M/Chip Mobile Secure Element Approval Guide

October 2018 - Version 1.7

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.

Tables of Contents

Chapter 1 Introduction

This chapter provides an introduction to the M/Chip Mobile Secure Element Approval Process.

Scope

This document describes all the processes that Vendors must follow to obtain approval for Secure Elements that are intended for use in Mastercard M/Chip Mobile implementations. It also covers the processes that Vendors must follow for already approved products in order to maintain Mastercard approval.

This process can also be used to test components such as an embedded Secure Element(eSE) which obtain a Component Conformity Statement(CCS) but not a Letter of Approval(LoA). By presenting this CCS when incorporating the component into a full product such as a NFC Mobile Device or a Fully Encapsulated Secure Element(FESE), the amount of testing required can be reduced (through inheritance) before an LoA is issued.

Audience

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

- Secure Element products complete with M/Chip Mobile application(s) eg. Single Wire Protocol(SWP) UICC, SWP MicroSD or eSE products.
- M/Chip Mobile application(s) that are designed to run on specific Secure Element products (including chip and OS) which may be developed by entities other than the application developer.

This document is aimed at the Vendor's Program Manager or Project Manager responsible for the delivery of products through the M/Chip Mobile Secure Element Approval Process.

Note **"M/Chip Mobile" is used as a generic term to cover M/Chip Mobile and Mobile Mastercard PayPass – M/Chip 4 technical specifications.**

The approval process for Fully Encapulated Secure Elements (i.e. products which include Near Field Communications (NFC) and antenna functionality) is covered in a separate guide.

Related Information

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

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

Title	Description
EMV® Contactless Specifications for Payment Systems - Book D *EMV Contactless Communication Protocol Specification*	Available from EMVCo web site. See https://www.emvco.com/document-search/
The EMV 4.3 Specifications	Latest EMV requirements. See http://www.emvco.com/specifications.aspx?id=223
M/Chip Mobile Technical Specification	Latest M/Chip Mobile payment applet specification. License can be requested from Digitallicensing@mastercard.com
Mastercard Contactless - Device Approval Application Notes	Latest applicable Application Notes. See https://mobilepartner.mastercard.com/documentation.html#1
M/Chip Mobile Secure Element Registration Form	Latest registration form for a M/Chip Mobile Secure Element product. See https://mobilepartner.mastercard.com/documentation.html#4
Mastercard CAST Approval Process for Mobile Payment Applications	A white paper describing The CAST (Compliance Assessment & Security Testing) process for Mobile. See http://globalrisk.mastercard.com/online_resource/cast-approval-for-mobile-payment-applications/

Chapter 2 The M/Chip Mobile Secure Element Approval Process

This chapter provides an overview of the M/Chip Mobile Secure Element Approval Process.

Overview

The M/Chip Mobile Secure Element Approval Process comprises the following subprocesses:

- Process Key Stage 1 : Planning and Admininstration Phase
  - Global Vendor Certification Program (GVCP) – where applicable
  - Obtain M/Chip Mobile Development License
  - Product Development
  - Approval Registration
- Process Key Stage 2 : Testing and Evaluation phase
  - Preparation for Testing.
  - Functional Testing
  - Compliance Assessment and Security Testing (CAST)
- Process Key Stage 3 : Assessment and Approval Review Phase
  - Test Assessment
  - Request Approval
  - Renew Approval

Figure 2-1 shows the process and the sequence flow between its subprocesses:

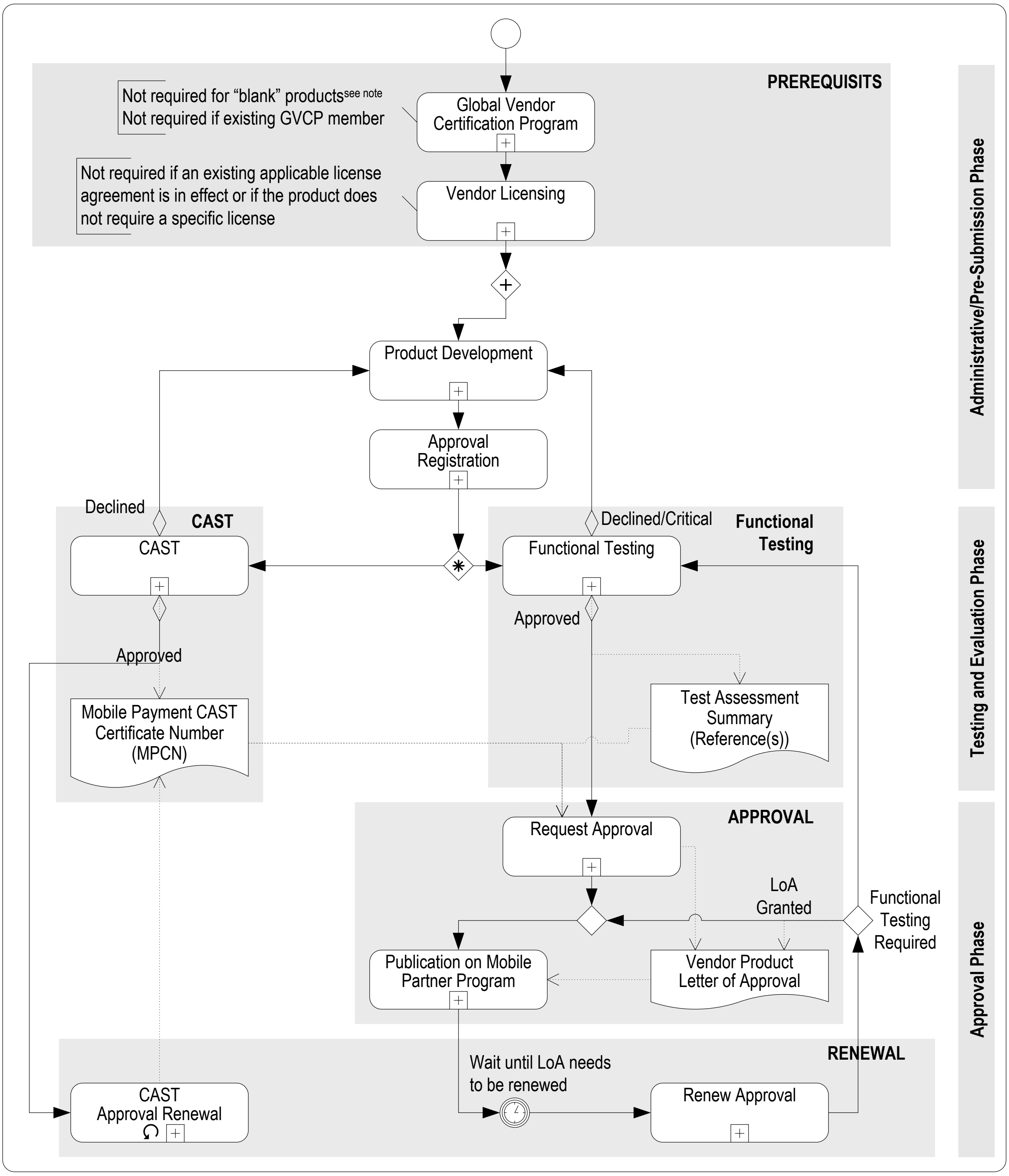
PREREQUISITS
Not required for "blank" products see note
Not required if existing GVCP member
Global Vendor Certification Program
Not required if an existing applicable license agreement is in effect or if the product does not require a specific license
Vendor Licensing
Administrative/Pre-Submission Phase
Product Development
Approval Registration
Declined
CAST
CAST
Declined/Critical
Functional Testing
Functional Testing
Approved
Approved
Mobile Payment CAST Certificate Number (MPCN)
Test Assessment Summary (Reference(s))
Testing and Evaluation Phase
APPROVAL
Request Approval
LoA Granted
Functional Testing Required
Publication on Mobile Partner Program
Vendor Product Letter of Approval
Approval Phase
RENEWAL
Wait until LoA needs to be renewed
CAST Approval Renewal
Renew Approval

