Mobile MasterCard *PayPass* Fully Encapsulated Secure Elements Approval Guide

September 2013 - Version 1.0

Notices

Following are policies pertaining to proprietary rights, trademarks, translations, and details about the availability of additional information online.

Proprietary Rights

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

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

Trademarks

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

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

Disclaimer

MasterCard makes no representations or warranties of any kind, express or implied, with respect to the contents of this document. Without limitation, MasterCard specifically disclaims all representations and warranties with respect to this document and any intellectual property rights subsisting therein or any part thereof, including but not limited to any and all implied warranties of title, non-infringement, or suitability for any purpose (whether or not MasterCard has been advised, has reason to know, or is otherwise in fact aware of any information) or achievement of any particular result. Without limitation, MasterCard specifically disclaims all representations and warranties that any practice or implementation of this document will not infringe any third party patents, copyrights, trade secrets or other rights.

Translation

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

Information Available Online

MasterCard provides details about the standards used for this document—including times expressed, language use, and contact information—on the Publications Support page available on MasterCard Connect™. Go to Publications Support for centralized information.

Table of Contents

Chapter 1 Introduction

This chapter provides an introduction to the approach to approve Mobile MasterCard PayPass fully encapsulated secure element products for defined categories of handsets.

Purpose

Fully Encapsulated Secure Element (FE SE) products enable handsets without factory installed contactless capability to be upgraded to incorporate this function. These products typically come in the form of a self-contained MicroSD or UICC and incorporate contactless technologies including an NFC controller, a Secure Element and an antenna. This document provides Vendors with guidelines on how to seek approval of fully encapsulated secure elements for a defined category or categories of handset reducing the cost of the approval process.

Audience

This document is intended for use by manufacturers and suppliers of:

- Fully encapsulated secure element products complete with an antenna and Mobile MasterCard *PayPass* application(s) such as:
  - UICC with internal or flexible external antenna,
  - MicroSD with internal or flexible external antenna,
  - Attachment with antenna and secure element,
  - Sleeve which either adapts the above mentioned MicroSD or UICC product or has its own self-contained contactless function built in.
- Mobile MasterCard *PayPass* application(s) that are designed to run on specific fully encapsulated secure element products which may be developed by entities other than the *PayPass* application developer

This document is aimed at the Vendor's Program Manager or Project Manager responsible for the delivery of products through the Mobile MasterCard *PayPass* fully encapsulated secure element Approval Process.

Fully Encapsulated Secure Element approval process overview

The process described below is an overview of the fully encapsulated secure element approval process.

1. The Vendor will submit the product using the **Fully Encapsulated Secure Element Registration Form** in which information will be provided about

the Secure Element, the contactless interface and antenna of the product. See http://www.mastercard-mobilepartner.com/documentation.html for the latest Registration Form.

2. The Vendor will form categories of similar handsets using criteria outlined in this document. A randomly selected handset within a category of handsets will be able to show similar performance representative of all other handsets within that category.
3. The Vendor is responsible for testing each handset and maintaining its own test reports. Test reports do not have to be submitted to MasterCard but should be used by the Vendor to judge which handsets are listed in each category.
4. The Vendor will detail the criteria used to form each category and will provide MasterCard a **Handset Category document** explaining the criteria and list the handset models in their respective categories.
5. Where the categorization is deemed acceptable, MasterCard will randomly select one or more handset(s) per category and will issue a Mobile Evaluation Plan Summary (MEPS). The Vendor will then source the handsets and send them fitted with their product to an accredited test laboratory.
6. For each handset, the Vendor will identify the placement of their product and the central point of their antenna. This then becomes the testing point which the test laboratory references for testing. This information will be recorded in the Fully Encapsulated SE registration form after agreement by MasterCard on the selected Handsets.
7. For products able to be approved (functional and security evaluation successful), MasterCard will issue a Letter of Approval (LoA) indicating that the product may freely be used and personalized by issuers. For each approved handset category the LoA will list the sample handset(s) which was tested and a link where information on additional handsets can be found. Approved products will be permitted to be used with all handsets in the passing handset category.
8. The Vendor must list the approved product/handset combinations on a consumer facing website.
9. On the exterior of the product packaging, the Vendor must make clear the necessity for handset compatibility and either list the approved handsets or where packaging area is too small include the website address given in 8) above.
10. Additional handsets (which are not available for testing at time of registration) can be added to the approved categories by carrying out own testing to ensure similar performance to approved handsets, updating the Handset category document and updating the reference website. MasterCard reserve the right to request formal testing of additional handsets.

