MasterCard
NFC Mobile Device
Approval Guide v2.0

30 July 2015

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

Table of Contents

Chapter 1   Introduction

This section provides an overview of the approval process for MasterCard contactless Near Field Communications mobile device implementations.

_

About MasterCard contactless mobile implementations

MasterCard has developed a comprehensive approval process for MasterCard contactless mobile implementations. This process enables world-wide interoperability as well as quality and reliability assurance at acceptable levels of time and cost.

Device manufacturers must follow the process to obtain approval for a Near Field Communications mobile device (with embedded or removable SE or supporting HCE) intended for use in a MasterCard contactless mobile implementation residing in a SE or based on a MasterCard Cloud Based Payment (MCBP) solution. Completing this process allows NFC mobile device manufacturers to demonstrate conformity to MasterCard contactless requirements.

Device manufacturers must also follow post-approval processes to maintain MasterCard approval of their devices.

MasterCard contactless NFC Device Assembly

The Assembly is the payment device made up of all the necessary components that enable a contactless transaction to take place when the device is placed in the payment reader's field. Depending on the architecture, this can range from being a single integrated device, to a combination of separate components that are developed and commercialized by multiple vendors.

The individual components and their respective approval requirements are listed below.

- The Secure Element

    – The IC

    – The Operating System

    – The Payment Application

- The NFC Mobile Device

    – NFC mobile device with embedded SE and/or removable SE and/or HCE support

The Secure Element

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

The Integrated Circuit

In M/Chip Mobile compliant contactless payment implementations the payment assets and Payment Application must be stored and processed on an integrated circuit (IC). MasterCard requires all such ICs to be secure and has developed a thorough evaluation process to ensure conformance with the security requirements as defined by CAST which has been adopted by EMVCo as an industrywide standardized approach.

The Operating System

For the Payment Application to function correctly, and to provide suitable logical security measures, vendors typically develop optimized operating systems for their secure elements that are installed on the integrated circuit. Any such operating system must also be assessed for its security compliance level. This can be done using EMVCo platform approval process or MasterCard CAST process.

The Payment Application

To perform an M/Chip Mobile compliant payment transaction by a contactless interface a Payment Application is needed. M/Chip mobile specification enables Payment Applications to be developed for Near Field Communications mobile devices.

Payment applications are typically programmed in Java for Java Cards, but may take any other form so long as they comply with the M/Chip mobile Technical Specifications and MasterCard Security Requirements.

Payment applications must therefore undergo the CAST evaluation to be certified as compliant with MasterCard's security requirements, and must also be tested to ensure they comply with MasterCard's functional requirements.

NOTE

A Payment Application must be CAST certified on every operating system and integrated circuit on which it runs.

To perform an MCBP payment transaction by a contactless interface a software based Mobile Payment Application (MPA) is needed. The MCBP specification defines the requirements for the MPA.

The Near Field Communications Mobile Device

The three most common architectures for a Near Field Communications (NFC) mobile device in a MasterCard contactless mobile implementation are an NFC mobile device with an embedded SE, an NFC mobile device with a removable SE and an NFC mobile device with HCE support.

NFC mobile device with an embedded SE

The approval of this configuration depends on the successful testing of the device's contactless module as well as successful CAST and functional evaluation of the embedded secure element with the payment application.

NFC mobile device with a removable SE

The approval of this configuration depends on the successful testing of the device's contactless module. The approved NFC mobile device can only be used with an approved removable SE. The removable SE which can be an SWP UICC or MicroSD is approved as a standalone component for use with any approved NFC mobile device.

NFC mobile device with HCE support

The approval of this configuration depends on the successful testing of the device's contactless module. The approved NFC mobile device can only be used with an approved MPA.
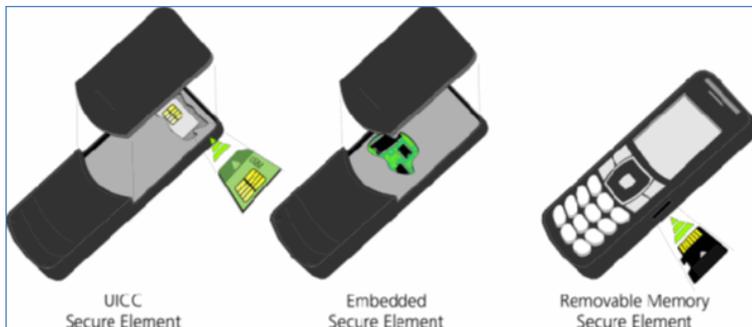
The Contactless Features enable the contactless communication between the Payment Application and the payment terminal. It will typically consist of three key components:

- An NFC chip that is an IC designed to perform the digital and analog signal processing

- An antenna that enables the RF communication with the payment terminal

- A hardware layer whose role is to adapt the NFC chip to the specific antenna in a specific mobile device

Who Uses the MasterCard contactless mobile Approval Process?

Ultimately the issuer and mobile operator must ensure that all components in any implementation of MasterCard contactless have been fully evaluated and have been approved. In the case of an SE based solution, issuers and mobile

operators will rely on Trusted Service Managers (TSMs) to correctly manage the provisioning and personalization process such that personalization requests where at least one component is not approved are blocked.

This information is designed primarily for mobile device manufacturers, but also includes a broader audience (such as TSM's, Mobile Network Operators (MNOs) and Issuers) as these other members of the MasterCard contactless mobile ecosystem must be aware of the process, its outcome, and importance.

This document will guide the device manufacturer (or any entity that wishes to submit a product for approval on their behalf) through the process by defining formal sub-processes and steps.

When Do I Use the MasterCard contactless mobile Approval Process?

Use the MasterCard contactless mobile approval process in the following situations:

- To approve a Near Field Communications (NFC) mobile device designed for use in a mobile implementations of MasterCard contactless.