Figure 2-1 – M/Chip Mobile Secure Element Approval Process

Note : A "blank" product is one without the M/Chip mobile applet loaded

Process Key Stage 1: Planning & Administration Phase

All Vendors wishing to develop and have their products approved by Mastercard must obtain the necessary licenses and agreement as described below before registering their product.

Global Vendor Certification Program (GVCP)

GVCP is a program covering assessment of the physical security of the manufacturing site and logical security of the production data network environment, hardware, and software. This program is used to maintain and improve your security infrastructure and to prevent attacks against Mastercard products, components, and related network and company image.

Applicability of GVCP

If the Secure Element is personalized with a Mastercard payment application at production, then the facility where the application is loaded onto the Secure Element must be a GVCP certified facility.

If the Secure Element contains any Mastercard logo, hologram or branding, then the facility where this is applied must be a GVCP certified facility.

If the Secure Element does not contain a Mastercard payment application at production, nor Mastercard Logo or branding then it is not required for the Vendor to be GVCP Certified, although Mastercard would recommend GVCP membership.

When the Secure Element does not contain a Mastercard application, and the issuer wishes to utilize the services of a third party Trusted Service Manager to load and enable a Mastercard application, then this Trusted Service Manager must be a GVCP certified facility.

Contact

Contact Mastercard GVCP team via GVCP-Helpdesk@mastercard.com to request whether the scope of your activities with regard to the cardholder product or component that you want to develop require you to be in this program.

Note **If you have already obtained GVCP Certification, you must still contact the GVCP team before you develop a new product or component as this may not be covered by, or may have an impact on, your existing GVCP Certification. Failure to do so could delay approval of your product or component.**

Obtain M/Chip Mobile License

All implementations that are based on M/Chip Mobile require the Vendor in question to sign a development license agreement.

If you have not previously obtained the required license from Mastercard, you should request the license document by sending an email to Digitallicensing@mastercard.com .

During this subprocess, you register your intent with Mastercard to develop a M/Chip Mobile product, execute an appropriate license agreement and provide a copy of your Product Liability Insurance (PLI) Certificate. In return Mastercard will provide you with access to the latest M/Chip Mobile specifications and supporting documents.

Product Development

Before a Secure Element is registered for formal testing, Mastercard recommends the Vendor performs debug testing at a Mastercard Accredited Test Laboratory. Debug testing is particularly valuable for Vendors new to the approval process or with a new product architecture.

The set of tests to be run during debug testing can be agreed between the Vendor and the Lab without the need for the Vendor to register. Mastercard can review the results of debug testing and provide feedback. Vendors can contact Chip Certification Cardholder Devices <chip_certification_chd@mastercard.com> for this type of support. This will help ensure the Secure Element complies with the various test requirements and reduces unnecessary costs and time delays to achieve approval.

Approval Registration

During this subprocess, you provide details of your product to Mastercard via a Registration Form, who then specify, in the Mobile Evaluation Plan Summary (MEPS), the test configuration and what formal functional tests need to be undertaken by an Accredited Test Laboratory.

If your product does not yet have a CAST Certificate confirming its compliance with Mastercard security requirements, you should also register the product for CAST approval using the same Registration Form. To enable exchange of confidential security related information a CAST Agreement needs to be in placed between Mastercard and the Vendor. For the CAST agreement please contact cast@mastercard.com

Process Key Stage 2: Testing and Evaluation phase

This phase includes preparation for testing and the actual testing.

Preparation for Testing

Booking a Test Slot at an Accredited Laboratory

The Vendor must provide the registration form and MEPS to a Mastercard Accedited Lab and agree to relevant contracts and schedules. The Test Laboratory will advise on the length of time to perform the tests based on the information in the MEPS. As a rough guideline allow 2 weeks for performing the tests.

