
# MasterCard TSM Functional Requirements

**May 2015 - Version 2.0.1**

# 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.

**Using this Manual** ..... i

Scope ..... i
Audience ..... i
Reader Guidance ..... i
Abbreviations and Acronyms ..... i
Related Information ..... iii
Terminology ..... iv
Revision History ..... viii

**1 Introduction** ..... 1

1.1 Background ..... 1
1.2 The MasterCard M/Chip Mobile Ecosystem ..... 1
1.3 Who needs to implement these requirements? ..... 3
1.4 When must these requirements be implemented? ..... 4
1.4.1 High level definition of a TSM ..... 4
1.4.2 Payment application life cycle ..... 4
1.4.3 EMV payment data management ..... 4
1.4.4 Post issuance management ..... 5
1.4.5 Secure Element Issuer/Mobile Network Operator TSM ..... 5

**2 Roles and Responsibilities** ..... 5

2.1 Role descriptions ..... 6
2.1.1 Secure Element Issuer ..... 6
2.1.2 Security Domain Manager ..... 7
2.1.3 Application Provider Security Domain Manager ..... 7
2.1.4 Card Issuer ..... 7
2.1.5 Secure Element Manufacturer ..... 7
2.1.6 Link Platform Operator ..... 7
2.1.7 Controlling Authority ..... 8
2.2 Configuration of the Actors and Roles ..... 8

**3 Application Life Cycle Management** ..... 9

3.1 Introduction ..... 9
3.2 Security Domain Life Cycle Management ..... 10

3.2.1 Pre and post issuance creation of Security Domains ..... 11
3.2.2 Key rotation and Controlling Authority ..... 11
3.3 Mobile Payment Application Issuance ..... 13
3.3.1 Eligibility Checking of Mobile Device and Assembly ..... 13
3.3.2 Mobile Payment Application ELF Loading ..... 17
3.3.3 Mobile Payment Application Instance Installation ..... 17
3.4 Mobile Payment Application Instance Personalization ..... 17
3.5 Post-Issuance Management of Payment Application ..... 18

**4 Determining your Role and the scope of requirements ..... 19**

4.1 Determining Your Role ..... 20
4.1.1 Secure Element Issuers ..... 20
4.1.2 Security Domain Managers ..... 20
4.1.3 Application Provider Security Domain Managers ..... 21
4.1.4 Secure Element Manufacturers ..... 21
4.1.5 Link Platform Operators ..... 21
4.1.6 Controlling Authorities ..... 21
4.2 Determining the Scope of Requirements ..... 21
4.2.1 Secure Element Issuers ..... 22
4.2.2 Security Domain Managers ..... 22
4.2.3 Application Provider Security Domain Managers ..... 22
4.2.4 Secure Element Manufacturers ..... 22
4.2.5 Link Platform Operators ..... 22
4.2.6 Controlling Authorities ..... 22

**5 Functional Requirements ..... 22**

5.1 Format of requirements ..... 23
5.1.1 Functional requirements groups based on roles ..... 23
5.1.2 Use of equivalent and future technologies ..... 23
5.1.3 Background and Rationale ..... 23
5.1.4 Definition of a Requirement ..... 23
5.1.5 Definition of a Conditional Requirement ..... 23
5.1.6 Definition of a Recommendation ..... 23
5.2 Generic requirements ..... 24

5.2.1 Requirement GEN_01 - SD key diversification ..... 24
5.2.2 Conditional Requirement GEN_02 – SE access control ..... 24
5.2.3 Requirement GEN_03 – TSM system identification ..... 24
5.3 Requirements for Secure Element Issuers ..... 25
5.3.1 Functional ..... 25
5.3.1.1 Requirement SEI_01 – SE lock and terminate policies ..... 25
5.3.1.2 Requirement SEI_02 – Instance lock and delete policies ..... 25
5.3.1.3 Requirement SEI_03 - Lock and terminate policies ..... 25
5.3.1.4 Recommendation SEI_04 – TSD/LPO SD cumulative granted memory ..... 25
5.3.1.5 Requirement SEI_05 – Profile identifier for device capability ..... 25
5.3.1.6 Requirement SEI_06 – Profile identifier for SE capability ..... 26
5.3.1.7 Conditional Requirement SEI_07 – CA certificate retrieval ..... 26
5.3.1.8 Requirement SEI_08 – Forbidden role as CA ..... 26
5.3.1.9 Conditional Requirement SEI_09 – UI application binding / unbinding ..... 26
5.3.1.10 Recommendation SEI_10 – Rule settings for UI application binding ..... 26
5.3.1.11 Conditional Requirement SEI_11 – Change notification for mobile subscription identifier/life cycle state ..... 27
5.3.1.12 Conditional Requirement SEI_12 – SE life cycle notification ..... 27
5.3.1.13 Conditional Requirement SEI_13 – Load, Install, extradite and delete of payment application load-file and instances ..... 27
5.3.1.14 Conditional Requirement SEI_14 – Authorization to load, install, extradite and delete of payment load-file and instances ..... 28
5.3.2 Security ..... 28
5.3.2.1 Requirement SEI_15 – Secure messaging for card content management commands 28
5.3.2.2 Requirement SEI_16 – Minimum security level for card content management commands 28
5.4 Requirements for Security Domain Managers ..... 28
5.4.1 Functional ..... 28
5.4.1.1 Conditional Requirement SDM_01 – TSD AID structure for authorized management ..... 28
5.4.1.2 Conditional Requirement SDM_02 – TSD AID structure for delegated management ..... 29
5.4.1.3 Conditional Requirement SDM_03 – APSD AID structure ..... 29

5.4.1.4 Conditional Requirement SDM_04 – TSM/APSD AID structure ..... 29
5.4.1.5 Requirement SDM_05 – TSD acceptance policy for other SD ..... 29
5.4.1.6 Requirement SDM_06 – TSD proximity access over the contactless interface 30
5.4.1.7 Conditional Requirement SDM_07 – Security Domain hierarchy ..... 30
5.4.1.8 Conditional Requirement SDM_08 – Ownership of APSDs under the management of SDM ..... 30
5.4.1.9 Requirement SDM_09 – Card content management capabilities ..... 31
5.4.1.10 Conditional Requirement SDM_10 – UI application binding/unbinding capabilities 31
5.4.1.11 Recommendation SDM_11 – Script sending capability ..... 31
5.4.1.12 Conditional Requirement SDM_12 – Script content ..... 31
5.4.1.13 Recommendation TSM SDM_13 – Memory management ..... 31
5.4.1.14 Conditional Requirement SDM_14 – Service activation ..... 32
5.4.1.15 Requirement SDM_15 – Service suspension ..... 32
5.4.1.16 Requirement SDM_16 – Service suspension, verification before instance lock 32
5.4.1.17 Conditional Requirement SDM_17 – Service suspension, instance lock priority 32
5.4.1.18 Requirement SDM_18 – Service suspension, instance lock retry ..... 33
5.4.1.19 Requirement SDM_19 – Service resumption ..... 33
5.4.1.20 Requirement SDM_20 – Service resumption, verification before instance unlock 33
5.4.1.21 Requirement SDM_21 – Service renewal ..... 33
5.4.1.22 Requirement SDM_22 – Service termination ..... 34
5.4.2 Security ..... 34
5.4.2.1 Requirement SDM_23 – Secure messaging for card content management commands 34
5.4.2.2 Requirement SDM_24 – Minimum security level for card content management commands 34
5.4.2.3 Conditional Requirement SDM_25 – Pre-shared TSD initial keys ..... 34
5.4.2.4 Conditional Requirement SDM_26 – Delivery of TSD key rotation scripts ..... 35
5.4.2.5 Conditional Requirement SDM_27 – Confidential Setup of TSD Initial Secure Channel Keys ..... 35

5.4.2.6 Conditional Requirement SDM_28 – CA certificate verification ..... 35
5.4.3 Mobile Device and Assembly Eligibility Checks ..... 35
5.4.3.1 Requirement SDM_30 – Eligibility checks prior to load or instantiate ..... 35
5.4.3.2 Requirement SDM_31 – Eligibility check on Mobile Device ..... 36
5.4.3.3 Requirement SDM_32 – Eligibility check on Secure Element ..... 36
5.4.3.4 Requirement SDM_33 – Approval checks on the payment application ..... 36
5.4.3.5 Recommendation SDM_34 – Load and instantiate retry ..... 36
5.4.3.6 Requirement SDM_35 – Eligibility check status to APSDM ..... 37
5.5 Requirements for Application Provider Security Domain Managers ..... 37
5.5.1 Functional ..... 37
5.5.1.1 Requirement APSDM_01 – Personalization capability ..... 37
5.5.1.2 Requirement APSDM_02 – APSD acceptance policy for other SD ..... 37
5.5.1.3 Requirement APSDM_03 – APSD proximity access over the contactless interface 38
5.5.2 Security ..... 38
5.5.2.1 Recommendation APSDM_04 – Executable load-file authenticity ..... 38
5.5.2.2 Conditional Requirement APSDM_05 – DAP verification ..... 38
5.5.2.3 Conditional Requirement APSDM_06 – DAP verification scheme ..... 38
5.5.2.4 Requirement APSDM_07 – Asset security ..... 39
5.5.2.5 Requirement APSDM_08 – Minimum security level for personalization/issuer script commands ..... 39
5.5.2.6 Conditional Requirement APSDM_09 – Pre-shared APSD initial keys ..... 39
5.5.2.7 Conditional Requirement APSDM_10 – Delivery of APSD key rotation scripts 39
5.5.2.8 Conditional Requirement SDM_11 – Confidential Setup of APSD Initial Secure Channel Keys ..... 40
5.5.2.9 Conditional Requirement APSDM_12 – CA certificate verification ..... 40
5.5.2.10 Conditional Requirement APSDM_13 – Delivery of personalization/issuer script via SEI or SDM's OTA/OTI channel ..... 40
5.5.3 Mobile Device and Assembly Eligibility checks ..... 41
5.5.3.1 Recommendation APSDM_15 – Personalization retry ..... 41
5.5.4 Issuer Scripts Delivery ..... 41
5.5.4.1 Requirement APSDM_16 – Script delivery time limit ..... 41
5.5.4.2 Requirement APSDM_17 – Script delivery failure ..... 41

5.6 Requirements for Link Platform Operators ..... 41
5.6.1 Conditional Requirement LPO_01 – LPO SD creation by SEI ..... 41
5.6.2 Conditional Requirement LPO_02 – LPO SD creation by SE Manufacturer ..... 42
5.6.3 Conditional Requirement LPO_03 – LPO capable of card content management . 42
5.6.4 Requirement LPO_04 – LPO SD proximity access over the contactless interface 42

# *Using this Manual*

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

## Scope

This document lists the requirements that must be met in order for a TSM solution (used in conjunction with MasterCard M/Chip Mobile implementations) to achieve MasterCard approval. It also lists recommendation for other parts of the ecosystem that are associated with TSM solutions.