- If any changes are made to a MasterCard approved NFC mobile device such as changes to the NFC chipset (hardware or firmware), mobile device firmware, NFC antenna, casing material and any other changes that could impact the behavior of the mobile payment implementation on the mobile device

- Renewal of approval of NFC Mobile Device because an LoA is due to expire

NOTE

Only changes to components relating to the mobile payment capability of the NFC mobile device will be seen as changes requiring resubmission for approval, as these changes will affect the contactless communications with contactless payment readers.

How is the MasterCard contactless mobile Approval Process Used?

The process relating to MasterCard contactless mobile implementations tests and evaluations is driven by the suppliers of components or the services they provide for use in a MasterCard contactless mobile implementation.

Letters of Approval are issued to the mobile device manufacturer or other entity that is submitting the product for approval.

It is the responsibility of the mobile device manufacturer (or any other entity submitting the product for evaluation on their behalf) to initiate the actions required to achieve approval or renewal of an existing approval.

To manage the process, the submitting entity appoints a project manager as the point of contact with MasterCard and the Testing Laboratories.

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

Chapter 2   MasterCard NFC Mobile Device Approval Process

This section gives a high level overview of the three key stages in the approval process: Planning and Administration Phase, Testing and Evaluation Phase, and Assessment and Approval Review Phase.

MasterCard NFC Mobile Device Approval Processes and Relationships

The individual MasterCard NFC mobile device approval processes and their relationships are in the flow.
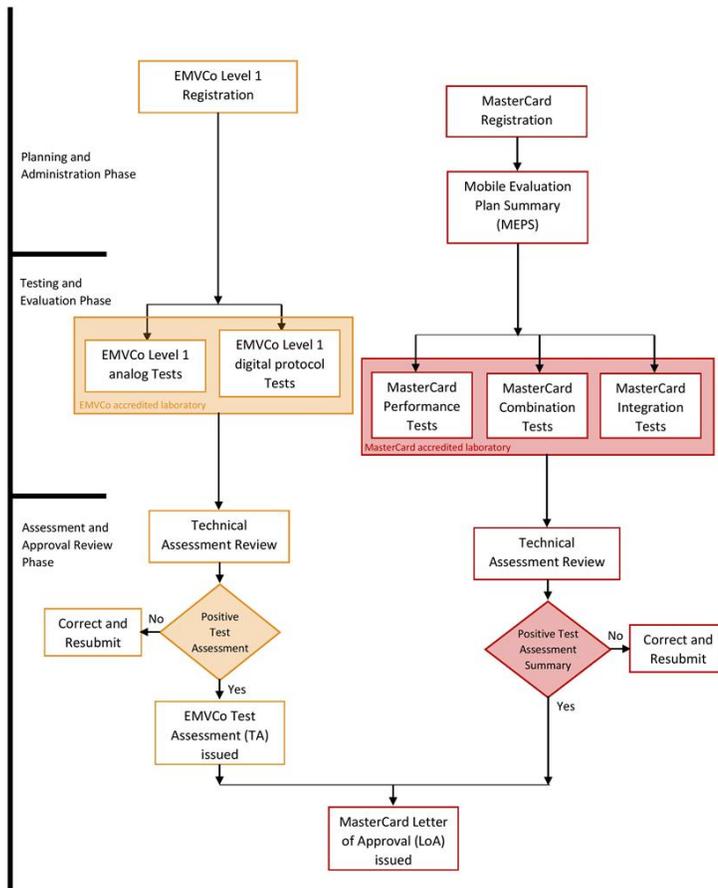
Process Key Stage 1: Planning and Administration Phase

All vendors who plan to submit their NFC mobile device for MasterCard approval must sign a MasterCard Mobile Device Testing Agreement.

Request this document by sending an e-mail to mobilepartner@mastercard.com.

Product Development Cycle

Before a Near Field Communications (NFC) mobile device is registered for formal testing, MasterCard recommends the vendor performs debug testing at an EMVCo accredited laboratory (for Level 1 tests) and/or a MasterCard accredited test laboratory for Integration, Combination and Performances tests. 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 the mobile device with MasterCard. MasterCard can review the results of debug testing and provide feedback.

Vendors can contact MasterCard's Device Approval team (Chip_Certification_Support@mastercard.com) for this type of support. This will help ensure the NFC mobile device complies with the various test requirements and reduces unnecessary costs and time delays in bringing NFC mobile devices to market.

Registration Process for Mobile Device Evaluation

The first administrative process in Key Stage 1 is the Registration Process during which the vendor registers their Near Field Communications (NFC) mobile device for evaluation by completing a form that captures information about the vendor, their key point of contact, and the product itself (including all relevant components and features).

Before being registered with MasterCard, the device must be registered for EMVCo Level 1 testing process. An EMVCo Level 1 Test Assessment is required as a pre-requisite by MasterCard for granting a Letter of Approval (LoA) to the device.

EMVCo ICS form

To register the device with MasterCard, the vendor must submit the EMVCo Implementation Conformance Statement (ICS) form available on EMVCo website (www.emvco.com). The EMVCo ICS form must be filled in correctly and validated by EMVCo before submitting the form to MasterCard. Only EMVCo ICS validated by EMVCo and to which an EMVCo registration number has been assigned will be accepted by MasterCard.

HCE Questionnaire

In addition to the EMVCo ICS form, if the device supports HCE, vendor must submit the HCE questionnaire available on www.mastercard-mobilepartner.com.The HCE Questionnaire must be filled in correctly before submitting it to MasterCard.

MasterCard's technical teams review the information in the forms and make decisions on what type of tests must be performed by an accredited lab. The required tests, number of device samples and accompanying instructions regarding the next steps are formally summarized in the Mobile Evaluation Plan Summary (MEPS) issued to the vendor.

NOTE

An NFC Mobile Device supporting both Embedded SE and Removable SE configurations must be registered separately with MasterCard for approval of each configuration.

Allow 5 working days for the processing of the registration form and issuance of the MEPS.
The MasterCard contact is chip_certification_chd@mastercard.com.

Process Key Stage 2: Testing and Evaluation Phase

The Process Key Stage 2: Testing and Evaluation Phase includes preparation for testing and actual testing.