Mastercard recommends that Vendors provisionally book test slots 10 weeks before the start of testing. Test slots can be provisionally booked before a MEPS is issued by Mastercard by providing the Lab with information about the Secure Element and assuming that Mastercard will require all tests to be run on the Secure Element.

Secure Element Samples

Before testing can begin the Vendor must provide a set of Secure Element samples to the Lab. The samples must be production quality where all features are enabled and can be tested. The test configurations required and the breakdown of Personalization Profiles required for each configuration will be listed in the MEPS.

Functional Testing

A Secure Element normally undergoes testing in the following areas to ensure that the device complies with the Mastercard requirements.

- Performance Testing (Timing Performance) against M/Chip Performance Requirements.
- Application Testing against the relevant M/Chip Mobile Application specification
- For SEs of type SWP UICC : Integration Tests of SWP UICCs with reference SWP Mobile Devices(with different NFC Controllers)

When the samples are received by the Lab all samples may undergo Pre-validation testing to ensure they have been personalized correctly. If there are any errors with the samples you will be requested to re-submit the samples. To avoid unnecessary delays please take care to prepare and verify the samples before submitting to the Lab.

Once testing has been completed, allow one week for compilation of the test report by the Lab. Once the test report is completed it will be issued by the test laboratory.

Compliance Assessment and Security Testing (CAST)

If your Secure Element does not yet have a CAST Certificate then the necessary architecture and technical documentation needs to be submitted to an Accredited Security Lab which will conduct the security analysis and produce a Security Evaluation report.

On submission of the Security Assessment to Mastercard's CAST team, a review is carried out and if the Secure Element meets the requirements of the CAST Program a CAST Certificate with a Mobile Payment Certificate Number (MPCN) is issued, normally with a validity period of 3 years from the MPCN issued date. The CAST Certificate will also note any conditions of approval e.g. compliance with the Guidance document provided by the Vendor.

Process Key Stage 3 : Assessment and Approval Review Phase

This stage details how test report assessment, approvals and renewals are carried out.

Review of Test Results

Once the Test Assessment Authority has received the Test Report, it will undergo a thorough assessment to ascertain the level of conformance with the various testing requirements. If the report identifies issues discovered during testing, Mastercard may request the Lab to perform extra tests or re-run some of the tests in order to determine the severity of the discovered issue.

The test assessment will be summarized in a formal statement called the Test Assessment Summary (TAS) that is issued to the Vendor.

Request Approval

For SWP UICC and SWP MicroSD SE products which have obtained the CAST Certificate, TAS document and any required pre-requistes, you can request approval from Mastercard, which is given in the form of an LoA. The LoA is also listed on https://mobilepartner.mastercard.com/approvals.html. When your product has obtained approval and the LoA is issued, this means that it can be proposed as a Mastercard-approved off-the-shelf product for issuers to personalize.

For eSE products which have a CAST Certificate, TAS and any required pre-requistes, you can request a CCS from Mastercard. This CCS can then be used by mobile device or FESE Vendors incorporating the eSE to inherit results when submitting their own product for approval.

Note **Both LoA and CCS will have a validity period linked to the associated CAST Certificate.**

Renew Approval

When the initial LoA needs to be renewed, you need to register your intent for renewal with Mastercard. For Functional testing, a set of delta tests will be specified in a MEPS and on receipt of a successful Test Report a new TAS will be issued which will be valid for 3 years. For CAST there are 2 possabilities. A Refresh CAST approval requires a full CAST evaluation (and a valid PCN) and if successful results in a CAST Certificate valid for 3 years. For a Renewal CAST a delta evaluation will be performed leading to an extended CAST Certificate valid for 2 years from which a new LoA can be issued. This extension process can be repeated for a maximum of 2 times.

In addition an LoA for End of Life(EoL) product which is being ramped down can be requested, in this case no additional testing is required but no new customers for the product are allowed and the LoA is valid for one year only with no possibility for further extention.

Chapter 3 Planning and Administration Phase

This section describes the Planning and Administration Phase processes.

Global Vendor Certification Program

The Mastercard Global Vendor Certification Program (GVCP) registers vendors, establishes security requirements, manages compliance, and ultimately grants certification to vendors found compliant with site security requirements applicable to SE production. SE production activities include SE manufacture, personalization, and specialized activities (such as data preparation and mobile provisioning).

Purpose

The Mastercard Global Vendor Certification Program (GVCP) program administers vendor compliance with site security requirements that promote a more secure Card production environment. The security Standards apply to the physical Card production environment and logical security that protects data during transport, storage, and usage.

The purpose of the program is to:

- Evaluate vendor compliance against a global Standard

- Minimize the risk that inadequate security controls place Mastercard-branded cards at risk.

Output

The output of this process will be a Certificate of Compliance with associated Certificate Number and Expiration Date. Certificates are issued to certified vendors to provide confirmation that the vendor is authorized to provide Card production services for all Mastercard brands and derivative products. The Vendor will be added to Mastercard's Certified Vendor List made available on Mastercard Connect.

Requirement Level

If the Secure Element is personalized with Mastercard payment applications at production, then the facility where the application is loaded onto the Secure Element must be a GVCP certified facility.

Procedure

1. The Vendor contacts the GVCP team and requests certification by filling the latest GVCP Application Form and signing a GVCP Vendor Agreement.

2. The vendor completes a self-assessment to assess their compliance with Mastercard security requirements. Self-assessment questionnaires are provided in an Excel document (or similar tool) sent to the vendor by email in response to their application for initial certification and certification renewal.

3. An On-site Evaluation is carried out by a Mastercard Accredited Audit Firm and the audit results are documented in an audit report and questionnaire and sent to the GVCP team for review .

4. Mastercard evaluates the onsite audit Findings and Exceptions.
   If the audit report contains findings indicating the vendor's facility does not comply with one or more Mastercard security requirements, Mastercard will notify the vendor that the certification process is not complete and request an action plan whereby the vendor describes the action it proposes to remediate each finding.