## Audience

This document is aimed primarily at:

- Trusted Service Managers.

However, other members of the mobile contactless payment ecosystem may also find the information contained in this document useful. These include:

- Card Issuers
- Mobile Network Operators (MNOs)
- Secure Element Manufacturers and Issuers
- Mobile device Manufacturers
- Payment Application Providers
- User Interface Application Developers/Providers

## Reader Guidance

This document lists the requirements that TSM solutions that are used in implementations of MasterCard M/Chip Mobile must adhere to.

## Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

| Acronym | Meaning |
|---|---|
| AID | Application Identifier |
| AM | Authorized Management |
| APSD | Application Provider Security Domain |
| APSDM | Application Provider Security Domain Manager |

| Acronym | Meaning |
|---|---|
| ARA | Access Rule Application |
| ARF | Access Rules File |
| ARPC | Authorisation ResPonse Cryptogram |
| CASD | Controlling Authority Security Domain |
| CCM | Card Content Management |
| DAP | Data Authentication Pattern |
| DM | Delegated Management |
| DMSR | Device and Mobile Subscription Registrar |
| ELF | Executable Load-File |
| EMV | Europay MasterCard Visa |
| ETSI | European Telecommunications Standards Institute |
| GVCP | Global Vendor Compliance Program |
| ICCID | Integrated Circuit Card Identifier |
| IMEI | International Mobile Equipment Identity |
| IMSI | International Mobile Subscriber Identity |
| ISD | Issuer Security Domain |
| LPO | Link Platform Operator |
| MCM | MasterCard M/Chip Mobile |
| MNO | Mobile Network Operator |
| mPIN | mobile Personal Identification Number |
| NFC | Near Field Communication |
| OTA | Over The Air |
| OTI | Over The Internet |
| SD | Security Domain |
| SDM | Security Domain Manager |
| SE | Secure Element |
| SEI | Secure Element Issuer |
| SIM | Subscriber Identity Module |
| SM | Simple Mode |
| SSD | Secondary Security Domain |
| TSM | Trusted Service Manager |
| TSD | Trusted Service Manager Security Domain |
| UI | User Interface |
| UICC | Universal Integrated Circuit Card |

| Acronym | Meaning |
|---|---|
| USIM | Universal Subscriber Identity Module |

# Related Information

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

**Note**

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

| Ref | Document name | Organization | Version | Date |
|---|---|---|---|---|
| [1] | White Paper: GlobalPlatform Proposition for NFC Mobile: Secure Element Management and Messaging | Global Platform | - | Apr-09 |
| [2] | Messaging Specification for Management of Mobile-NFC Services | Global Platform | 1.1 | Feb-13 |
| [3] | GlobalPlatform Card UICC Configuration | Global Platform | 1.0.1 | Jan-11 |
| [4] | Security Requirements for Mobile Payment Provisioning (draft) | MasterCard | Rev 2 | |
| [5] | GlobalPlatform Card Specification | Global Platform | 2.2.1 | Jan-11 |
| [6] | GlobalPlatform Card - Confidential Card Content Management - Card Specification v2.2 - Amendment A | Global Platform | 1.0.1 | Jan-11 |
| [7] | GlobalPlatform Card - Remote Application Management over HTTP - Card Specification v 2.2 - Amendment B | Global Platform | 1.1.2 | May-14 |
| [8] | GlobalPlatform Card - Contactless Services - Card Specification v 2.2 - Amendment C | Global Platform | 1.0.1 | Feb-12 |
| [9] | GlobalPlatform Card – Secure Channel Protocol 03 - Card Specification v 2.2 – Amendment D | Global Platform | 1.1 | Sep-09 |
| [10] | GlobalPlatform Card – Security Upgrade for Card Content Management - Card Specification v 2.2 – Amendment E | Global Platform | 1.0 | Nov-11 |
| [11] | GlobalPlatform Card - Secure Element Configuration | Global Platform | 1.0 | Oct-12 |

| | | | | |
|---|---|---|---|---|
| [12] | GlobalPlatform Device Technology - Secure Element Access Control | Global Platform | 1.0 | May-12 |
| [13] | GlobalPlatform Device Technology - Secure Element Remote Application Management | Global Platform | 1.0 | May-11 |
| [14] | EMV Profiles of GlobalPlatform UICC Configuration | EMVCo | 1.0 | Dec-10 |
| [15] | NFC UICC Requirement Specification | GSMA | 4.0 | Aug-13 |
| [16] | ETSI TS 102 225 – Smart Cards; Secured packet structure for UICC based applications (Release 9) | ETSI | 9.1.0 | Sep-11 |
| [17] | ETSI TS 102 226 - Smart Cards; Remote APDU structure for UICC based applications (Release 9) | ETSI | 9.3.1 | Sep-11 |
| [18] | ISO/IEC 7816-5, Identification cards - Integrated circuit cards - Part 5: Registration of application providers | ISO | - | 2004 |
| [19] | Mobile MasterCard *PayPass* NFC Mobile Device Approval Guide | MasterCard | - | Nov-12 |

# Terminology

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

| Term | Meaning |
|---|---|
| Access Rule Application | An application in SE for storing access control rules, see reference [12]. |
| Access Rules File | An application in UICC for storing access control rules, see reference [12]. |
| Application | The combination of an application instance and the ELF from which it is instantiated. |
| Application instance | An instance of a MasterCard M/Chip Mobile application that, if personalized, may be used for making a mobile payment. |
| Application Provider Security Domain | A Security Domain on a Secure Element to which one or more MasterCard M/Chip Mobile application instances are directly associated. The secure channel keys of the APSD are used to protect the MasterCard or Card Issuer assets during the personalization process of a MasterCard M/Chip Mobile application. |

| Term | Meaning |
|---|---|
| APSD Manager | An actor that is in possession of the secure channel keys of an APSD, and therefore has knowledge of personalization data sent to MasterCard M/Chip Mobile application instances associated to that APSD. The APSD Manager acts as the Personalization Bureau for MasterCard M/Chip Mobile application instances. |
| Assembly | A combination of a Secure Element, an NFC Controller and an NFC antenna that, when brought together, can perform a contactless payment and can therefore be tested for functional compliance with MasterCard M/Chip Mobile requirements. |
| Assets (MasterCard or Card Issuer) | One or more of the following:<br>MasterCard M/Chip Mobile application code,<br>MasterCard M/Chip Mobile application personalization data, such as: Cardholder personal data and EMV data, PINs, Payment application keys,<br>Issuer Scripts and Issuer Updates. |
| Authorized Management | A deployment model where the SDM or LPO is granted full CCM by the SEI without the need for authorization. |
| Card Issuer | The bank that is responsible for a personalized mobile payment application instance. The Cardholder holding this application instance is a customer of the Card Issuer. |
| Cardholder authentication | A process establishing that:<br>The designated Mobile Device is physically in the possession of the rightful Cardholder,<br>The rightful Cardholder consents with the intended action. |
| Component | Any product, part or combination of parts used in a MasterCard M/Chip Mobile implementation (e.g. Mobile Device or User Interface Application) |
| Controlling Authority | An actor controlling a Controlling Authority Security Domain on every Secure Element. |
| Controlling Authority Security Domain | A (self-extradited) Security Domain containing an asymmetric key pair that can be used by SD Managers and APSD Managers to guarantee full confidentiality of secure channel key sets during key rotation processes. |
| Delegated Management | A deployment model where the SDM or LPO is granted CCM by the SEI and requires authorization. |
| Device and Mobile Subscription Registrar | An actor responsible for answering eligibility checks regarding Mobile Devices and/or Secure Elements, and for keeping track of the relationship between a particular Mobile Subscription, a Mobile Device and Secure Element(s). |
| Executable Load-File | A container of MasterCard M/Chip Mobile application code. |
| Formal Evaluation | Generic term used to refer to the set of testing sub-processes that have a defined start (sample submission etc.) and end point (Assessment Summary etc.). |

| Term | Meaning |
|---|---|
| Issuer Security Domain | The first Security Domain installed on the Secure Element, owned by the SE Issuer and having the privileges specified in ref. [3]. |
| Link Platform Operator | An actor responsible for setting up the remote OTA or OTI channel to the Secure Element. This is normally the MNO. |
| MasterCard M/Chip Mobile | A payment application designed specifically for the features of mobile devices. |
| Mobile Device | A device that supports one or more remote communication technologies (such as GSM, LTE, Wi-Fi) needed to set up a remote OTA or OTI channel to a Secure Element. It also contains or is connected to an Assembly that includes NFC functionality and can be used as part of a MasterCard M/Chip Mobile implementation. |
| Mobile device Manufacturer | The manufacturer of the mobile device; the scope of the role of this entity can range from simply manufacturing the hardware that will house the other key components to providing a device that incorporates SE and/or Payment Application and/or User Interface or Wallet application. |
| On-device Personalization Application | May also be known as “Personalization Agent” or “Personalization Client”. Software that provides interaction between the M/Chip Mobile application within the Secure Element and the mobile network for over-the-air personalization. It also enables downloading of the M/Chip Mobile application over-the-air to the Secure Element. May be implemented in a number of ways, for example a Java MIDlet. |
| NFC Ecosystem | An end-to-end configuration that typically comprises of multiple actors taking 1 or more functional roles. Each role can be a Card Issuer, Secure Element Issuer, Secure Element Manufacturer, SD Manager, APSD Manager, Link Platform Operator, or Controlling Authority. |
| OTA | Over-The-Air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile device or any component within the mobile device via a mobile network. |
| Over The Air [channel] | A remote connection from a Security Domain in the Secure Element to a server of the LPO, using the specifications of reference [16] and [17]. |
| Over The Internet [channel] | A remote connection from a Security Domain in the Secure Element to a backend server, using TLS over HTTP, as specified in reference [7]. |
| Payment Application | The software implemented within the secure memory domain (e.g. on the secure SIM card) meeting the requirements of the MasterCard M/Chip Mobile Specification. |