EMVCo Level 1 Testing

Vendor must follow the EMVCo Mobile Product Level 1 Type Approval Administrative Process for which documentation is available on the EMVCo website (www.emvco.com) in order for the device to be granted an EMVCo Level 1 Test Assessment.

All questions related to the EMVCo process regarding sample preparation, test scope, or any other topic must be directed to EMVCo. EMVCo contacts can be found on the EMVCo website (www.emvco.com).

Through the EMVCo Mobile Product Level 1 process the NFC mobile device undergoes two specific tests to ensure that the device complies with the EMV Contactless Specifications for Payment Systems – Book D – EMV Contactless Communication Protocol Specification. The two tests are: analog and digital protocol.

Preparation for MasterCard Testing

Preparation for MasterCard testing includes booking a test slot at a MasterCard accredited test laboratory and providing the mobile device samples.

Booking a Test Slot at the Laboratory

The vendor must provide the registration forms and MEPS to a MasterCard accredited lab and agree to relevant contracts and schedules. The Accredited 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 one week for performing the tests.

MasterCard recommends that vendors provisionally book test slots 4 weeks before start of testing. Test slots can be provisionally booked before an MEPS is issued by MasterCard by providing the lab with information about the device and assuming that MasterCard will require all tests to be run on the device.

Mobile Device Samples

Before testing can begin the vendor must provide mobile device samples to the lab. The samples must be production quality where all features are enabled and can be tested. For mobile devices with an embedded secure element, the laboratory will provide the mobile device vendor with configuration requirement of the applet for each sample. For mobile devices with a removable secure element such as SWP UICC or MicroSD, three mobile device samples must be provided to the laboratory. This is specified in the MEPS issued by MasterCard.

The labs use reference UICCs with the M/Chip Mobile applet for approval of all NFC mobile devices that work with an SWP UICC as well as using non SWP UICC for devices supporting HCE.

For mobile devices with an embedded secure element, the lab will request the vendor to provide the samples needed for approval where the applet on the secure element needs to be configured differently for each test run on the device.

Testing Near Field Communications Mobile Devices

A Near Field Communications mobile device (independently of the Secure Element used) undergoes three specific tests to ensure that the device complies with the MasterCard requirements. The three tests are: Performance, Combination, and Integration.

The multiple samples provided enable these tests to be performed in parallel. Additionally, if a sample used to perform a particular test results in a failure; the lab can re-try the test with another sample to determine if the failure is caused by an issue with a particular sample or all samples. The re-test could result in extra cost for the vendor (to be determined by 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. MasterCard will review the test report in the final phase.

NOTE

Testing of an NFC mobile device with an embedded SE must not start until the embedded SE has been issued with a CCS indicating it has successfully passed MasterCard functional and security testing.

Process Key Stage 3: Assessment and Approval Review Phase

The Process Key Stage 3: Assessment and Approval Review Phase includes review of test results and approval of the Near Field Communications (NFC) mobile devices.

EMVCo Test Assessment

Following EMVCo Level 1 testing according to the EMVCo Mobile Product Level 1 Type Approval Administrative Process, the NFC mobile device will be issued an EMVCo Level 1 Test Assessment by EMVCo if successful. The EMVCo Test Assessment must be submitted to MasterCard as evidence of compliance with the EMV Contactless Specifications for Payment Systems – Book D – EMV Contactless Communication Protocol Specification.

Review of Mobile Device MasterCard Test Results

Once MasterCard has received the Test Report for the MasterCard tests requested in the MEPS, 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 Device under Test (DUT) test assessment will be summarized in a formal statement from MasterCard called the Test Assessment Summary (TAS) that is issued to the vendor.

Approval of NFC Mobile Devices with Removable SE

If the TAS shows the DUT has passed all the required tests and the EMVCo Level 1 Test Assessment has been submitted to MasterCard, a Letter of Approval (LoA) is issued to the vendor thus formally confirming compliance of the NFC mobile device with all the MasterCard testing requirements. The LoA for an NFC Mobile Device with removable SE has a validity period of three years from the date of the Test Assessment specified in the TAS.

As a rough guideline, allow one week for reviewing of the final report and issuance of the TAS and LoA if no issues are identified during testing.

Approval of NFC Mobile Devices with Embedded SE

Approval of NFC mobile devices with embedded SEs is dependent on the following MasterCard evaluations.

1. A TAS is issued for the DUT confirming the device has passed all the required tests specified in the MEPS issued by MasterCard and the EMVCo Level 1 Test Assessment has been submitted to MasterCard.

2. The embedded SE and applet have a CAST Certificate confirming compliance with the MasterCard security requirements. It is the responsibility of the embedded SE vendor to submit the embedded SE and applet for CAST evaluation. This can be done independently of the testing of the NFC Mobile Device. The results can be inherited by any NFC Mobile Device using that embedded SE/applet combination.

3. A TAS is issued for the SE and applet confirming compliance with the M/Chip Mobile functional requirements. It is the responsibility of the embedded SE/applet vendor to submit the embedded SE and applet for functional testing. This can be done independently of the testing of the

NFC Mobile Device. The results can be inherited by any NFC Mobile
Device using that embedded SE/applet combination

.

Chapter 3   Planning and Administration Phase

This section outlines the Planning and Administration Phase processes.

Product Development Cycle

The Product Development Cycle represents a vendor's internal development procedures for a MasterCard contactless product or component.

Purpose

Vendors may use the services of EMVCo and/or MasterCard accredited Laboratories to assist with product development and testing.

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 pre-validation 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 usability, 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 mobile device under development with the MasterCard requirements.

Contacts

The MasterCard contact during the Product Development Cycle is mobilepartner@mastercard.com.

MasterCard documentation that is relevant before and during the Product Development Cycles is also available from www.mastercard-mobilepartner.com.

Registration

Registration or Renewal Registration is designed to register full details of an NFC mobile device.