5. The Action plan is evaluated by Mastercard and if it is determined to conform to GVCP requirements a Certificate of Compliance is issued.

6. GVCP requires an annual renewal audit and the GVCP team will send a renewal reminder email three months prior to the renewal date to inform you of the renewal process.

Contacts

The Mastercard contact is the GVCP team at GVCP-Helpdesk@mastercard.com.

Obtain M/Chip Mobile License

This section details the subprocess where you register your intent with Mastercard to develop a product based on M/Chip Mobile specifications.

Purpose

To obtain access to M/Chip Mobile specifications the Vendor must execute an appropriate license agreement, and provide Mastercard with a Product Liability Insurance Certificate.

Output

Executed license agreement giving the Vendor access to the latest M/Chip Mobile specifications and supporting documents.

Requirement Level

Mandatory for any development which requires access to M/Chip Mobile specifications.

Procedure

1. Send an e-mail to Digitallicensing@mastercard.com to request a Vendor Development License Agreement for M/Chip Mobile.

2. You will receive, by return email, a copy of the License Agreement, and accompanying notes/instructions.
3. Complete the information requested in the License Agreement:
   - Effective date (this is the date that the agreement is signed by your company)
   - Company name
   - Company address
   - Name and title of your authorized signatory
4. Send an electronic copy of the signed agreement to digitallicensing@mastercard.com.
5. Mastercard will counter sign the agreement and return an electronic copy with legal stamp to the Licensee.

Note **If you have any legal questions regarding the License Agreement before signing it, please address these by e-mail to Digitallicensing@mastercard.com who will then forward them to the appropriate legal counsel in Mastercard to respond.**

6. Send, by courier, both copies of the completed M/Chip Mobile License Agreement, and a copy of your Product Liability Insurance Certificate to the Mastercard address provided. Indicate clearly, when you send the agreement copies, if your organization is a member of the GVCP, M/Chip 4 Card Development Program, Mastercard Vendor Program (MVP) or a member of CAST. Refer to the note below for the reason this information is required.
7. Pay any fees as detailed in the License Agreement.

Note **If your organization is a member of the GVCP, M/Chip 4 Card Development Program, MVP or a member of CAST, no fee is applicable.**

8. You will be provided access to the following documentation:
   - M/Chip Mobile Technical Specifications
   - M/Chip Mobile Implementation Guide
   - M/Chip Mobile Standard Profiles
   - M/Chip Issuer Cryptographic Algorithms
   - Other relevant reference documents.

Contact

The Mastercard contact is Digitallicensing@mastercard.com .

Product Development

The Product Development Cycle represents a Vendor's internal development procedures for a M/Chip Mobile product.

Purpose

Vendors may use the services of Mastercard accredited Laboratories to assist with product development and testing. Vendors should also plan for implementation and validation of applicable pre-requistes e.g. GP LoQ and EMVCo PPSE LoC (see latest Application Notes)

Use of these services is at the discretion of the Vendor. It is recommended that these services are used, as they may increase the efficiency of subsequent formal testing.

Testing during the Product Development Cycle is known as in-house testing and is considered a development aid or de-bugging exercise. It does not form any part of the formal testing requirement.

Output

The output of this process will be Vendor specific, but should generally result in improvements with regards to functional reliability and/or performance, any or all of which should lead to a higher likelihood of achieving approval.

Requirement Level

The process is optional and Vendor specific.

Procedure

Procedures will be Vendor specific. Vendors may ask the Mastercard certified lab to run some or all of the Mastercard formal tests in debug mode to check the compliance of the Secure Element under development with the Mastercard requirements.

Contacts

During this subprocess, services and support is available from Mastercard, for example, simulators for debugging (https://www.terminalsimulator.com/), or ad hoc queries regarding functional, technical, and specification enquiries:

- Queries relating to the development of M/Chip Mobile solutions in general should be addressed to chip_certification_chd@mastercard.com
- Queries regarding security related developments such as the introduction of nonstandard (possibly innovative) features in card operating systems for example should be sent to cast@Mastercard.com.

You can obtain services and support from a Mastercard Accredited Test Laboratory.

Approval Registration

This section details the subprocess where you request and complete the latest M/Chip Mobile Secure Element Registration Form, and receive the MEPS.

Note **Even if you are only developing/submitting a M/Chip Mobile application it must be registered for evaluation on a specific Secure Element product as the functional testing and security evaluation of the application(s) must always be associated with a Secure Element product/platform.**
If you are developing M/Chip Mobile application(s) for use on multiple Secure Element products (either your own or other Vendors' Secure Element products) you will need to register each combination of application and Secure Element product separately.

Purpose

The following cases will result in the Vendor submitting a Registration Form :

1. Register a new Secure Element product and provide all the details needed to plan and execute testing.
2. Update a Registration Form for a product under testing to correct an error or omission in a previous version.
3. Register a variant or derivative Secure Element (e.g. variant for a particular Mobile Network Operator(MNO) similar to an already approved Secure Element.)
4. Register changes to an already approved Secure Element.
5. Register a Secure Element for renewal of the LoA which is approaching expiry.

It is the Vendor's responsibility to provide Mastercard with all the relevant information for Mastercard to determine what testing is required. This may require the Vendor to submit additional supporting documents e.g. an architecture document describing the deltas between a variant product and an already approved product.

Output

The normal output of this process is a MEPS containing the list of tests to be performed on the registered Secure Element product. In some cases where no new testing is required, Registration can be followed by issuance of an LoA, provided the necessary CAST Certificate is available.

Requirement Level

The process is mandatory for all approval requests.

Procedure

1. Go to https://mobilepartner.mastercard.com/documentation.html#4 to download the latest version of the M/Chip Mobile Secure Element Registration Form.