Note **In case where the Fully Encapsulated Secure Element is designed to work with specific handsets e.g. a Sleeve product then the information should be entered directly to the Registration Form and there is no need to define handset categories.**

Category creation overview

The Figure below gives a quick overview of category creation, sample formal testing and approval outcome.

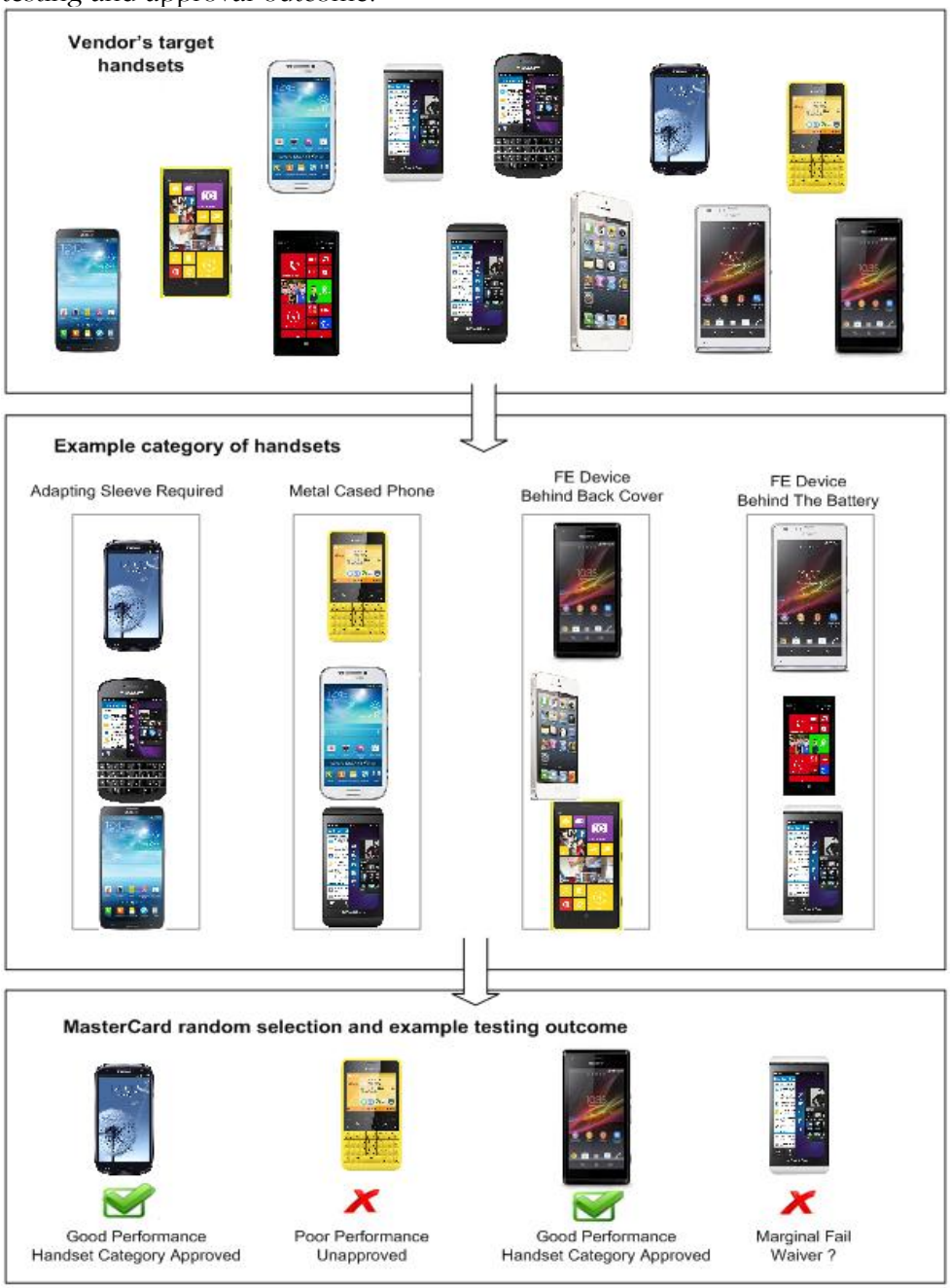

Fig. 1 Example categorization of handsets and possible testing outcome.