Purpose

1. Provide information about a new NFC mobile device and all component parts and features relevant to the testing process.

2. Register a variant or derivative NFC mobile device similar to an already registered or approved mobile device. It is the vendor's responsibility to provide information in the registration form describing all the differences between the variant mobile device and the already registered/approved device. MasterCard will use this information to determine the tests (if any) to be performed on the variant device to approve it.

3. Provide information about changes to an already approved NFC mobile device. It is the vendor's responsibility to provide information in the registration form describing all the changes to the approved device for MasterCard evaluation.

4. Register an NFC mobile device for which renewal of approval is required because of an expiry of a LoA.

It is the vendor's responsibility to provide MasterCard with all the relevant information for MasterCard to determine which tests (if any) to run and passed for approval of the NFC mobile device and issue the appropriate MEPS document to the vendor.

Output

The result of this process is a Mobile Evaluation Plan Summary (MEPS) containing the list of tests to be performed on the registered product as well as a list of accredited labs the vendor can use for performing the testing. In some cases no additional testing will be required and an approval based on inheritance will be granted.

Requirement Level

The process is mandatory for all approval requests.

Procedures

1. The vendor completes all the fields in the appropriate registration forms (ie the EMVCo Level 1 ICS form and the MasterCard HCE Questionnaire when applicable).

2. The forms are submitted no later than two weeks before the start of formal testing.

3. MasterCard reviews the information in the submitted form.

4. Based on the information in the received forms the set of tests to be performed on the registered product will be identified.

5. MasterCard will summarize all the tests and give a clear set of instructions to the vendor in the form of an MEPS document which will be issued to the vendor.

NOTE
MasterCard may contact the designated contact point referenced in the registration form during the registration review phase if any information is

unclear or missing to ensure that the Mobile Evaluation Plan Summary when issued by MasterCard is correct.

Contacts

The MasterCard contact is chip_certification_chd@mastercard.com.

Chapter 4 Testing and Evaluation Phase

This section outlines the Tests and Evaluation Phase Processes.

Preparation for Testing

Preparation for testing includes planning for testing. Information in this section is only related to MasterCard testing. For information regarding EMVCo Mobile Product Level 1 Type Approval Administrative Process, please contact EMVCo.

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 accredited lab at least 4 weeks before the start of formal testing.
- Mobile device 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 registration forms and MEPS are provided to the lab before the start of testing.

Output

The vendor secures that the testing of the NFC mobile device will start on time according to the vendor's plans.

Requirement Level

The process is mandatory.

Procedure

The procedure follows:

1. The vendor contacts a MasterCard accredited lab at least 4 weeks before the planned start of formal testing to secure a test slot. This can be done before the device is registered with MasterCard (registration forms submitted/MEPS issued) by providing the lab with information about the device and assuming all tests will be run for approval of the device.

2. Once the mobile device is registered with MasterCard, the vendor must provide the registration forms and MEPS to the lab. If after registering the device with MasterCard and before the testing starts, the device hardware and/or software changes, the vendor must submit updated registration forms to EMVCo and MasterCard before testing starts as the required tests could change depending on the changes made to the device. The same device configuration must be used for MasterCard testing and EMVCo Level 1 testing. Therefore the vendor may also need to submit updated EMVCo ICS to EMVCo. The vendor must provide the updated registration forms and MEPS to the test lab for start of testing. If the change to the device is minor, MasterCard may instruct the lab to start the testing in parallel with issuance of the updated MEPS. Vendors must ensure the lab has the latest registration forms and associated MEPS as they will both be included in the

final report issued by the lab to show the mobile device configuration that was tested.

3. The vendor provides the lab with the required samples for performing the testing. The samples must match the information in the registration forms used to register the product with MasterCard and the samples device SW version must be identical to the samples used for EMVCo Level 1 testing. All samples must be production quality and are exactly the same as the devices planned to be launched to the market, that is, all features are implemented and working.

NOTE

MasterCard reserves the right to reject any test report received from the vendor where the mobile device samples tested do not match the details in the registration forms used by MasterCard to issue the MEPS.

Contacts

The MasterCard contact is chip_certification_chd@mastercard.com.

Testing

The purpose of the formal testing phase is to demonstrate that the DUT conforms to MasterCard contactless requirements for mobile implementations. Information in this section is only related to MasterCard testing. For information regarding EMVCo Mobile Product Level 1 Type Approval Administrative Process, please contact EMVCo.

Purpose

- **Performance Requirements—**The DUT is tested to determine if it complies with the current performance requirement (specific transaction time for a MasterCard contactless transaction and according to MasterCard contactless – Device Approval Application Note #3).
- **Combination Requirements—**The DUT enters the operating volume of of widely deployed MasterCard contactless terminals and is positioned at different distances and offsets from the center of each terminal to perform transactions. The mobile device is tested in around 30 different positions against each payment terminal based on offset from center and distance from 0 to 4 cm. Although the tests are performed for distances up to 4 cm, currently for approval of the DUT, MasterCard only considers the results for 0 to 2 cm. The results for 2 cm to 4 cm are for information only. A pass rate of around 70% against each payment terminal for 0 to 2 cm is required.
- **Integration Requirements—**The DUT works correctly with a number of widely deployed MasterCard contactless terminals. The device is tested in around 20 different positions against each payment terminal based on offset from center and distance from 0 to 1 cm. This is the final stage in ensuring interoperability. The DUT must be able to conduct MasterCard contactless transaction against all the payment terminals. The pass criteria is 15 out of 20 pass transactions.

NOTE

MasterCard does not publish the test cases that will be run on a mobile device. This is because MasterCard does not want vendors to make a mobile device that only passes those test cases. Vendors wishing to ensure their device will pass formal testing are encouraged to ask the lab to run some or all of the formal tests in debug mode to determine how well the device performs and if any issues need to be resolved.

Output

The output of the Testing process is a Test Report.

Requirement Level

The process is mandatory.