2. You need to complete the information requested in this form.
3. Submit the completed M/Chip Mobile Secure Element Registration Form by e-mail to chip_certification_chd@mastercard.com ; and cast@mastercard.com no later than two weeks before the start of formal testing.
4. Mastercard will then send you a Registration Number.
5. If you are required to do Functional Testing, you will also receive a MEPS, which specifies details such as inheritance applied, configurations and tests requested.

Contact

The Mastercard contact is chip_certification_chd@mastercard.com.

Chapter 4 Testing and Evaluation Phase

This section details the subprocess where you submit your product to an Accredited Test Laboratory to be tested according to the Mobile Evaluation Plan Summary (MEPS).

Preparation for Testing

Purpose

Vendors must plan ahead for the start of testing to avoid any delay achieving approval from Mastercard. The purpose of planning ahead is to help ensure the following:

- Test slots are secured at a Mastercard Accedited Lab at least 10 weeks before the start of formal testing.
- Any special jig or adjustment to the standard testing configuration are agreed in advance with the Lab.
- Secure Element samples are received by the Lab one week before the start of testing to avoid any delay that may be introduced by local authorities/customs.
- The latest registration form and MEPS are provided to the Lab before the start of testing.

Output

The Vendor secures that the testing of the Secure Element will start on time according to the Vendor's plan.

Requirement Level

The process is mandatory.

Procedure

The procedure follows:

1. The Vendor contacts a Mastercard Accedited Lab at least 10 weeks before the planned start of formal testing to secure a test slot. This can be done before the Secure Element is registered with Mastercard by providing the lab with information about the Secure Element and assuming all tests will be run.
2. Once the Secure Element is registered with Mastercard, the Vendor must provide the latest registration form and MEPS to the lab.
3. The Vendor provides the Lab with the required samples for performing the testing. The samples must match the information in the registration form and the profiles

must be prepared according to the latest Personalization Profiles for Interface and Application Testing document.

Contact

The Mastercard contact is chip_certification_chd@mastercard.com.

Functional Testing

The purpose of the formal functional testing phase is to demonstrate that the Secure Element conforms to M/Chip Mobile requirements.

Purpose

Prevalidation Test (Optional)

The purpose of this optional test is to ensure that your samples have been correctly personalized according to the requested test profiles. If this test fails you will be asked to provide new sample Secure Elements that correct the error(s) discovered during this test.

Performance Test

The purpose of this test is to check the Secure Element complies with the current performance requirement (specific transaction time for a M/Chip transaction). If this test fails this is considered a critical failure and none of the remaining tests are performed (because successful completion of the performance tests is a mandatory prerequisite for the remaining tests).

Application Test

The purpose of this test is to check that the behavior of the application is in accordance with the specifications for the payment application covering areas such as :

- Check implementation (syntax/semantic) of the specified instructions/commands.
- Check the behavior versus the specified state machine.
- Check the behavior versus the specified cryptogram calculations.
- Check the behavior versus the specified Card Risk Management functionalities.
- For SWP UICCs – Integration testing with a selection of NFC Mobile Devices.

Requirement Level

The process is mandatory when a MEPS has been issued.

Output

The output is a Test Report issued by the Test Lab.

Procedure

1. The Accredited Test Laboratory will test your device according to the tests specified in the MEPS (which you will have previously submitted to them).

2. There are three possible responses, detailed in the following table, and the subsequent action/step that you need to do:

Response…	Action required / step to go to…
The Prevalidation Test failed	No further tests can be performed due to an oversight that can be easily corrected. You need to take the corrective action as necessary and provide new samples.
The Performance Test failed	This is a critical error, and no other tests can be performed due to this condition. You need to go back to Product Development to correct the major issues that have been identified.
All tests completed — Test Report Supplied	Go to step #3

3. You need to make an assessment on how you want to proceed based on the *Test Report*.

Test Report Indicates…	Action to take…
Favorable	Request the Test Assessment Summary from the Test Assessment Authority based on the Test Report.
Minor Issue(s) Identified	Products with minor issues are not re-engineered but accepted without conditions. Request the Test Assessment Summary from the Test Assessment Authority based on the Test Report.
Major Issue(s) Identified and a Deviation is required	Request a Deviation. See Step #4
Critical	Correction mandatory. Go back to Product Development.

4. Request a Deviation by sending an e-mail to chip_certification_chd@mastercard.com. Include the Test Report and any additional information to justify the Deviation. You will receive a response to your request for a Deviation.

Response…	Action to take…
Deviation Granted	Request the Test Assessment Summary from the Test Assessment Authority based on the Test Report. A Technical Deviation Notification(TDN) will be noted in the TAS.

Response…	Action to take…
Deviation Refused	Go back to Product Development.

Note **A Test Assessment Summary (based on a granted Deviation or otherwise obtained) does not constitute an Approval, it is merely an intermediate step that is used as input to an Approval.**

Contact

The Mastercard contact is chip_certification_chd@mastercard.com.

Compliance Assessment and Security Testing (CAST)

Purpose

This process tests the conformity of the Secure Element, including the IC, the OS and all payment applications running on it to the CAST program. The Secure Element security evaluation considers the security measures implemented by the Vendors against the CAST security guidelines, including the relevant product security guidelines. An important factor is how the Vendor build upon the security of the IC and the OS to provide overall security for a payment application.

This process can only be initiated if the IC, on which the OS and applications run, has already been evaluated by EMVCo, and has been issued with an Integrated Circuit Certificate Number(ICCN) according to the EMVCo Security Evaluation process.

To take full advantage of the CAST process for mobile payment products, the target operating system must be evaluated and maintained through the EMVCo platform security evaluation process. A successful evaluation will result in approval from EMVCo and a corresponding platform certificate number (PCN). This certificate will apply to a specific OS onboard a specific IC.

EMVCo Security evaluation includes the following:

- IC (white box) security evaluation, including vulnerability analysis and penetration testing as defined by EMVCo security guidelines.
- OS (white box) security evaluation, including vulnerability analysis and penetration testing as defined by EMVCo security guidelines.
- Development and Production facilities will be considered for security as part of the EMVCo evaluation.