| Term | Meaning |
|---|---|
| Payment Application Provider | A legal entity that has signed a MasterCard M/Chip Mobile Specification License Agreement, is entitled to use MasterCard Contactless brands and supply M/Chip Mobile applications and whose name will be stated on the MasterCard M/Chip Mobile Implementation -Letter of Approval. |
| Payment Service | The combination of the Payment Application and personalization data that enable the NFC payment transaction to take place. |
| Secondary Security Domain | A Security Domain other than the ISD. In this document used as a collective name for TSM SDs and APSDs, but not the CASD. |
| Secure Element | A component in a Mobile Device that contains a MasterCard M/Chip Mobile application and the associated MasterCard or Card Issuer assets, and which offers the security needed for the protection of these assets. |
| Secure Element Issuer | An actor that controls the Issuer Security Domain (ISD) on a Secure Element on which one or more MasterCard M/Chip Mobile applications are residing, and that by virtue thereof may lock or terminate the Secure Element and lock or delete the MasterCard M/Chip Mobile applications |
| Secure Element Manufacturer | An actor that manufactures a Secure Element according to the specifications of the SE Issuer. |
| Security Domain | An application on a Secure Element providing support for the requirements regarding control, security and communication of an (off-card) actor, such as the SE Issuer, an SD Manager or an APSD Manager. |
| Security Domain Manager | An actor that is in possession of the secure channel keys of a TSD, and that is therefore able to perform CCM on MasterCard assets, but has no knowledge of the personalization data of a particular payment application instance. |
| Simple Mode | A deployment model where the SDM or LPO is not granted CCM by the SEI. |
| TSM Security Domain | A Security Domain on an SE containing MasterCard assets, and having either the Authorized Management or the Delegated Management privilege allowing it to perform CCM on these assets. |
| TSM Platform | An application suite that typically comprises of functional modules including payment application personalization & lifecycle management, SE lifecycle management, SE security key management, inter-system messaging communication & notification, NFC service eligibility control, remote administration management and monitoring & reporting services. |
| TSM Supplier | An entity that supplies the TSM Platform to a TSM Vendor. A TSM Supplier and TSM Vendor can be the same entity. |

| Term | Meaning |
|---|---|
| TSM System | An application server which is configured from a TSM Platform to operate certain TSM roles in an NFC ecosystem. It connects to one or more external entities within the same ecosystem for inter-TSM messaging and notification purposes. There can be more than 1 TSM system in a TSM vendor's facility. |
| TSM Vendor | An entity that owned the facility where the TSM system is hosted. A TSM Vendor is responsible for all matters pertaining to TSM approval process. |

# Revision History

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

Each revision includes a summary of changes which is added to the revision history below, describing what has changed and how.

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

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

| Version | Date | History | Impact |
|---|---|---|---|
| 1.0 | December 2009 | First published version. | Set of defined requirements for User Interface Applications, augmenting *PayPass on Mobile Requirements* |
| 2.0 | February 2015 | Second publication | Clarification and updates to all requirements. The requirements have become role based. Dependency on mobile device software removed. |
| 2.0.1 | May 2015 | Requirements update | Requirements SDM_34 and APSDM_15, LPO_03 are reclassify as recommendations. |

# 1 Introduction

This document lists the requirements for any MasterCard accredited TSM Service in the context of MasterCard M/Chip Mobile implementations. Requirements for mobile device based provisioning software, such as TSM proxies or agents, are out of scope for this document.

**Note**

**Any UI Application that that forms part of a TSM solution and interfaces with a MasterCard compliant Payment Application and/or makes use of any MasterCard brand identifiers or other properties will also need to comply with the MasterCard Mobile User Interface Application Requirement.**

## 1.1 Background

MasterCard has developed a comprehensive test and validation process for MasterCard M/Chip Mobile implementations and components used in implementations that are derived from the existing processes that are applied in the context of issuing MasterCard Contactless card products. This enables world-wide interoperability as well as quality, reliability and security assurance at acceptable levels of time and cost.

All components and sub-components used in an implementation of MasterCard M/Chip Mobile must go through a test and validation process. All approved products; services, components and subcomponents are documented and held in a database by MasterCard. Information relating to approved products and services is made available to Card Issuers via the Mobile Partner Program website (www.mastercard-mobilepartner.com). The information is provided to enable Card Issuers to ensure that only approved implementations are brought to market.

As most implementations of MasterCard M/Chip Mobile will utilize an OTA solution of some description (especially for personalization), the engagement of a third party who has access to the relevant keys allowing access to the payment domain within the Secure Element (SE) is required. These organizations are referred to as a Trusted Service Manager (TSM). This document describes the requirements that need to be met by TSMs when delivering the service in a convenient and secure manner.

## 1.2 The MasterCard M/Chip Mobile Ecosystem

MasterCard M/Chip Mobile allows consumers to pay at a contactless Point of Sale using a Mobile Device that is equipped with NFC technology, and perform remote payments including In-App purchases with compatible mobile device applications.

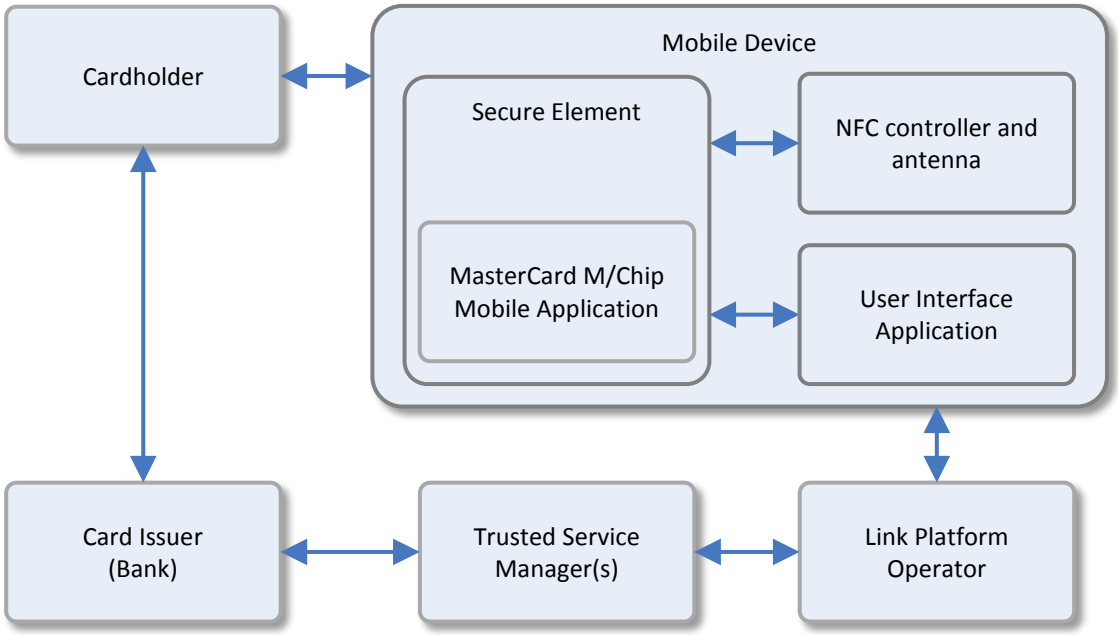


**Figure 1 - MasterCard M/Chip Mobile Infrastructure**

The **Cardholder** signs up for and uses a MasterCard M/Chip Mobile application.

In order to do so, the Cardholder must use a **Secure Element** and a **Mobile Device.**

The Secure Element is a secure chip, on which a **MasterCard M/Chip Mobile application** is installed. Secure Elements may either be embedded in the Mobile Device or be Cardholder removable. In the latter case, a Secure Element may take the form of a UICC or a secure microSD card.

A Mobile Device offers a remote data connection, allowing the Card Issuer to install and personalize the MasterCard M/Chip Mobile application on the Secure Element. Additionally, a Mobile Device either contains or is connected to an NFC antenna and an NFC controller controlling that antenna. These NFC components allow communication with a payment terminal, using the same contactless communication protocol as a regular contactless payment card. The Secure Element, the NFC antenna and the NFC controller together are known as the Assembly. The Assembly is able to perform a contactless payment transaction and can therefore be tested for functional compliance with MasterCard M/Chip Mobile requirements.

A **User Interface Application** runs on the Mobile Device and allows the Cardholder to interact with the applications in the Secure Element, through an SE access API provided by the Mobile Device operating system. Depending on the implementation of the UI application, it may act as an Admin Agent (see reference [13]) and connects securely to an associated TSM for Cardholder authentication or Mobile Payment service management, or it can also be a Wallet, retrieving recent transactions or to set up the payment application for a next transaction. User Interface Applications can be software running on the Mobile Device itself, but can also run on the Secure Element, e.g. via the Card Application Toolkit technology defined by ETSI.

The **Card Issuer** issues the mobile version of a payment card to the cardholder. This may involve the issuing of a MasterCard M/Chip Mobile application and personalization of the application.