Procedure

The procedure is as follows:

1. The Test Laboratory performs all the tests requested by the MEPS issued for the mobile device. For new NFC mobile devices all three tests will be requested in the MEPS. For variant or derivative NFC mobile devices, MasterCard may only request a subset of the three tests to be performed by allowing the device to inherit the test results for the remaining tests from the previously registered/approved version of the NFC mobile device.

2. If a sample used to perform a particular test results in a failure; at the request of MasterCard or the vendor the lab can retry the test with another sample to determine if the failure is due to an issue with a particular sample or all samples.

3. During the testing, the lab will report the progress to MasterCard on a regular basis.

4. Once testing is completed the lab issues a Test Report.

Contacts

The MasterCard contact is chip_certification_chd@mastercard.com.

Chapter 5   Assessment and Approval Review Phase

This section outlines the Review and Approval processes.

Review of Mobile Device Test Results

The purpose is to review the test results in the test report generated by the lab to determine if the NFC Mobile Device has passed all the tests requested in the MEPS issued by MasterCard.

Output

A TAS is issued by MasterCard summarizing MasterCard's assessment of the test results.

NOTE

A TAS issued by MasterCard may show the device has passed all the tests even if the test report from the lab shows the DUT has failed one or more test cases. This is because MasterCard may decide the failure is minor and should not affect approval. The TAS will contain a note regarding such cases.

Requirement Level

This process is mandatory.

Procedure

The procedure is:

1. MasterCard reviews the test report received
2. If any further testing or investigation is required, MasterCard will inform the vendor and will send a request to the laboratory. It is the responsibility of the vendor to agree to the schedule and any additional cost with the laboratory for the additional activities.
3. MasterCard will then review the results of all the tests (Technical Assessment Review) and a TAS is issued referencing the complete set of test results and all the relevant technical information relating to the DUT as specified in the registration form.
4. If the outcome of the MasterCard review is negative because of critical failures during testing, the submitting entity will be informed. They may choose to fix the discovered issues and re-register the modified mobile device for formal testing.

Contact

The MasterCard contact is chip_certification_chd@mastercard.com.

Approval of NFC Mobile Devices with Removable SE

The purpose is to formally confirm compliance of the NFC Mobile Device supporting removable SE with the M/Chip Mobile technical and functional requirements. Approval of the removable SE is performed independently of the NFC mobile device. See Mobile MasterCard Secure Element Approval Guide.

Output

A LoA is issued that acts as formal confirmation to the submitting entity of a given product's conformity to all relevant requirements.

Requirement Level

The process is mandatory.

Procedure

The procedure follows:

1. Once a successful TAS has been issued and an EMVCo Level 1 Test Assessment submitted to MasterCard, MasterCard's Approval Authority will then issue a LoA to the submitting entity (listing the technical details of the product and relevant components as well as any restrictions that may apply).
2. The LoA for an NFC Mobile Device with removable SE has a validity period of three years from the date of the Test Assessment specified in the TAS.
3. Once a LoA has been issued, the NFC Mobile Device vendor name and commercial name will be published on the MasterCard Mobile Partner Program website www.mastercard-mobilepartner.com.

Contacts

The MasterCard contact is chip_certification_chd@mastercard.com.

Approval of NFC Mobile Devices with Embedded SE

The purpose is to formally confirm compliance of the NFC Mobile Device supporting embedded SE with the M/Chip Mobile technical, functional, and security requirements.

Output

A LoA is issued that acts as formal confirmation to the submitting entity of a given product's conformity to all relevant requirements.

Requirement Level

The process is mandatory.

Procedure

Once a successful TAS has been issued for the NFC Mobile Device with eSE and an EMVCo Level 1 Test Assessment submitted to MasterCard, approval of the device depends on the following MasterCard evaluations:

1. The embedded SE and applet vendor completes the MasterCard security evaluation and provides MasterCard with a CAST certificate confirming compliance with the MasterCard security requirements. This can be done independently of the testing of the NFC Mobile Device with embedded SE.

2. The embedded SE and applet vendor completes the MasterCard functional testing of the applet and SE and is issued with a successful TAS showing compliance with the MasterCard functional requirements. This must be done before testing of the NFC Mobile Device with embedded SE.

3. If the above evaluations are all successful, MasterCard's Approval Authority will then issue a LoA to the submitting entity (listing the technical details of the product and relevant components as well as any restrictions that may apply). The LoA for an NFC Mobile Device with an embedded SE has the same expiry date as the CCS issued for the embedded SE/applet.

4. Once a Letter of Approval has been issued, the NFC Mobile Device vendor name and commercial name will be published on the MasterCard Mobile Partner Program website: www.mastercard-mobilepartner.com.

Contacts

The MasterCard contact is chip_certification_chd@mastercard.com.

Chapter 6   Post Approval Changes

After approval is achieved, a need could arise for the NFC Mobile Device vendor to make some changes to the approved device. Changes that may need to be made and actions required from the vendor to maintain MasterCard approval of the NFC device include device firmware/operating system upgrades, NFC chip firmware changes, hardware changes, and changes to the embedded SE. As the MasterCard approval process leverage the EMVCo Level 1 process, vendors may also be required to maintain the EMVCo Level 1 assessment of the NFC device and should consult with EMVCo approval process to ensure this.

Device Firmware/Operating System Upgrade

If upgrading the firmware or operating system of an already approved NFC Mobile Device does not cause any change to the NFC related parts, the NFC Mobile Device vendor can perform the upgrade without prior notification to MasterCard. If however, the upgrade will cause changes to the NFC related functionality, the vendor will need to inform MasterCard before the approved NFC devices in the field are upgraded and share information about the changes so that MasterCard can review and decide if any further testing is needed.

An example of an upgrade that will affect device approval is a device approved for SWP or eSE that is upgraded to an OS release that supports HCE. This will require the device to be tested to ensure the HCE implementation will work correctly when used for mobile payment.