CAST Security evaluation includes the following:

- Applet (white box) security evaluation, including vulnerability analysis and penetration testing as defined by CAST security guidelines .
- Development and Production facilities will be considered for security as part of the CAST evaluation .

Output

The output of the CAST process is a CAST Certificate issued by Mastercard.

Requirement Level

The process is mandatory for Secure Elements which do not already have a valid CAST Certificate.

Procedure

1. Sign a CAST Agreement with the CAST team by contacting cast@mastercard.com.
2. You will receive all relevant CAST documentation including security guidelines and the CAST process description in detail

3. You will discus your product and its configuration with the CAST team to agree the next steps. If the process as explained previously is followed and the product is of a standard configuration, the next step will be to select one of Mastercard's approved security evaluation laboratories, setup the relevant NDAs with the laboratory, disucss a test plan, book a test slot and proceed with the security evaluation.

   A product submitted to a laboratory for a CAST evaluation must be identical to the product delivered to issuing banks. The product must be uniquely identified in the details supplied in the Registration form (Product Name/Version/OS detail and so on). These supplied registration details will be confirmed by the laboratory in the CAST evaluation report.

4. As soon as a favorable evaluation report is available for your product from the accredited security laboratory it should be submitted by the evaluation laboratory to cast@mastercard.com in order to request CAST certification based on the results of the report.

5. Mastercard will review the report.

6. If the assurance level of the product is deemed to be sufficient for CAST approval a CAST certificate will be granted.

7. Mastercard will notify the Vendor and will issue an official certificate (with a unique number MPCN) including references to the

   - IC and its Hardware certification - ICCN
   - OS name and version
   - Payment Application(s) name(s) and version(s)
   - Other applications running in a shared memory domain on the IC will also need to be specified

8. The CAST Certificate will normally have a validity period of 3 years.

9. For open platform products that permit the downloading of additional applets (without prior security lab review), CAST approval will be issued with additional conditions, these conditions will be that the accompanying guidance document(s) will be followed. The guidance document will address any residual vulnerabilities and additional application requirements as a result of the evaluation, plus the addition of CAST requirements for Post Issuance Applet Downloading.

   For full details of the additional applet requirements, please contact cast@mastercard.com. As a minimum example, the following details the CAST requirements applied to an open platform product:

Product evaluation confirms the loading mechanism and applet separation is strong (High assurance)

Approval issued with conditions.

- Applets can only be downloaded by a trusted party.
- Applets must pass the latest Oracle byte code verifier.
- Applets must not contain malicious code.
- Applets can only be downloaded in a secure way.
- No assets can be shared between the additional applet(s) and the asterCard applet.
- Applets must not extend the Security Functionality of the platform product or Mastercard banking product.
- Applets that execute crypto routines must consider the underlying product guidance to address any specific requirements / limitations.
- Applets that provide a shared library must enforce the versioning policy:
  - The minor version shall be incremented when the modifications performed have no impact on binary compatibility
  - The major version shall be incremented otherwise
- When shared libraries are used by the Application, the version imported shall be binary compatible with the one loaded on the targeted platform (major version equal, minor lower or equal).

CAST security evaluation approval for additional applets is not required but conditions of approval (product guidance) must be followed.

Note1: The guidelines supplied with the product should include any other requirements / best practices for loading additional applets.

Note2: When evaluating an open platform product, other security evaluation requirements may apply (eg: GP loading / DAP / Token).

Note3: If the additional applet(s) extend the Security Functionality of the platform product or Mastercard banking product, the CAST security evaluation laboratory must review the additional applet(s). Any changes to such additional applet(s) will require a delta review by CAST.

Note **A valid MPCN is a mandatory pre-requisite for an LoA/CCS to be granted.**

Contact

The Mastercard contact is cast@mastercard.com.

Chapter 5 Assessment and Approval Phase

Assessment of Test Results

Purpose

The purpose is to review the test results in the test report generated by the Lab to determine if the Secure Element has passed all the tests requested in the MEPS issued by Mastercard.

Output

A TAS is issued by Test Assessment Authority summarizing the assessment of the test results.

Requirement Level

This process is mandatory if a Vendor wants to receive a TAS.

Procedure

1. Submit the *Test Report* (and Deviation, if appropriate) by e-mail to the Test Assessment Authority to request a Test Assessment Summary.
2. The Test Assessment Authority then assesses the Test Report and you will receive a Test Assessment Summary issued based on the test results submitted.

Note : In most cases the Mastercard Accedited Laboratory is qualified as a Test Assessment Authority and can produce the TAS.

Contact

The Mastercard contact is chip_certification_chd@mastercard.com .

Request Approval

Purpose

This section details the subprocess where you request approval when you have obtained the necessary CAST Certificate, TAS and any necessary pre-requistes.

Output

For SWP UICC and SWP MicroSD Secure Element products the output is an LoA. For embedded Secure Elements the output is a CCS.

Requirement Level

This is process is mandatory to receive an LoA or CCS.

Procedure

1. To request approval, send a request by e-mail to chip_certification_chd@mastercard.com, and include the following for your product:
   - The CAST Certificate
   - The Test Assessment Summary
   - Any Pre-requistes e.g. GP LoQ and EMVCo PPSE LoC
2. If all the details are in order you will receive the LoA/CCS in the form of a PDF that has been digitally signed by Mastercard.
3. If you receive an LoA you can then offer your product as an "off-the-shelf" product for issuers to personalize and then deploy. The LoA will have the same expiry date as the associated CAST.
4. If you receive a CCS for your embedded Secure Element it can be then used by Mobile Device and Fully Encapsulated Secure Element Vendors to inherit results from the testing.
5. The list of approved Vendor products will be published on https://mobilepartner.mastercard.com/approvals.html .

Contact

The Mastercard contact is chip_certification_chd@mastercard.com

Renew Approval

Purpose

This section details the subprocess you need to follow to renew approval when the LoA/CCS is about to expire. You need to register your intent for renewal with Mastercard.

