the submitting entity can easily keep track of what tasks have been completed and which ones may still be required.

Check the box next to each step you have completed.

1.	☐	Check latest requirements	These can be obtained from www.mastercard-mobilepartner.com
2.	☐	Complete Registration Form.	The latest registration form can be obtained from www.mastercard-mobilepartner.com Help with completing the form can be obtained from mobilepartner@mastercard.com
3.	☐	Submit Registration Form to MasterCard	Send completed form to mobilepartner@mastercard.com
4.	☐	Receive Evaluation Plan.	An Evaluation Plan can only be issued once a completed Registration Form has been received. Every Evaluation Plan is specific to a submission.
5.	☐	Follow instructions for GVCP process.	When required the GVCP process will be detailed in the Evaluation Plan, the contact for all GVCP-related queries will be GVCP-HelpDesk@mastercard.com
6.	☐	Complete evaluation questionnaire and provide supporting documents for project implementation to MasterCard contact for Functional Evaluation to be carried out	As specified in the Evaluation Plan if required.
7.	☐	Receive Functional Evaluation Report	MasterCard will issue the Evaluation Report from the filled questionnaire and supporting documents received.

8.	☐	Receive feedback from MasterCard	If the Evaluation Report indicates non-conformance with requirements corrective action will need to be taken and the relevant tests will need to be repeated.
9.	☐	Audit Report	The result of the Security Audit (which will be coordinated by GVCP) is an audit report.
10.	☐	Pass Audit Report to MasterCard GVCP as soon as possible	The Security Audit Report should be sent to MasterCard GVCP as soon as possible: GVCP-helpdesk@mastercard.com.
11.	☐	Compliance Certificate	A Compliance Certificate will be issued if the results of all the required tests and security evaluation prove that a TSM meets MasterCard's requirements.