NFC Chip Firmware Change

All NFC chip vendors are required to test new firmware releases and share the release notes and test results with MasterCard before issuing the new firmware to NFC Mobile Device vendors for upgrading MasterCard approved NFC Mobile Devices. MasterCard maintains a list of qualified NFC chip firmware for NFC chips having regular updates. This list is available on www.mastercard-mobilepartner.com.

If the new firmware has not been tested by the NFC Chip vendor, the mobile device vendor willing to implement this new firmware must register the device with MasterCard for delta testing.

Based on the test results, MasterCard will review the new firmware and decide whether:

1. The firmware can be approved and rolled out to other MasterCard approved NFC devices without further testing. In this case, the FW qualified by MasterCard should appear on mobile partner website.

2. The firmware can be approved but any MasterCard approved NFC devices planned to be upgraded to the new firmware will need to be registered with MasterCard for delta testing to confirm the mobile payment function is not affected by the changes introduced by the new firmware. Depending on MasterCard assessment, registration with EMVCo for Level 1 testing may also be required for upgrade.

A mobile device vendor must not upgrade the NFC chip firmware of a MasterCard approved NFC mobile device unless the NFC chip vendor can confirm the new firmware has been qualified by MasterCard and MasterCard has agreed no further testing is needed before performing the upgrade. Failure to follow this process will result in the LoA for an approved NFC Mobile Device to be withdrawn.

Hardware Change

If any NFC related hardware such as NFC chip or NFC antenna as well as other hardware such as casing supported by the approved NFC Mobile Device are planned to be changed, the vendor must inform MasterCard by submitting a registration form containing details of the planned changes. MasterCard will review the registration form and inform the vendor if further testing is needed.

Changes to the Embedded SE

An NFC Mobile Device with embedded SE is only approved for use with the embedded SE and applet versions specified in the registration form for the mobile device and indicated in the subsequent LoA issued for the device.

Follow the process below to change an approved applet, change an OS running on the embedded SE, or add a new applet to the embedded SE of an already approved NFC mobile device.

1. **Adding a new M/Chip Mobile Applet to the embedded SE**—In this case the new applet and embedded SE will need to be submitted for CAST (security) testing as well as MasterCard functional testing. This process can take up to four months depending on the complexity of the product.

2. **Adding a third party applet to the embedded SE**—This includes both additional payment applications for other payment networks as well as transit, loyalty and network operator related applications:

   a. **CAST**—When an embedded SE and applet are approved by MasterCard, they are approved along with a formal guidance document that specifies the actions that must be performed in order to maintain approval of the embedded SE. The guidance document also lists the actions that must be taken when adding a 3rd party applet to the embedded SE. Vendors should obtain the guidance document from their eSE provider.

   b. **Functional Evaluation**—For any product using a Flash-based IC, MasterCard approves the OS (including all libraries) and the payment applet. When using the Flash technology, the vendor is allowed to add any applet without notifying MasterCard as long as the software (OS and libraries, payment applet) is not modified (no code change, no new compilation of the code even unchanged) and additional applets do not have any impact on the behavior of the payment applet, namely: they do not share any data with the payment applet, they do not act as a filter, they do not require a different protocol configuration of the product, and they are not selected by default.

3. **Changing an Approved M/Chip Mobile Applet or the embedded SE OS of an already approved NFC Mobile Device**—In this case the applet and embedded SE will need to be submitted for CAST (security) testing as well as MasterCard functional and performance testing. This process can take up to four months depending on the complexity of the product.

Appendix A   NFC Mobile Device Checklist

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

NFC Mobile Device Checklist

To assist any entity wishing to submit an NFC mobile device for testing and approval, the following checklist 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.

1.	☐	Complete the EMVCo ICS form.	Download the latest EMVCo ICS form from EMVCo website (www.emvco.com).
2.	☐	Submit the EMVCo ICS form to EMVCo for Level 1 testing.	Ensure all fields are filled in correctly and submit the completed registration form to EMVCo.
3.	☐	Book a test slot at an EMVCo accredited test laboratory.	The list of EMVCo accredited test laboratories is available on EMVCo website (www.emvco.com).
4.	☐	The EMVCo accredited test laboratory issues a test report once Level 1 testing is completed.	The test report must be provided to EMVCo for review. If successful, EMVCo will issue an EMVCo Level 1 Test Assessment.
5.	☐	Complete the MasterCard HCE Questionnaire.	Download the latest HCE Questionnaire form from the www.mastercard-mobilepartner.com website.
6.	☐	Submit the EMVCo ICS form validated by EMVCo and the MasterCard HCE Questionnaire to MasterCard.	Ensure all fields are filled in correctly and submit the completed forms to MasterCard (chip_certification_chd@mastercard.com).
7.	☐	Receive the Mobile Evaluation Plan Summary (MEPS).	An MEPS can only be issued once correctly completed EMVCo ICS and MasterCard HCE Questionnaire forms have been received. Every MEPS is specific to a submission
8.	☐	Book a test slot at a MasterCard accredited test laboratory.	The list of MasterCard accredited test laboratories is specified in the issued MEPS.
9.	☐	Provide the registration forms, MEPS and production quality samples to the test laboratory for tests.	The issued MEPS contains details regarding the number of samples needed for testing.
10.	☐	The MasterCard accredited test laboratory issues a test report once MasterCard testing is completed.	The test report must be provided to MasterCard for review.

| 11. | ☐ | Receive a Test Assessment Summary (TAS). | MasterCard will review the MasterCard test report as well as the EMVCo Level 1 Test Assessment and issue a Test Assessment Summary (TAS) which provides MasterCard's assessment of the test results. If the TAS indicates non-conformance with the requirements, corrective action will need to be taken and the mobile device will need to be re-registered for formal approval. |
| 12. | ☐ | Receive LoA. | If all tests have been successfully completed and a positive TAS has been issued the final stage is the receipt of the Letter of Approval. |

Appendix B Frequently Asked Questions about NFC Mobile Device Approval

This appendix contains a list of frequently asked questions and answers to cover any issues not already addressed by the other parts of the document.