Note **The expiry date of an LoA/CCS is linked to the expiry date of a CAST certificate. Please contact the CAST team to get more information about the correct procedures: cast@mastercard.com.**

Output

An new or extended LoA/CCS or a LoA/CCS for End-of-Life product.

Requirement Level

Mandatory to be able to continue issuance for a product approaching the LoA/CCS expiry date.

Procedure

1. When the initial LoA/CCS is about to expire, you need to register your intent for renewal with Mastercard by sending the M/Chip Mobile Secure Element Registration Form (using the latest form template) for your existing approved product to chip_certification_chd@mastercard.com ; and cast@mastercard.com
2. If Functional testing is required a set of delta tests will be specified in a MEPS and on receipt of a successful Test Report a new TAS will be issued which will be valid for 3 years.
3. For CAST renewal evaluations Mastercard recommends the vendor should discuss booking a renewal slot with the security evlaution laboratory about 12 months prior to the CAST certificate expiry. The start time for the actual evaluation must be no earlier than 6 months prior to the CAST certificate expiry date. The CAST report can be reviewed up to 3 months prior to expiry so Mastercard recommend the report be submission around 4 months prior to the CAST certificate expiry
4. For CAST there are 2 options :

i. Refresh CAST : A full CAST evaluation is carried out (a maintained/valid PCN is required when the lab begin testing). If a favourable result is achieved a new CAST Certificate, with new issued date is granted and is valid for 3 years.

ii. Renewal CAST : If the PCN has not been maintained or has expired, and a further extension to the LoA/CCS is required, a delta evaluation may be performed leading to an extended CAST Certificate for 2 years from which a extended or new LoA/CCS can be issued. This extension process can be repeated for a maximum of 2 times.

5. In addition to 4i and 4ii above, the LoA/CCS for End-of-Life(EoL) (for a product which is being ramped down) can be requested. In this case no additional testing is required but CAST will consider the request taking into account any known field issues and current threats and if the review is successful a Restricted CAST Certificate(RMPCN) will be issued. The Restricted CAST certificate is for existing commitments only and the issuance quantity and customers are limited during the EoL period.. No new customers for the product are allowed and the LoA is valid for one year with no extension possible.

Contact

The Mastercard contact is chip_certification_chd@mastercard.com and cast@mastercardMastercard.com

Chapter 6 Post Approval Changes

You may want to obtain a LoA/CCS for a Secure Element that has similarities to a Secure Element for which Mastercard already issued a LoA/CCS. The new product should be registered for both CAST and functional testing to determine what testing will be required. As with any Secure Element product you will need a CAST Certificate and TAS to obtain a LoA/CCS. Please note that this section only describes the impact of changes with regard to functional testing. Mastercard will separately evaluate all changes with regard to their impact on CAST certification.

The M/Chip Mobile Secure Element Registration Form is used to register the product. In the form you should register the product with a unique Technical Product name and version and describe the changes with respect to the original Secure Element(quoting the Mastercard Registration Number). Additional supporting documentation in the form of architecture diagrams explaining the changes will often be required. Mastercard will determine the impact of the changes. Properties of the Secure Element that are not likely to be affected by the change(s) may not need to be tested again.

Mastercard will send you a response informing you about the testing you need to do in order to obtain an LoA or a CCS for your new Secure Element. The following responses are possible:

Standard Response	Consequence(s)
No Functional Testing Needed.	Mastercard registered new SE and determined that no additional functional testing is needed as a consequence of the change. LoA/CCS can be issued when the corresponding CAST Certificate is issued.
Full Functional Testing Needed	Mastercard determined that the change necessitates full functional testing in order to issue a LoA/CCS.
Full Application Testing Needed	Mastercard determined that the change necessitates full application testing in order to issue a LoA/CCS.
Regression Testing Needed	Mastercard determined that the change necessitates regression testing (Functional Testing only) in order to issue a LoA/CCS. The scope of the regression testing depends on the change. Mastercard will detail the required regression testing in a MEPS.
Performance Testing Needed	Mastercard determined that the change necessitates performance testing, in order to make sure that the performance of the Secure Element (including the M/Chip Mobile application) conforms to Mastercard's requirements.

Mastercard will make an individual assessment of every change. However, the following table gives an overview of the most common types of changes and the standard response that Mastercard expects to give in case of such a change.

Area	Change	Expected Standard Response
UICC form factor	e.g. from ID-000 to 3FF or 4FF	No Functional Testing
Chip hardware	New integrated circuit	Full Functional Testing
	Change in amount of available memory (hardware change)	No Functional Testing
	Change in amount of available memory (software change (1))	No Functional Testing
Chip OS	Minor OS changes (2)	Regression Testing
	Major OS changes (2)	Full Functional Testing
M/Chip Mobile application	M/Chip Mobile application related library update (3)	Regression Testing
	M/Chip Mobile application update	Full Application Testing
	Changing application (ELF) location from EEPROM to ROM or vice versa	Performance Testing
Contactless Protocol	Change in default Contactless Parameters	No Functional Testing

(1) e.g. when during the boot procedure of the chip software settings limit the addressable memory space.

(2) Mastercard reserves the right to determine whether a given OS change is minor or major. However, Mastercard will base its determination partly on self-declaration by the Secure Element Vendor, for example as evident from the increase in the major or minor version numbers. In any case, the following kinds of changes are most likely to be viewed as major OS changes:

- Any changes meant to patch a known security problem in the Secure Element.
- Any changes to APIs that may be used by the M/Chip Mobile application.

(3) e.g. a cryptographic library used by the application to calculate a cryptogram**.**

The above table is offered as guidance only to aid the Vendor in planning for approval of a delta product. Deatiled assessment of the testing required will be made after the Registration Form and any supporting documents are received.