The **Link Platform Operator** is responsible for setting up the remote connection to the Mobile Device and the Secure Element. This is normally the Mobile Network Operator.

Finally, there will be one or more **Trusted Service Manager(s)** (TSM), acting as a central party in a mobile payments infrastructure. A TSM can fulfil many different responsibilities. Some of these are:

- Creating and managing Security Domains on the Secure Element in Mobile Devices,
- Acting as a Personalization Bureau for mobile payment applications, on behalf of Card Issuers,
- Installing and managing payment applications on Secure Elements, on the request of Card Issuers,
- Arranging the off-card processes needed to enable this card management, providing billing and management information to both Service Providers and MNOs, and so on.

## 1.3 Who needs to implement these requirements?

The requirements need to be met by any Trusted Service Manager who wishes to gain approval from MasterCard to provide their TSM solution to MasterCard issuing institutions in the context of MasterCard M/Chip Mobile issuance.

TSM vendors need to apply for TSM approval if their TSM system performs any of the following:

- Mobile payment application personalization, such as preparation and personalization of card holder data and card data into the mobile payment application.
- Post-issuance remote management of mobile payment application, such as administration of issuer scripting via an OTA/OTI channel.

Banks that wish to set up and run their own mobile provisioning services using their own technology infrastructure do so at their own risk and need not therefore request approval from MasterCard for doing so.

# 1.4 When must these requirements be implemented?

The requirements apply to all TSM solutions and must be implemented by the TSM in all their deployments. The following paragraphs give high level definitions of a TSM, but “Chapter 2 – Roles and Responsibilities” gives more details of the actors and roles within the mobile ecosystem. “Chapter 4 - Determining your Role and the scope of requirements” describes how to determine which roles each actor plays and which requirements and recommendations apply.

## 1.4.1 High level definition of a TSM

A TSM is a system that interconnects Card Issuers with SEIs and provides mobile provisioning services. The TSM is trusted by both Card issuers and SEIs, and can be operated by a third party. The TSM may also be operated by a Card Issuer (with no approval require). The TSM may support one or more of the following services.

- Payment application life cycle
- EMV data life cycle
- Post issuance commands

## 1.4.2 Payment application life cycle

Payment application life cycle is concerned with the life cycle management of the MasterCard M/Chip Mobile payment application load-file and instances, but not data that the payment application acts upon. The life cycle phases included the download, instantiation, extradition and deletion of the MasterCard M/Chip Mobile payment application in the Secure Element. The TSM may be capable of downloading actual payment application load-file to the mobile device over the air.

## 1.4.3 EMV payment data management

EMV payment data management may include the data preparation and implement the personalization script to be sent OTA/OTI into the Secure Element. The TSM may play a part in either the preparation of the data, the delivery of the data, or both.

The TSM may be capable of accepting and combining data from sources (for example Card Issuers or traditional card bureaus) in order prepare it for personalization and deliver it to the Secure Element.

The TSM may be capable of accepting data prepared by other sources (for example Card Issuers or traditional card bureaus) and delivering it to the Secure Element.

### 1.4.4 Post issuance management

Post issuance management is concerned with the preparation and/or sending of post issuance commands or scripts from the TSM, OTA/OTI to the payment application, to the payment application. These scripts may include commands such as Put Data, Get Data, Update Record commands, commands related to payment PIN management, and commands to update or reset payment counters such as ARPC responses etc.

### 1.4.5 Secure Element Issuer/Mobile Network Operator TSM

SEI or MNO TSM system can be used to manage the access to the Secure Element. In many cases, ELF with payment application code or data is transmitted from a TSM via SEI/MNO TSM system to the SE.

# 2 Roles and Responsibilities

An ecosystem for mobile payments consists of multiple actors, each fulfilling certain responsibilities and offering services to other actors in the system. Each actor takes on one or multiples roles in the ecosystem. Several general descriptions of role models for mobile payment ecosystems exist, for example those by GlobalPlatform in references [1] and [2]. In all of these descriptions, a central role is played by a so-called Trusted Service Manager (TSM). The actual responsibilities a TSM fulfills show a lot of variation between different mobile payment ecosystems. However, on the technical level they all have to do with the management of the Secure Element, the Security Domains on this Secure Element and the applications within those Security Domains.

The center of Figure 2 shows the layout of a Secure Element that is assumed in this document. Around the Secure Element, the roles that may be involved in the management of such a Secure Element are depicted.

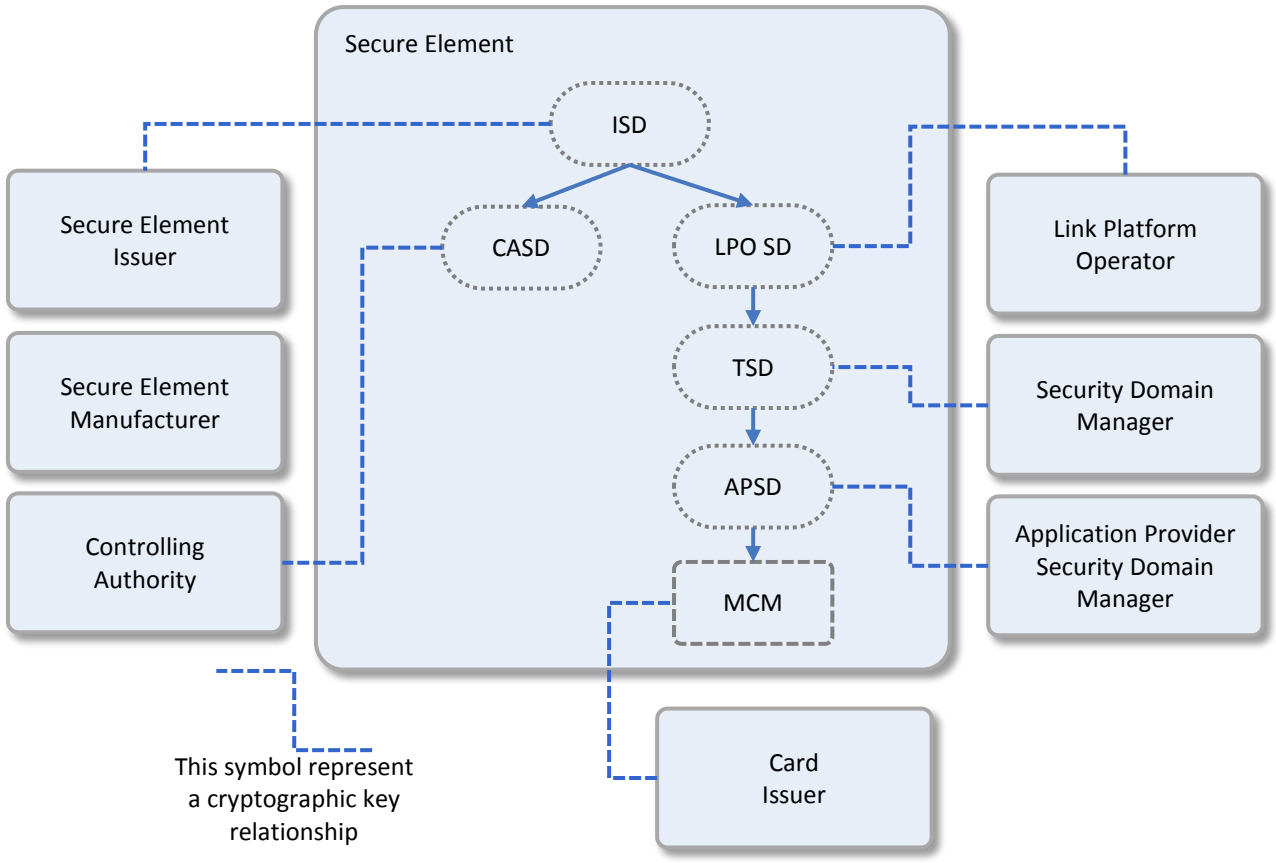


**Figure 2-Layout of Security Domains in a Secure Element and their associated off-card entities**

# 2.1 Role descriptions

A short description of each role is given in this section. Chapter 4 gives more details on the (possible) responsibilities of each role, during the entire life cycle of the Secure Element and the MasterCard M/Chip Mobile applications on it. Chapter 5 contains MasterCard's functional requirements for each of these roles.

## 2.1.1 Secure Element Issuer

The ISD on the SE is owned by the SEI. To communicate securely with the ISD, the SEI has one or multiple key sets. These keys are stored in the ISD and are called the secure channel key set. The privileges of the ISD allow the SEI to retain overall control over the SE, by locking, deleting and/or terminating the Secure Element or any of its contents, including Application Provider Security Domains and payment applications.

Note: The ISD privileges usually include Authorized Management. This means that the SEI is able to perform CCM on APSDs and MasterCard M/Chip Mobile applications. If that is the case, MasterCard considers the SEI to be a SDM, as defined in the next paragraph, unless the SEI has clear policies and procedures in place that prevent it from actually carrying out such content management.

### 2.1.2 Security Domain Manager

There is one or more TSDs associated to the ISD. A SDM is an entity that is in the possession of the secure channel key set that enables it to securely communicate to a TSD. The privileges of this TSD may include Authorized Management or Delegated Management. The SDM is able to perform CCM on APSDs and MasterCard M/Chip Mobile applications. It can create, personalize and delete APSDs and can also create and delete payment applications. However, the SDM, as defined in this document, is not involved in the personalization of payment applications.

### 2.1.3 Application Provider Security Domain Manager

An APSD is managed by an APSDM. An APSD is characterized by the fact that one or more MasterCard M/Chip Mobile applications are directly associated with it. Like the ISD and the TSD, the APSD contains a secure channel key set, which is only known to the APSDM and which allows the APSD to securely communicate with the APSDM. The privileges of the APSD do not include Authorized Management or Delegated Management. Therefore, the APSDM cannot create, move or delete payment applications. Instead, it uses the APSD and its keys to securely personalize the payment application. The APSDM role is functionally equivalent to the Card Personalization Bureau in the issuing process of contact or contactless payment cards.