Frequently Asked Questions about NFC Mobile Device Approval

The following is a list of frequently asked questions.

Do I have to register my NFC mobile device with EMVCo for L1 (Analog and Protocol) testing?

From 1st of May 2015, all SWP mobile devices have to be registered with EMVCo for L1 (Analog and Protocol) testing.

From 1st of October 2015, all embedded SE mobile devices will have to be registered with EMVCo for L1 (Analog and Protocol) testing.

Can I use MasterCard PayPass applet for EMVCo L1 testing of my eSE NFC mobile device?

For EMVCo L1 testing of and eSE NFC mobile device, a vendor will need to implement an applet running on the eSE based on the EMVCo applet requirements (see https://www.emvco.com/approvals.aspx?id=246) Bulletin n°7, Mobile Level 1 Test Applet Requirements.

Can an approved mobile device be sold to several Mobile Operators and in different markets without further approval?

MasterCard approval is global. Once a mobile device is approved it can be sold to any operator without further approval if no changes are made to the device that can affect the mobile payment feature of the device. For more information, see Post Approval Changes. If the device commercial name is changed to sell the device in a different market, the vendor should inform MasterCard by submitting an updated registration form so that MasterCard can update the database of approved devices to include the new name of the approved device and also publish the new commercial name on the Mobile Partner website.

If two similar devices are registered for MasterCard approval, will MasterCard require full testing to be done on both devices?

MasterCard will consider inheritance of test results for a mobile device if it is a variant model of another device. In the registration form a section is provided to allow vendors to indicate that a device being registered is a variant/derivative of another device by listing the differences between the two devices which will determine the amount of inheritance applied. Here are some examples of variant devices where inheritance can be applied by MasterCard:

- Two devices are the same except for radio support, that is, one device supports 3G and the other supports CDMA or one device supports Wi-Fi and the other does not. In this case MasterCard will request only require one of mobile device to be fully tested and the second mobile device would inherit all the test results for approval of both devices. MasterCard will issue a notification approval email for the inheriting device.

- Two devices have NFC antenna from different suppliers but both suppliers manufacturer the antenna according to the same antenna specification, the

same material is used and the antenna is integrated into the device by single entity. In this case MasterCard might only request one of mobile device to be fully tested and the second mobile device would inherit all the test results for approval of both devices. MasterCard will issue a notification approval email for the inheriting device.

- The chassis/casing is different between two devices where one device is made from different material or has different shape. In this case MasterCard will require more information before deciding how much inheritance if any can be applied.

- The features supported by the two devices are different. If the differences are not NFC related, approval should not require any additional testing and the mobile device can inherit the test results from the approved version of the device. The vendor will need to register the device with MasterCard and list the differences in the registration form. If feature differences are due to for example NFC peer-to-peer being implemented after a mobile device is approved which causes changes to the NFC stack MasterCard will require additional testing.

What is the difference between approval of a mobile device with an embedded Secure Element and a mobile device with a removable Secure Element (such as uses UICC/MicroSD)?

Although the tests run at the lab for mobile device with an embedded Secure Element are the same as those run on a mobile device that uses a removable Secure Element, approval of a mobile device with an embedded Secure Element also depends on the Secure Element and applet achieving MasterCard CAST (security) compliance (CAST certificate issued) as well as passing MasterCard functional testing (TAS issued for Secure Element/applet showing all tests are passed). Since the CAST certificate for an embedded Secure Element and applet will have duration of three years, the LoA issued for a mobile device using that Secure Element and applet will have the same expiry date as the CAST certificate. After 3 years the Secure Element and applet vendor can re-submit the Secure Element and applet for CAST approval and if successful, the CAST certificate will be extended by a further year. The LoA for a mobile device using that SE and applet will also be extended to match the new expiry date of the CAST certificate if:

- Any changes made to the SE and Applet can be implemented for all devices already in the market such as software download

- The mobile device passes any additional testing that maybe required to prove the SE/Applet changes have not adversely affected the mobile payment capability of the device.

This process can be repeated annually for a further two years after which the CAST certificate will expire as well as the LoA for the mobile device and no new accounts can be provisioned for that mobile device.

What is the duration of approval for a mobile device?

The best duration for approval is as follows:

- Mobile device with an embedded Secure Element

    – Registration of mobile device with MasterCard and issuance of MEPS (one week from reception of a correctly completed registration form)

    – Testing of mobile device at the lab and issuance of final report (two weeks)

    – Review of the mobile device test report and issuance of TAS (one week)

    – Registration of embedded Secure Element and applet for CAST approval and issuance of CAST certificate (four months)

    – Functional testing of embedded Secure Element and applet by embedded SE vendor, issuance of final report by the lab and issuance of TAS by MasterCard (two weeks)

    – Issuance of LoA for mobile device based on successful CAST, functional testing of applet and testing of mobile device (one week).

- Mobile device with removable Secure Element (such as uses UICC, MicroSD)

    – Registration of mobile device with MasterCard and issuance of MEPS (one week from reception of a correctly completed registration form)

    – Testing of mobile device at the lab and issuance of final report (two weeks)

    – Review of final report of testing of mobile device and issuance of TAS and LoA (one week)

These durations have strong dependency on the lab, number of devices being processed and whether any issues are discovered during the testing of the device which may require detailed investigation.

What kind of licenses need to be signed by an NFC Mobile Device vendor?

All vendors who submit their NFC Mobile Device for MasterCard approval must sign a MasterCard Mobile Device Testing Agreement. The agreement covers the conditions that must be followed by all vendors submitting devices for approval including post approval maintenance of the approved NFC Mobile Device.

In addition to the MasterCard Mobile Device Testing Agreement, vendors submitting NFC Mobile Devices with embedded SE for approval may need to sign a MasterCard M/Chip Mobile Specification License Agreement. This is necessary for vendors that require access to the MasterCard M/Chip Mobile Specifications to develop the applet and also vendors who will not develop the applet but will handle/use a MasterCard M/Chip Mobile applet provided by a third party.