Chapter 2 Prevalidation and planning

This chapter provides a high-level overview of the requirements for creating categories of handsets for the approval of a fully encapsulated secure element and preparation needed for Registration

Handset Categories.

The following section gives an overview of how handset categories are defined. At a high level, handset categorizations may include for example handsets where the Fully Encapsulated Secure Element device will be behind the battery, in-front of the battery, used with a metal cased phone, attached externally or requires an adapting Sleeve. These are meant as examples and are not exhaustive.

- The Vendor will detail the criteria used to form each category and will provide MasterCard with a Handset Category document listing all the handsets in their respective categories and explaining the criteria. Note that all target handsets available at time of registration should be reviewed when creating Handset Category document.
- Vendor must complete their own testing of each handset and be confident of the similar performances of handsets within a category (see Prevalidation Report guide below).
- The Vendor is strongly recommended to prepare a reference standalone board which allows testing without a specific handset. This allows the absolute behavior of the device to be measured and to better assess the impact when inserted in a specific handset.

A Vendor can register a Fully Encapsulated Secure Element for one or more handset categories.

Prevalidation Report guide

The Vendor is responsible for testing of handsets to ensure compatibility and maintaining a Prevalidation report. This section gives advice on a minimum set of test results to be included in the Prevalidation report.

1. The Prevalidation Report may contain results from tests performed in-house by the Vendor and/or from tests performed by an external Test Laboratory. Please note that formal testing must be conducted by a MasterCard accredited laboratory.
2. For each type of test results included in the Prevalidation Report, the Vendor must record the test methods used and the purpose of the tests as well as how to read the results (units used, identification of devices).

For each handset tested a photo of the handset indicating the center of antenna marking should be included.

3. The Vendor must record the analog test results to prove compliance of the Fully Encapsulation Secure Element and handset combination with the latest EMV Contactless Specifications for Payment Systems. This must include load modulation values at 0, 1 and 2 cm and may also include values at 3 and 4 cm.
4. The Vendor must record the transaction Mag Stripe and EMV transaction timing performances for at least one handset within each category.
5. The Vendor must record the maximum read range values where a transaction is successful when presenting the handset at the center of the antenna of a terminal. These test results must include values for a set (at least 5) of approved *PayPass* terminals.
6. The Vendor may also record the maximum read range values where a transaction is successful when presenting the handset at other position than the center of the antenna of a terminal. This must include results for the same set of approved terminals and details of each position used (compared to the center of the antenna of the reader).
7. Where a Vendor has prepared a reference standalone board it should also be tested and results recorded in the Prevalidation report.

Note

The test results presented in the Prevalidation Report are for information only and will not be considered applicable for the approval step. Only test results from a MasterCard Accredited laboratory are valid for the formal approval step. The Vendor cannot challenge the test results coming from the MasterCard accredited laboratory (for instance if the test results are weaker during the approval than shown in the preliminary report).

Maintaining the CAST Security Assurance Level

You must also obtain acknowledgement by MasterCard that the secure element chip, operating system, and application(s) meet the security requirements as documented in Compliance Assessment and Security Testing Program.

If you do not have a Mobile Payment Certificate Number (MPCN) for the Secure Element used in the Fully Encapsulated Secure Element please contact CAST@mastercard.com for details of how to register for the program.

The section below provides an overview of the fully encapsulated secure element formal testing and evaluation process

Chapter 3 Formal Testing and evaluation

The section below provides an overview of the formal functional testing and report assessment

1. On receipt of and acceptance of the Fully Encapsulated Registration Form and the Handset Category document MasterCard will issue a Mobile Evaluation Plan Summary (MEPS) listing which handsets will be used for formal testing.
2. The Vendor will submit the Fully Encapsulated Secure Elements samples prepared as requested in the MEPS fitted to the selected handsets marked with center of antenna to their selected MasterCard Accredited Test Laboratory for formal testing. Where a reference standalone board has been prepared it should also be submitted to the Test Laboratory.
3. The Test Laboratory will perform a full set of functional testing (e.g. Performance, Analog, Protocol, Application, RF Interference, Integration, Combination) on one handset and run regression tests on the remaining handsets as specified in the MEPS and issue a Test Report. Where a reference standalone board has also been submitted it will also be tested.
4. MasterCard will formally assess the Test Report and issue a Test Assessment Summary (TAS) based on the results and noting any restrictions. Note that the criteria to judge the results will be the same as applied to handsets with built-in NFC functionality.