### 2.1.4 Card Issuer

A Card Issuer is responsible for a (personalized) mobile payment application instance and its behavior. The Cardholder holding this application instance is a customer of the Card Issuer. The Card Issuer does not have a Security Domain on the Secure Element.

### 2.1.5 Secure Element Manufacturer

A SEM is responsible for the manufacturing of the SE, according to the profile that is created by the SEI. The SEM does not have a SD on the SE. The SEM is responsible at least for the creation of the ISD and the CASD (see below) and possibly for all SDs on an SE. See section 3.2 for more details.

### 2.1.6 Link Platform Operator

A LPO is responsible for setting up a connection to a UICC in a Mobile Device. This connection uses any remote communication technology, such as GPRS, UMTS or CDMA. A LPO is represented by a LPO SD in the UICC.

In many cases, a LPO operates as a separate entity. The SEI, SDM and/or APSDM use the LPO to set up to remote connection to the UICC.

### 2.1.7 Controlling Authority

The presence of a Controlling Authority is an actor having a Controlling Authority Security Domain (CASD) on each Secure Element. This CASD contains an asymmetric key pair. SDMs and APSDMs can encrypt their Secure Channel keys with the public key of this key pair to ensure full confidentiality.

The Controlling Authority could also function as a verifier for the authenticity of any loadfile by mandating this checking to be carried out by CASD in the Secure Element during application loading.

## 2.2 Configuration of the Actors and Roles

MasterCard does in no way mandate a particular layout for Secure Elements on which MasterCard M/Chip Mobile applications are provisioned, over and above the requirements by GlobalPlatform in reference [5]. Similarly, MasterCard does not mandate a particular set-up for the off-card actors involved in Secure Element management. Figure 2 can be simplified in several ways, reflecting the division of functions between the actors in the ecosystem. For example:

- If the SEI carries out all CCM itself, or gives a TSM access to the ISD to do so, there will not be a separate TSD on the SE. The ISD will have all keys and privileges associated in this document with the TSD.
- A separate APSDM will be absent in the case when the Card Issuer manages the keys of the APSD. In such a case, the requirements for the APSDM will be applicable to the Card Issuer.
- A separate APSD will be absent in case the SDM is also responsible for the secure personalization of payment applications. The TSD will have all keys associated in this document with the APSD.
- There is no need for the TSD to be directly associated with the ISD. In fact, the TSM could form the top of a separate hierarchy on the SE. Alternatively, there could be another Security Domain next to the ISD, to which the TSD is associated.
- The Link Platform Operator will usually not be a separate entity. Rather, the SEI, SDM and/or APSDM will function as an LPO themselves, meaning they have the technical capability to set up to remote connection to the Secure Element.
- The presence of a Controlling Authority may be required, depending on the SEI's deployment mode.

However, MasterCard will use the above model to clearly define the responsibilities of a certain role within a MasterCard M/Chip Mobile ecosystem. In particular,

- SEI will be taken to mean an actor that controls the ISD on a SE on which one or more MasterCard M/Chip Mobile applications are residing, and

that by virtue thereof may lock or terminate the Secure Element and lock or delete the MasterCard M/Chip Mobile applications.

- SDM will be taken to mean an actor that is in possession of the secure channel keys of a TSD, and that is therefore capable of performing CCM on MasterCard assets, but has no knowledge of the personalization data of a particular payment application instance.
- APSDM will be taken to mean an actor that is in possession of the secure channel keys of an APSD, and therefore has knowledge of personalization data sent to MasterCard M/Chip Mobile application instances associated to that APSD. This means that functionally, the APSDM is equivalent to a Personalization Bureau in the issuance process for traditional payment cards.

# 3 Application Life Cycle Management

## 3.1 Introduction

Chapter 2 introduced the different roles in a MasterCard M/Chip Mobile ecosystem. Chapters 5 list requirements for each of these roles. In order to provide a clear background for these requirements, this chapter explains the functions of each role in more detail, by describing the four basic processes involved in a typical life cycle of a mobile payment application. For each process, this chapter describes which actions need to take place, and which actor carries out each action. Special attention is given to variability that may exist between different implementations.

From a high level point of view, the 8 main processes in which a TSM may be involved are:

- Cardholder Authentication – this involves verification of the Cardholder during mobile provisioning.
- Mobile Subscriber Eligibility Check – this involves checking the Cardholder has a valid subscription to use mobile payment service.
- Mobile Device and Assembly Eligibility Check – this involves checking the components are MasterCard approved.
- Access Control Management of Mobile Payment Application – this involves the security binding/unbinding of UI Application to the Mobile Payment Applications and their associated Security Domains in SE.
- Security Domain Life Cycle Management – this involves the creation, personalization, management and deletion of Security Domains on Secure Elements.
- Mobile Payment Application Issuance – this involves the downloading, installation, extradition and deletion of a mobile payment application in a Security Domain on a Secure Element.

- Mobile Payment Application Personalization - this involves the insertion of card holder data and card data into a mobile payment application. The process results in a virtual payment card residing on the Secure Element, which can be used by the Cardholder to make a payment at the Point of Sale.
- Post-Issuance Mobile Payment Application Management - this involves the management of a mobile payment application, executed via Issuer Scripting as defined in the EMV and EMV Contactless specifications.

## 3.2 Security Domain Life Cycle Management

Figure 3 shows the roles involved in creating and personalizing Security Domains on Secure Elements. Roles that could potentially be performed by a Trusted Service Manager are indicated by boxes with solid outlines. Roles that are not expected to be fulfilled by a TSM are indicated by boxes with broken outlines. Interactions expected to exist are indicated by arrows with solid lines. Interactions that may exist, depending on the set-up of a particular implementation of a mobile payments ecosystem, are indicated by arrow with broken lines.

Please note again that MasterCard does not mandate a particular division of responsibilities between actors. All actors in a particular ecosystem for mobile payments can assume one or more of the roles indicated in Figure 3, depending on business agreements between these actors.

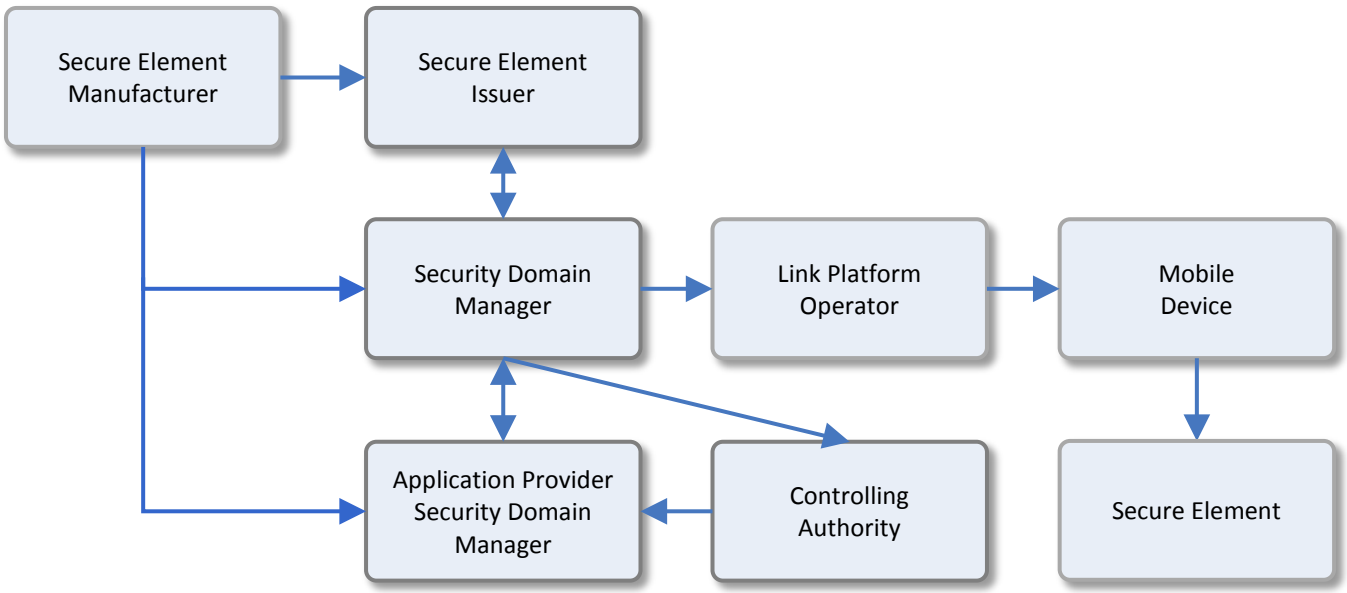


**Figure 3 - Roles involved in Security Domain Life Cycle Management**

Secure Element life cycle management starts with the SEI. This is the owner of the Secure Element, who directly or indirectly issues the Secure Element to the Cardholder. The SEI controls the ISD on the SE.

### 3.2.1 Pre and post issuance creation of Security Domains

For the creation of TSDs and APSDs on the SE, there are in principle two possibilities:

- Pre-issuance creation by the SE Manufacturer, or
- Post-issuance creation by the SEI and/or the SDM, depending on the business agreements between these actors. By definition in this document, these are the only two actors that have a Security Domain with AM or DM privileges. Other parties therefore cannot create SDs.

The possibility of pre-issuance creation is described in reference [2]. Using this possibility, all Security Domains on the SE are created and personalized pre-issuance, but are allocated to a particular actor post-issuance, at the moment that this actor needs a Security Domain on the SE. Allocation means that the SE Manufacturer sends the initial secure channel key set of a particular Security Domain directly to the actor requesting a Security Domain. This usually involves a two-step process. In the first step, the SE Manufacturer sends the Master Key used for a particular Security Domain on all SEs to the actor. This will take place once, at the moment this actor is connected to the ecosystem. In the second step, the SE Manufacturer sends the derivation data used for deriving the keys for a particular Security Domain on a particular SE to the actor. This will take place every time the actor requests a Security Domain on a particular SE. This means that the SEI has no knowledge of the initial secure channel key set.