Appendix A Checklist

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.	□	M/Chip Mobile License Agreement	A M/Chip Mobile License Agreement can be obtained from Digitallicensing@mastercard.com
3.	□	CRI License	Each IC Vendor is required to hold a valid CRI license and should contact CRI directly to sign a license if they do not already hold such a license.
4.	□	Book Functional Testing	The Vendor will need to book a test slot at a Mastercard accredited Test Laboratory.
5.	□	Register for Approval (submit Registration Form)	Latest Secure Element Registration Form can be obtained from https://mobilepartner.mastercard.com/documentation.html#4
6.	□	Mobile Evaluation Plan Summary (MEPS)	The Mobile Evaluation Plan Summary (MEPS) will be provided by Mastercard once the completed registration form has been reviewed.
7.	□	Send Samples for Testing	The Vendor will need to send personalized samples to an accredited Test Lab for testing.
8.	□	Receive Functional Test Report	Once testing has been completed the Test Lab will provide a test report to the Vendor.
9.	□	Receive TAS	The Test Assessment Authority will issue a Test Assessment Summary with unique reference number.
10.	□	CAST Certificate	The Vendor must have a CAST certificate for the product being submitted for approval.
11.	□	Request Approval (send CAST ref, TAS ref)	Once the Vendor has received the TAS, CAST reference and has all the required pre-requistes approvals in place a formal request for approval can be made by contacting Mastercard
12.	□	Receive LoA/CCS	If the product meets all requirements a LoA/CCS will be granted.

Appendix B Frequently Asked Questions about Secure Element Approval

The following is a list of frequently asked questions.

I have an approved SWP UICC product and I want to certify an eSE product with the same IC/OS/Applet combination?

Please submit a completed registration form for the eSE product requesting inheritance from the original SWP UICC product. To describe the changes please also supply detailed documentation (e.g. platform architecture) describing the changes and the interfaces supported in the eSE product.

I have an approved SWP UICC product and I want to certify a variant product for a specific MNO?

Please submit a completed registration form for the new SWP UICC product requesting inheritance from the original SWP UICC product. Please supply documentation describing the changes made for the MNO variant.

I have an approved SE product and I want to certify a new version of the M/Chip Mobile applet on the same platform?

A new applet will be treated as a new product. Please submit a completed registration form for the product.

I have an approved M/Chip Mobile applet on a particular platform and I want to certify the same M/Chip Mobile applet on a different platform?

Each combination of Applet/OS/IC is treated as a new product. Please submit a completed registration form for the product.

I want to request a Renewal for a SE product, do I need to update the approvals of pre-requites e.g. GP. PPSE?

For platforms already deployed in the field no updated approval of the pre-requites is required. Please refer to the relevant Application Note.

Appendix C 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.
eSE	embedded Secure Element
EoL	End of Life
FESE	Fully Encapsulated Secure Element
GVCP	Global Vendor Certification Program
IC	Integrated Circuit
ICCN	Integrated Circuit Certificate Number
LoA	Letter of Approval
MEP	Mobile Evaluation Plan (issued by Test Lab)
MEPS	Mobile Evaluation Plan Summary (issued by Mastercard)
MNO	Mobile Network Operator
MPCN	Mobile Payment Certificate Number
MVP	Mastercard Vendor Program
NFC	Near Field Communications
OCS	Online Capture System
OS	Operating System
PLI	Product Liability Insurance
SE	Secure Element
SWP	Single Wire Protocol
TAS	Test Assessment Summary
TDN	Technical Deviation Notification

Acronym	Meaning
TSM	Trusted Service Manager
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 M/Chip Mobile.
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 M/Chip Mobile applet conform to the Mastercard security requirements.
Component	Any product, part or combination of parts used in a M/Chip Mobile implementation (e.g. mobile device, secure element)
Debug Testing	Early functional evaluation of a M/Chip Mobile Secure Element to obtain an indication whether or not it will pass formal testing.
Formal Selective Testing	Functional evaluation of a M/Chip Mobile 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 M/Chip Mobile 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.
Inheritance	This is the process by which one Secure Element (variant) can inherit some or the entire test results of another Secure Element (registered or approved). The amount of test results that can be inherited depends on the similarity between the two SEs. This can help reduce the time and cost of approving the variant.

Term	Meaning
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 Mastercard accounts 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.
MPCN	Mobile Payment Certificate Number - an individual reference number to confirm the M/Chip Mobile application as well as the secure element on which it runs has successfully completed the CAST evaluation process
NFC Mobile Device	Any mobile phone, smartphone, tablet or consumer electronics device that includes NFC functionality with an embedded or add-on secure element and can be used as part of a M/Chip Mobile 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.
M/Chip Mobile Formal Type Approval	The umbrella term for all the evaluations and review processes and outputs relating to the approval of a M/Chip Mobile product. The final output of this group of processes is the Test Assessment Summary and Letter of Approval (LoA).
M/Chip Mobile - Letter of Approval (LoA)	Acknowledgement by Mastercard that the Secure Element to be used as part of any M/Chip Mobile implementation has demonstrated compliance to all the M/Chip Mobile requirements. This means it can be used by issuers with other approved components.
Payment Application	The software implementation of the M/Chip Mobile Specification within a secure element e.g. residing on a secure UICC, MicroSD or embedded secure element covering the requirements of the M/Chip Mobile specification.
PCN	Platform Certificate Number - Security Compliance Certificate granted to an approved Platform including the Operating System and the Integrated Circuit.
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 Authority	A review authority qualified to review a Test Report and issue a TAS. This can be a qualified expert at the Test Lab or a Mastercard expert.
Test Assessment Review	The Test Assessment Authority 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.
Test Assessment Summary (TAS)	A formal summary document containing assessment of the tests conducted on the Secure Element.

Term	Meaning
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 M/Chip Mobile products.
Variant Secure Element	This is a Secure Element that is similar to an already registered or approved M/Chip Mobile Secure Element where the differences are limited to form factor, operator or market specific additional applets, commercial name etc.