Chapter 4 Approval and extensions

Requesting Approval

The section below provides an overview of the fully encapsulated secure element approval process:

1. Once a successful Test Assessment Summary and CAST Certificate are available the Vendor can request a Letter of Approval (LoA).
2. MasterCard's Approval Authority will review the TAS, CAST Certificate, together with the Registration Form, Mobile Evaluation Plan Summary , Test Reports and any other supporting documentation and will then
   - issue a Mobile MasterCard *PayPass* Vendor Product – Letter of Approval (LoA) to the Vendor or submitting entity (listing the technical details of the product, the handset(s) for which use has been approved as well as any restrictions that may apply). The approved handset categories, tested handsets and a link to full handset lists will be noted in the LoA.

   or

   - not approve the implementation and inform the Vendor or submitting entity about this decision.
3. Once a Letter of Approval (LoA) has been issued it will be made available on the Mobile MasterCard *PayPass* Approvals List on the Mobile Partner Program website www.mastercard-mobilepartner.com/approvals.html and on the PayPass.com site as well.

Note **The Letter of Approval (LoA) will have an expiry date linked to the expiry date of the CAST Certificate used in the product.**

Extending Approval with additional handsets

The section below provides an overview of how additional handsets (these should be ones which were not available for testing at time of launch) are added to the approval after the original LoA has been issued.

1. The Vendor completes own testing and confirms that the performance of the additional handsets is similar to existing approved handsets.
2. The Vendor submits an updated Handset Category document including the additional handsets added to the existing categories. MasterCard acknowledges the update but a new LoA is not issued. MasterCard reserves

the right to request formal testing for additional handsets if deemed needed.

3. The Vendor should update their website and marketing materials with any additional approved handsets.

Note **Should a Vendor wish to define a new handset category after the original LoA has been issued it will be treated as a new registration.**

Renew Approval

Approval renewal is required when the initial LoA (3 years) is about to expire and the Vendor wishes to continue to have issuance with the product.

Please contact MasterCard at mobilepartner@mastercard.com to request approval renewal.

Both functional testing and security evaluation (CAST) extension are needed before the LoA can be issued.

Appendix A. Glossary

This chapter defines various terms, concepts, acronyms, and abbreviations used in this document. These definitions appear for convenience only and are not to be used or otherwise relied on for any legal or technical purpose. MasterCard specifically reserves the right to amend any definition appearing herein and to interpret and apply all such definitions in its sole discretion as MasterCard deems fit.

The following terms are specific for this document. Other terms are explained in the *MasterCard Dictionary*.

Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

Acronym	Meaning
CAST	Compliance Assessment and Security Testing
CCS	Component Conformity Statement
CRI	Cryptography Research Inc.
FESE	Fully Encapsulated Secure Element
GVCP	Global Vendor Certification Program
IC	Integrated Circuit
ICCN	Integrated Circuit Certificate Number
LoA	Letter of Approval
MEPS	Mobile Evaluation Plan Summary (issued by MasterCard)
MPCN	Mobile Payment Certificate Number
NFC	Near Field Communications
OS	Operating System
SE	Secure Element
TAS	Test Assessment Summary
UICC	Universal Integrated Circuit Card

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*.
Approval Authority	The individual or department within MasterCard that has been assigned the authority to formally issue Letters of Approval.
Compliance Assessment and Security Testing Certification	Compliance Assessment and Security Testing (CAST) program is a global program whose objective is to ensure that the secure element, OS and Mobile MasterCard *PayPass* payment applet conform to the MasterCard security requirements.
Component	Any product, part or combination of parts used in a Mobile MasterCard *PayPass* implementation (e.g. mobile device, secure element)
Formal Selective Testing	Functional evaluation of a Mobile MasterCard *PayPass* Secure Element for the purpose of deploying a limited number of devices for a mobile payment pilot or trial.
Formal Testing	Functional evaluation of a Mobile MasterCard *PayPass* Secure Element for the purpose of issuing a LoA or CCS.
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.
ICCN	Integrated Circuit Certificate Number - Security Compliance Certificate granted to an approved Integrated Circuit which forms the basis of the Secure Element.
Issuer	In the context of this document an issuer is a bank wishing to provide its customers with a mobile payment service based on NFC. All Issuers are required to ensure that they only issue Mobile MasterCard *PayPass* to fully approved implementations – i.e. all components of the implementation have been tested and approved. The issuer is responsible for personalization of customer account-holder details to the device.