MasterCard recommends that implementations use post-issuance creation of all Security Domains except the ISD and, if present, the CASD. This means that the SEI creates a TSD, or the SDM creates an APSD at the moment it is needed. It does so by setting up a secure channel to the ISD, or the TSD, and sending the CCM commands to install and extradite the Security Domain. A SDM can create a Security Domain either in Authorized Management (AM) mode or in Delegated Management (DM) mode. In AM mode, the SDM is able to perform CCM operations without explicit prior authorization by the SEI. In DM mode, the SDM needs a Receipt for every CCM operation it performs on the Secure Element. Such a Receipt is checked on-card by the Security Domain having the Receipt Verification privilege, which usually is the ISD.

MasterCard makes no distinction between SDMs operating in AM mode or in DM mode. In both cases, MasterCard's requirements are identical.

### 3.2.2 Key rotation and Controlling Authority

After a new Security Domain has been created, the SEI (or the SDM) personalizes it with an initial secure channel key set. In accordance with the EMVCo requirements in reference [14], this initial key set is derived from a Master Key. MasterCard mandates that a different Master Key will be used for every actor requesting a Security Domain. The Master Key is exchanged once between the actor creating the Security Domains and the actor that will

be the owner of the new Security Domain. For every new Security Domain, also the derivation data and method used to derive the Security Domain keys from the Master Key is communicated to the owner of the new Security Domain.

Once the new Security Domain is created and the actor that has requested it has knowledge of its initial secure channel key set, this actor can set up a secure channel to the new Security Domain. However, the actor who created this Security Domain also knows this key set. Therefore, MasterCard mandates the new owner of the Security Domain to replace the initial secure channel key set by a new key set, using a Master Key known solely by them. This is known as key rotation. Note that two separate key rotation processes may take place in the lifetime of a Secure Element:

- When a new SDM becomes part of the ecosystem, it may request a TSD on every SE in the ecosystem. The SDM will rotate the keys of each new TSD it gets to manage.
- When a new APSDM becomes part of the ecosystem, it may request an APSD on every SE in the ecosystem. The APSDM will rotate the keys of the new ASPD it gets to manage.

However, there are some inherent risks in this key rotation process. The new owner of the Security Domain can replace the initial secure channel key set only by using that same initial secure channel key set to set up a secure channel to the Security Domain. This means that there is a risk that the SE Manufacturer (in case of pre-issuance creation of Security Domains) or the SEI or SDM (in case of post-issuance creation of Security Domain may decrypt the messages used to replace the keys and thus obtain knowledge of the new key set. To do so, they must of course be able to intercept the messages. Especially for SEIs or SDMs who operate its own LPO platform over which these message are sent, this may however not pose a problem.

To counter this risk, GlobalPlatform introduced the Controlling Authority in reference [3] and [6]. The GlobalPlatform in reference [1] calls this role the Confidential Key Loading Authority, which reflect its actual responsibilities. The Controlling Authority is an actor that has a separate Controlling Authority Security Domain (CASD) on the SE. A CASD, if it is present, must be created and personalized before the SE is delivered to the SEI. The CASD contains a private key, which is part of an asymmetric key pair. An actor requesting a new Security Domain on a Secure Element may use the CASD public key to encrypt the new key set. Since the actor that created the new APSD or TSD does not have the corresponding private key, they do not have a possibility to get to obtain knowledge of the new key set.

Note that there must be a way for SDMs and APSDMs to obtain the CASD public key certificate for the CASD on the Cardholder's SE. Depending on the set-up and on agreements between actors, these actors also need a Controlling Authority root certificate, in order to be able to verify the authenticity of a CASD certificate.

In accordance with EMVCo, reference [14], MasterCard currently does not require support for the CASD. However, MasterCard recognizes the fact that if there is no Controlling Authority present in an ecosystem for mobile payments, there is a risk that a SE Manufacturer, SEI or SDM may get to know the secure channel keys of the APSD during the key rotation process of the APSD. Eventually, these actors may then also get knowledge of the MasterCard or Card Issuer assets loaded into a payment application that is associated with the APSD, such as PINs and payment application keys. Therefore, MasterCard recommends that during key rotation processes, the new secure channel keys are encrypted by a CASD public key, such that the confidentiality of these keys is guaranteed, also with respect to the SE Manufacturer, SEI and/or SDM. If a Controlling Authority is present in the ecosystem and the CASD is involved in all key rotation processes, MasterCard will consider this as sufficient to ensure the full confidentiality of MasterCard assets. However, if no CASD is involved in any key rotation process, MasterCard may require the relevant involved actors involved (APSDM, SDM, SEI and/or SE Manufacturer) to comply with MasterCard requirements in reference [4]. For exact requirements, see Chapter 4 of this document.

# 3.3 Mobile Payment Application Issuance

The issuing process of a MasterCard M/Chip Mobile application starts with the presence of an Application Provider Security Domain on an SE and results in a MasterCard M/Chip Mobile application instance that is ready to be personalized. This process can be divided into 3 sub-processes:

1. Eligibility checking of the Mobile Device and the Assembly,
2. Loading of an ELF containing MasterCard M/Chip Mobile application code,
3. Instantiation of a payment application instance from the ELF.

These processes are each discussed in the next subsections.

## 3.3.1 Eligibility Checking of Mobile Device and Assembly

Before a MasterCard M/Chip Mobile application may be issued, MasterCard requires that an eligibility check is done to make sure that all components that the Cardholder intends to use with the new M/Chip Mobile application are approved by MasterCard. These components are:

- A Mobile Device that is able to set up the remote connection needed to provision the M/Chip Mobile application,
- A Secure Element that will contain the M/Chip Mobile application data and the personalization data,
- The NFC Antenna that is used for the proximity communication to the contactless card reader during a payment transaction,

- The NFC Controller that controls the low-level behavior of the NFC Antenna and communicates with to the Secure Element.

MasterCard refers to the combination of the last 3 components as the Assembly. When an active payment application is present on the SE, the Assembly enables a contactless payment and can therefore be tested for functional compliance with MasterCard M/Chip Mobile requirements.

The question of the eligibility of all components is thus directly related to the question of the relationship between the Assembly and the Mobile Device. There are potentially many ways in which the components of the Assembly can be connected to a Mobile Device. Some examples include:

- All components are embedded in the Mobile Device,
- The Secure Element is removable from the Mobile Device, whereas the NFC antenna and the NFC controller are embedded in the device (Note that in this situation, if the Secure Element is on a UICC and is communicating to the Mobile Device via the Single Wire Protocol (SWP), MasterCard M/Chip Mobile NFC Mobile Device Approval Guide, see reference [19] is applicable.
- All components are removable from the Mobile Device. This includes situations in which
    - All components, including the antenna, are on a single removable chip, either a UICC or a microSD card,
    - The antenna is a separate component from the SE and the NFC Controller, which in turn may or may not be combined on a single chip.

The MasterCard requirements and testing processes for Mobile Devices and Assemblies (including Secure Elements) are out of scope of the current document. However, these processes will lead to a number of components or combinations of components that are approved by MasterCard. The purpose of the eligibility check is to make sure that the Cardholder only uses approved components for making contactless payments using MasterCard M/Chip Mobile. The Card Issuer is required to ensure that approved components are used.

Figure 4 shows the roles that are (potentially) involved in these eligibility checks. (Note that at least two additional eligibility checks must take place before a mobile payment application can be provisioned:

- The Cardholder must be eligible for a mobile application. It is the responsibility of the Card Issuer to carry out this check before starting the provisioning process, and this check is out of scope of the current document
- The mobile subscription of the Cardholder must be commercially and technically eligible for provisioning mobile payment applications. For example, if the subscription does not include a data plan, provisioning may be impossible. This check is out of scope of the current document.)

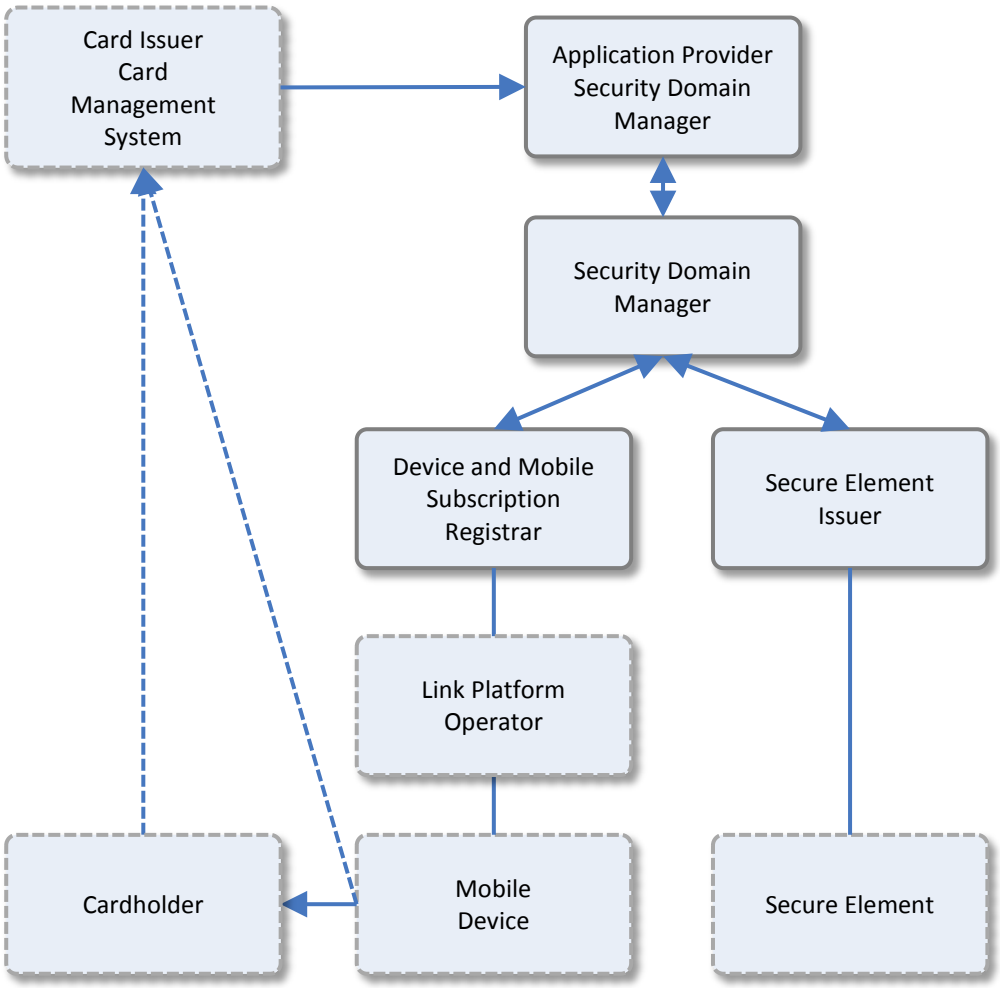


**Figure 4 - Roles involved in the eligibility check of SEs and Mobile Devices**

Since the process that a Cardholder must use to apply for a MasterCard M/Chip Mobile application can be very different each implementation, and the way in which the process checks the eligibility of the SE and the Mobile Device is organized, can be very different. The example process depicted in Figure 4 is partly based on the GlobalPlatform Messaging Specification (see reference [2]), and is as follows:

1. The Cardholder signs up with the Card Issuer for a mobile payment application, either via the Mobile Device or via some other means.
2. The Card Issuer starts the provisioning process by sending a request to the APSDM.
3. The APSDM requests the SDM to carry out an eligibility check for the SE and the Mobile Device (including the NFC controller and the NFC antenna).

4. The SDM requests the identifier for the Cardholder's Secure Element from the SEI and the identifier for the Cardholder's Mobile Device from the Device and Mobile Subscription Registrar (DMSR). GlobalPlatform proposes in reference [2] that the result of the eligibility check is not an identifier for the used SE and Mobile Device, but an identifier of a profile which indicates the technical capabilities of the SE and the Mobile Device. MasterCard does not consider this as a sufficient eligibility check. Secure Elements and Mobile Devices shall not only have all technical capabilities to perform mobile payment transactions, but shall also be explicitly approved by MasterCard for implementation with MasterCard M/Chip Mobile.
5. The SDM checks whether these identifiers are listed in a database containing all MasterCard-approved devices (Mobile Devices, SEs and/or Assemblies). For Mobile Devices, an identifier that could potentially be used is the International Mobile Equipment Identity (IMEI). For UICC Secure Elements, the International Mobile Subscriber Identity (IMSI) or Integrated Circuit Card Identifier (ICCID) may be available for this purpose. For other types of Assembly components, obtaining a unique identifier that can be looked up in a database may be difficult. This database may be kept by the SDM itself or by another actor, including MasterCard.
6. In case of a positive result (all devices used by the Cardholder are approved by MasterCard for MasterCard M/Chip Mobile applications), the SDM carries on with the provisioning process. If not, the SDM shall stop the provisioning process.

Many variations on this process are possible:

- In the first place, the process will be very dependent on the actual architecture of the NFC controller, the NFC antenna and the Secure Element within the Mobile Device, as explained above.
- The process will also be highly dependent on the chosen system architecture. For example, implementations may allow the Cardholder to sign up for a mobile payment application only via a specific application on the same Mobile Device that will be used for making mobile payments. By making sure that this specific application can only be installed or used on a MasterCard-approved Mobile Device, the eligibility check for the Mobile Device is implicitly done already at the moment the Cardholder signs up with the Card Issuer. The eligibility check for the Secure Element could in principle also be done upfront. An explicit eligibility check process by the SDM or any other actor may not be needed in this case.
- Thirdly, different choices may be made regarding the storage of information. For example, the DSMR role may be taken up by a separate actor, but also by the LPOs or a TSM.
- Finally, note that this document assumes that the installation of a payment application instance is the responsibility of the SDM, whereas the personalization of such an application instance is performed by the APSDM. In both process, MasterCard assets are involved. Therefore,

both roles have the responsibility to carry out eligibility checks. In order to limit cardholder inconvenience, eligibility checks should be combined to the maximum extent possible.

### 3.3.2 Mobile Payment Application ELF Loading

The second step in issuing a MasterCard M/Chip Mobile application is to load an Executable Load-File (ELF) into the SE. The ELF contains the application code, but is not a functioning application (executable) itself. A Security Domain having the AM or DM privileges can instantiate one or more functioning MasterCard M/Chip Mobile applications from the ELF.

The SE Manufacturer may load the ELF on the Secure Element before the SE is issued. Alternatively, the SEI or SDM may do this after the SE is issued, using a remote connection. In the latter case, if the SEI is responsible for loading the ELF on behalf of SP, MasterCard recommends that the authenticity of the ELF is ensured by means of either the DAP Verification or Mandated DAP verification mechanism described by GlobalPlatform in reference [5].

The ELF that is loaded on the SE may be associated with the ISD, a TSD, an APSD or any other SD on the SE.

### 3.3.3 Mobile Payment Application Instance Installation

The third step in issuing a MasterCard M/Chip Mobile application is the installation of the MasterCard M/Chip Mobile application instance from the ELF. The result of this step is a MasterCard M/Chip Mobile application instance that is ready to be personalized. Like the previous step (ELF loading) this process may be carried out either pre-issuance by the SE Manufacturer, or post-issuance by the SEI or SDM.

## 3.4 Mobile Payment Application Instance Personalization

Personalization of a payment application instance turns a blank application instance into a virtual payment card by storing all necessary cardholder data and card data. Figure 5 shows the roles that are involved in the personalization process. Roles that potentially could be taken up by a TSM are indicated by boxes with solid outlines, while roles that are not expected for a TSM are shown by boxes with broken outlines.

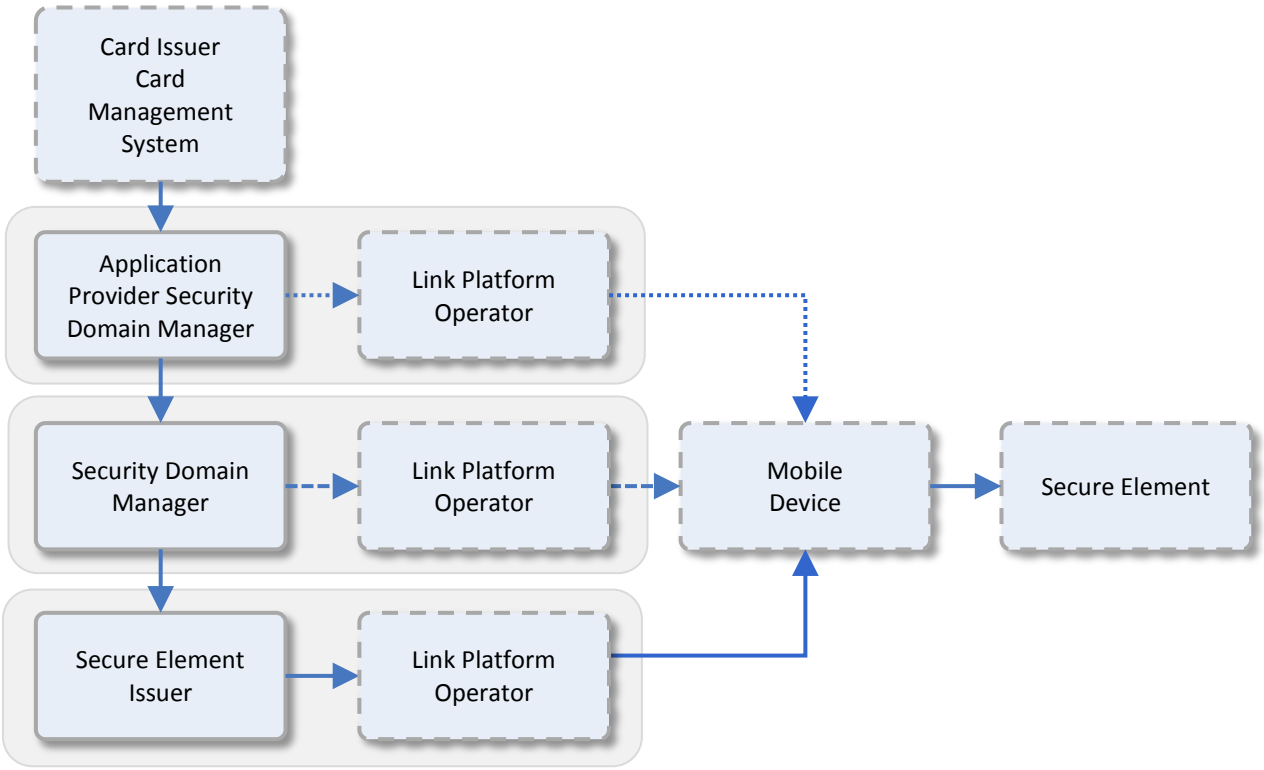


**Figure 5 - Roles involved in the Personalization of the MasterCard Mobile**

The APSDM plays the same role in the issuing process of a MasterCard M/Chip Mobile application as a Card Personalization Bureau does in the issuing process for traditional payment cards. It takes the cardholder data and card data delivered by the Card Issuer and encapsulates them into a script which can be delivered directly to the APSD on the SE.

Figure 5 assumes that the APSDM does not operate a LPO itself. Therefore, it sends the personalization script in its entirety to the SDM. The SDM is, possibly in cooperation with a separate actor acting as LPO, responsible for any further encapsulation that is necessary to send the script to the SE. Note that if the APSDM does operate a LPO, MasterCard considers the APSDM to be a SDM as well.

After personalization, the MasterCard M/Chip Mobile application is ready for use by the Cardholder.