Appendix C   References for MasterCard contactless NFC Mobile Device Approval

This section contains lists of abbreviations, acronyms, terminology, documents, and resources relevant to MasterCard contactless NFC mobile device approval.

Abbreviations and Acronyms

The table lists abbreviations and acronyms relevant to MasterCard
NFC mobile device approval.

Acronym	Description
CAST	Compliance Assessment and Security Testing
DUT	Device Under Test
eSE	embedded Secure Element
HCE	Host Card Emulation
HCI	Host Controller Interface
ICS	Implementation Conformance Statement
LoA	Letter of Approval
MEPS	Mobile Evaluation Plan Summary
MCBP	MasterCard Cloud Based Payment
MNO	Mobile Network Operator
MPA	Mobile Payment Application (SW component for MCBP solutions)
NFC	Near Field Communications
OS	Operating System
PICC	*PayPass* Integrated Circuit Card
RF	Radio Frequency
SE	Secure Element
SIM	Subscriber Identity Module
SWP	Single Wire Protocol
TAS	Test Assessment Summary
TSM	Trusted Service Manager
TSS	Test Session Summary
UICC	Universal Integrated Circuit Card

Terminology

The table explains key terms and concepts relevant to MasterCard
NFC mobile device approval.

Term	Description
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 Approval	Compliance Assessment and Security Testing (CAST) program is a global program whose objective is to ensure that the Secure Element, OS and MasterCard M/Chip Mobile payment applet conform to the MasterCard security requirements.
Component	Any product, part or combination of parts used in a MasterCard contactless mobile implementation (such as mobile device, payment application)
Debug Testing	Early functional evaluation of a MasterCard NFC mobile device to obtain an indication whether or not the mobile device will pass formal testing.
Device Firmware	Is the Operating System (with a specific version) of a mobile device and will generally include all software modules (such as drivers and runtime environments) that are needed to support all the functions of the device (including the NFC module)
Formal Selective Testing	Functional evaluation of a MasterCard contactless NFC mobile device for the purpose of deploying a limited number of devices for a mobile payment pilot or trial
Formal Testing	Functional evaluation of a MasterCard contactless NFC mobile device for the purpose of issuing a LoA which permits the device to be used globally and without any restrictions for any mobile payment deployment project
Inheritance	This is the process by which one mobile device (variant) can inherit some or the entire test results of another mobile device (registered or approved). The amount of test results that can be inherited depends on the similarity between the two devices such as NFC hardware/software, casing material, cellular radios supported. This can help reduce the time and cost of approving the variant device. Inheritance criteria for EMVCo Level 1 process should be discussed with EMVCo representatives.
Issuer	In the context of this document an issuer is a bank or MNO wishing to provide its customers with a mobile payment service based on NFC. All Issuers are required to ensure that they only issue MasterCard contactless to fully approved implementations such as all components of the implementation have been tested and approved. The issuer is responsible for personalization of customer account-holder details to the device.

Commented [HH1]: Add explanation for EMVCo ICS.

Term	Description
Mobile Device	Any mobile phone, smartphone, tablet or communications device that includes NFC functionality with an embedded or removable Secure Element and can be used as part of a MasterCard contactless implementation.
Mobile Device Manufacturer	The scope of the role of this entity can range from manufacturing an NFC reference mobile device which can be used and customized by a number of vendors to manufacturing the end product NFC mobile device sold to the consumer.
Mobile Device Samples	These are the samples that must be provided to the test laboratory for testing of the NFC mobile device to commence.
Mobile Evaluation Plan Summary (MEPS)	Test plan defining at high level the tests that need to be successfully executed by a MasterCard certified lab. For NFC mobile devices being certified for use with a removable Secure Element, it also specifies the number of mobile device samples to be submitted by the vendor to the lab for performing the testing.
MasterCard contactless NFC mobile Device Approval	The umbrella term for all the functional evaluations and review processes and outputs relating to the approval of a MasterCard NFC mobile device. The final output of this group of processes is the Letter of Approval (LoA).
MasterCard contactless NFC mobile device– Letter of Approval (LoA)	Acknowledgement by MasterCard that an NFC mobile device to be used as part of any MasterCard contactless mobile implementation (and all of its specified components) has demonstrated compliance to the requirements. This means it can be used by issuers with other approved MasterCard contactless mobile 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 MasterCard contactless mobile implementations, either at an issuer level or at a supplier level. The program is supported by a website (www.mastercard-mobilepartner.com) 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 MasterCard contactless – M/Chip Mobile Specification within a Secure Element such as residing on a secure UICC, MicroSD or embedded Secure Element covering the requirements of the MasterCard contactless – M/Chip Mobile Specification.

Term	Description
SWP enabled NFC Mobile Device	The generic term used throughout this document to refer to any NFC enabled mobile device compliant with *EMV Contactless Protocol* that incorporates an SWP implementation according to *ETSI TS 102.622* and *ETSI TS 102.613*. The SWP protocol was developed to enable the removable SE to communicate with the NFC mobile device hence to allow payment applications running on removable SEs to communicate with contactless readers. In future SWP protocol is also expected to be used for communication between the embedded Secure Element and the NFC mobile device.
Technical Assessment	MasterCard reviews the results of every test that is performed on the DUT and where test results meet or exceed requirements a Test Assessment Summary (TAS) confirming the compliance with relevant requirements is issued by MasterCard.
Test Assessment Summary (TAS)	A formal summary document containing MasterCard's assessment of the tests conducted on the NFC mobile device
Test Report	Summary of the test results issued by an Accredited Laboratory as a result of Formal Testing or Formal Selective Testing
Accredited Test Laboratory	A facility Accredited by MasterCard to perform tests on MasterCard contactless mobile products
Variant Mobile Device	An NFC mobile device that is similar to an already registered or approved MasterCard contactless NFC mobile device where the differences are limited to cellular RF support, operator or market specific software, SE configuration (embedded SE vs removable SE) or commercial name