Term	Meaning
MPCN	Mobile Payment Certificate Number - an individual reference number to confirm the *PayPass* application as well as the secure element on which it runs has successfully completed the CAST evaluation process
Mobile Device	Any mobile phone, smartphone, tablet or communications device that includes NFC functionality with an embedded or add-on secure element and can be used as part of a Mobile MasterCard *PayPass* implementation.
Mobile Evaluation Plan Summary (MEPS)	Test plan defining at high level the type of tests that need to be successfully executed by a MasterCard accredited test lab.
Mobile MasterCard *PayPass* Device Formal Type Approval	The umbrella term for all the functional evaluations and review processes and outputs relating to the approval of a Mobile MasterCard *PayPass* device. The final output of this group of processes is the Test Assessment Summary and Letter of Approval (LoA).
Mobile MasterCard *PayPass* Handset - Letter of Approval (LoA)	Acknowledgement by MasterCard that Secure Element to be used as part of any Mobile MasterCard *PayPass* implementation has demonstrated compliance to all the Mobile MasterCard *PayPass* requirements. This means it can be used by issuers with other approved Mobile MasterCard *PayPass* components.
Mobile Partner Program	MasterCard runs a program for all companies that are involved in or wish to be involved in any mobile payment initiative related to Mobile MasterCard *PayPass*, either at an issuer level or at a supplier level. The program is supported by a website (https://mobile.mastercard.com/Partner/Home) which acts as a communication and reference tool for all partners. The website contains Testing and Approval process documentation and list of approved products.
Payment Application	The software implementation of the Mobile MasterCard *PayPass* Specification within a secure element e.g. residing on a secure UICC, MicroSD or embedded secure element covering the requirements of the Mobile MasterCard *PayPass* Specification.
Secure Element Samples	These are the samples that must be provided to the test laboratory for testing of the Secure Elements to commence.
Test Assessment Review	MasterCard reviews the results of every test that is performed on the Secure Element and where test results meet or exceed requirements a Test Assessment Summary (TAS) confirming the compliance with relevant requirements is issued by MasterCard.

Term	Meaning
Test Assessment Summary (TAS)	A formal summary document containing assessment of the tests conducted on the Secure Element and an acknowledgement by MasterCard that the samples used for testing were compliant with the MasterCard requirements.
Test Report	Summary of test results issued by a accredited Laboratory as a result of Formal Testing or Formal Selective Testing.
Testing Laboratory	A facility accredited by MasterCard to perform tests on Mobile MasterCard *PayPass* products.

Appendix B. Check List

In order to assist Vendors, 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.	☐	GVCP Membership	Only applicable for products that have payment applications loaded during the production process.
2.	☐	Mobile MasterCard *PayPass* M/Chip 4 License Agreement	A Mobile MasterCard *PayPass* M/Chip 4 License Agreement can be obtained from mobilepartner@mastercard.com
3.	☐	CRI License	Ensure the SE chip supplier holds a CRI license.
4.	☐	Prevalidation Testing	The vendor is responsible for testing all handsets and maintaining test results in a Prevalidation test report.
5.	☐	CAST Certificate	The vendor must have a CAST certificate for the product being submitted for approval.
6.	☐	Register for Approval (submit Registration Form and Handset Category document)	Fully Encapsulated Secure Element Registration Form can be obtained from http://www.mastercard-mobilepartner.com/documentation.html
7.	☐	Mobile Evaluation Plan Summary (MEPS)	The Mobile Evaluation Plan Summary will be provided by MasterCard once the completed registration form has been reviewed.
8.	☐	Personalization Profiles	MasterCard will also provide personalization profiles along with the MEPS for the samples that will need to undergo functional testing.
9.	☐	Book Functional Testing	The vendor will need to book a test slot at an accredited test lab specified.
10.	☐	Send Samples for Testing	The vendor will need to send samples to the test lab for testing.
11.	☐	Receive Functional Test Reports	Once testing has been completed the test lab will provide test reports to the vendor.
12.	☐	Receive TAS	MasterCard will issue a Test Assessment Summary with unique reference number.

13.	☐	Request Approval (send CAST ref, TAS ref)	Once the vendor has received the TAS, CAST reference and has all the required licenses in place a formal request for approval can be made by contacting MasterCard at: mobilepartner@mastercard.com
14	☐	Receive LoA	If the product meets all requirements a Letter of Approval will be granted.