## 3.5 Post-Issuance Management of Payment Application

After a MasterCard M/Chip Mobile application has been issued, the Card Issuer may need to remotely manage the application. These management functions involve administration of the MasterCard M/Chip Mobile application, such as changing a PIN, unblocking a blocked PIN, or management of the risk parameters inside the application.

The EMV and EMV Contactless specifications define Issuer Scripts and Issuer Updates that can be sent to a payment application in order to perform post issuance application management. For traditional dual interface cards, these scripts can be sent to the payment application only in the course of an online payment transaction, using the MasterCard payment network. For MasterCard M/Chip Mobile applications this option remains available. However, in addition there is also the option of sending Issuer Scripts and Issuer Updates over the remote OTA channel offered by a Link Platform Operator or OTI through an User Interface Application in the mobile device. There are a number of use cases for which using these channels may be more convenient, such as:

- When the Card Issuer triggers the sending of the Issuer Script during a payment transaction, but the script cannot be delivered via the Point of Sale (PoS) terminal. This may be the case for example when the PoS terminal does not support a 'double tap' by the Cardholder.
- When the sending of the Issuer Script is not triggered by the Card Issuer, but by the Cardholder or the User Interface Application.

If Issuer Scripts and Issuer Updates must be sent to a MasterCard M/Chip Mobile application residing on a Secure Element in a Mobile Device, Card Issuers need a way to do so. In principle, this can be done via any SDM or APSDM via a Link Platform Operator, connecting the Card Issuer systems responsible for creating the Issuer Scripts and the mobile payment application for which they are intended.

The contents of an Issuer Script are very specific to the exact internal state of a MasterCard M/Chip Mobile application. In general, if a payment transaction (or any other action) is performed in the time between the moment the Card Issuer prepares the Issuer Script and the moment the script arrives at the application, the script will fail. Therefore the time that elapses between the triggering of an Issuer Script and the moment it is delivered to the application must be as short as possible.

# 4 Determining your Role and the scope of requirements

MasterCard will use the following questions to help determine whether a particular vendor is fulfilling one of the roles defined in this document, and consequently must fulfill the requirements for that particular role.

Note that one vendor may take on different roles in different MasterCard M/Chip Mobile ecosystems. For example, a TSM vendor may be a SDM in one ecosystem, managing a Security Domain with CCM privileges and being responsible for remotely loading and installing MasterCard M/Chip Mobile applications. That same vendor may be an APSDM in another ecosystem, where the vendor is responsible for personalizing MasterCard M/Chip Mobile

application instances. The questions in this section must therefore be answered separately for all capabilities of the TSM.

If a vendor does not yet actively participate in some ecosystem(s), but intends doing so, these questions can be answered with regards to the functions the vendor wishes to perform.

Also note that one vendor may take on different roles within one ecosystem. For example, the roles of SE Manufacturer and Controlling Authority may be fulfilled by one and the same actor. SEIs and SDMs will often also be Link Platform Operators. In fact, all roles can be combined. An actor assuming more than one role shall comply with all requirements pertaining to all roles he fulfills.

For each of the roles in this section, if the associated questions are answered affirmatively, it is likely that MasterCard will require the vendor in question to comply with the requirements for that role. However, the exact set of requirements for a specific vendor in a specific MasterCard M/Chip Mobile ecosystem shall always be at MasterCard's sole discretion.

If a vendor is required to comply with the requirements for any of the roles defined in this document, that vendor shall also comply with the generic requirements in section 5.2 Generic requirements, if applicable.

# 4.1 Determining Your Role

## 4.1.1 Secure Element Issuers

Does your TSM system

- Setup root Security Domain to grant other actor in the ecosystem to manage the mobile provisioning?
- Manage the SE lifecycle?
- Manage the SE content?
- Perform eligibility check on mobile subscription?
- Provide mobile device capabilities to other actor within the ecosystem?
- Provide SE capabilities to other actor within the ecosystem?

## 4.1.2 Security Domain Managers

Does your TSM system

- Perform eligibility check on SE?
- Perform eligibility check on mobile device?
- Manage the service and/or end-user lifecycle?
- Manage the SE content?

- Manage the access control for UI application to mobile payment application?

Note: if one or more mobile payment application in the SE are directly associated to your Security Domain, MasterCard may consider you to be an APSDM as well.

### 4.1.3 Application Provider Security Domain Managers

Does your TSM system

- Prepare the EMV data?
- Personalize the mobile payment application?
- Manage the issuer scripts for post-issuance?

Note: if the privileges of your Security Domain include Authorized Management or Delegated Management, MasterCard will consider you to be a SDM as well.

### 4.1.4 Secure Element Manufacturers

Do you manufacture Secure Elements intended to store MasterCard assets?

### 4.1.5 Link Platform Operators

Are you responsible for operating an OTA platform to setup a secure connection to the UICC to transport the mobile provisioning script via BIP/CAT-TP, SMS using SCP80 or HTTP (admin agent in UICC, see references [7] and [13]) with SCP81?

Note: if the privileges of your Security Domain include Authorized Management or Delegated Management, MasterCard will consider you to be a SDM as well.

### 4.1.6 Controlling Authorities

Do you have knowledge of the asymmetric key pair in a Controlling Authority Security Domain on a Secure Element intended to enable the confidential setup of the initial secure channel keys for Security Domain managing MasterCard assets?

Do you have knowledge of the secure channel keys and the DAP Verification key(s) of a Security Domain having the Mandated DAP Verification privilege on a Secure Element containing an ELF containing MCM application code?

## 4.2 Determining the Scope of Requirements

The section describes which sets of requirements are applicable for each role. It also describes whether the vendor performing the role needs to be GVCP certified.

### 4.2.1 Secure Element Issuers

If the SEI has access to EMV personalization data or post issuance EMV scripts either directly or via decryption using known keys, then the SEI SHALL be certified by GVCP and comply with the following sets of requirements from this document:

- 5.2 Generic requirements
- 5.3 Requirements for Secure Element Issuers

### 4.2.2 Security Domain Managers

SDMs SHALL be certified by GVCP and comply with the following sets of requirements from this document:

- 5.2 Generic requirements
- 5.4 Requirements for Security Domain Managers

### 4.2.3 Application Provider Security Domain Managers

APSDMs SHALL be certified by GVCP and comply with the following sets of requirements from this document:

- 5.2 Generic requirements
- 5.4 Requirements for Security Domain Managers

### 4.2.4 Secure Element Manufacturers

Secure Element Manufactures are out of scope for TSM approval.

### 4.2.5 Link Platform Operators

If the LPO has access to EMV personalization data or post issuance EMV scripts either directly or via decryption using known keys, then the LPO SHALL be certified by GVCP and comply with the following sets of requirements from this document:

- 5.2 Generic requirements
- 5.6 Requirements for Link Platform Operators

### 4.2.6 Controlling Authorities

Controlling Authorities are out of scope for TSM approval.

# *5 Functional Requirements*

This chapter contains MasterCard's requirements for each of the roles introduced in chapter 2 and explained in more detail in chapter 3.

# 5.1 Format of requirements

This section explains the format and definitions of terms used to specify the requirements.

## 5.1.1 Functional requirements groups based on roles

The functional requirements groups are based on the role descriptions given in previous chapter. There is also a generic requirements group. The groups of requirements must be applied depending on the roles played by the TSM that have been determined using chapter 4.

## 5.1.2 Use of equivalent and future technologies

Some requirements and recommendations specify the use of specific existing technologies. The use of other equivalent technologies or improved future technologies is allowable at the discretion of MasterCard.

## 5.1.3 Background and Rationale

Individual requirements or groups of requirements may contain background information or a rationale explaining the reasons for the requirement. The background and rationale are there to provide context for the requirements and are not considered as requirements themselves. The actual requirements are stated separately.

## 5.1.4 Definition of a Requirement

A requirement is a statement that is mandatory and must be applied to the TSM solution (if contained within an applicable role based requirements group). When a statement is a requirement, it will be emphasized by the use of the word ‘SHALL”. Requirements may also be written in the negative, i.e., “SHALL NOT”.

## 5.1.5 Definition of a Conditional Requirement

A conditional requirement is a statement that is mandatory and must be applied to the TSM solution if a condition is met (and if contained within an applicable role based requirements group). When a statement is a conditional requirement, it will be emphasized by the use of the word ‘SHALL” but will also be prefaced by a condition. Conditional requirements may also be written in the negative, i.e., “SHALL NOT”.

## 5.1.6 Definition of a Recommendation

A recommendation is a statement that should be met by the TSM solution. This means that in particular circumstances valid reasons to ignore the statement may exist, but the full implications must be understood and carefully weighed before choosing a different course. When a statement is a recommendation, it will be emphasized by the use of the word ‘SHOULD”. Recommendations may also be written in the negative, i.e., “SHOULD NOT”.

## 5.2 Generic requirements

### 5.2.1 Requirement GEN_01 - SD key diversification

All symmetric keys of a Security Domain SHALL be unique to that Security Domain. This means that

1. Keys SHALL be diversified based on a globally unique identifier for the SE on which they are residing.
2. Keys SHALL be diversified based on a SE-unique identifier for the Security Domain they belong to.

Rationale: This follows from the basic principle that keys shall never be shared between unrelated parties. Diversifying keys based on an SE identifier prevents keys from being shared between two (or more) Cardholders. Diversifying keys based on a SD identifier prevents keys from being shared between two or more banks.

### 5.2.2 Conditional Requirement GEN_02 – SE access control

Condition: Applicable if the Mobile Device supports the security mechanism for SE access control, see reference [12].

All MasterCard asset, including MasterCard M/Chip Mobile application instances on a SE SHALL be protected by an access control mechanism.

The access control mechanism SHALL ensure that only authorized applications on the Mobile Device that are allowed access to a specific Security Domain or application instance. Access control may be managed by the SEI, the SDM and/or the APSDM.

Rationale: MasterCard considers the Mobile Device as an insecure environment, potentially hosting malware and other threats to the security of the MasterCard assets on the SE. Therefore, only trusted applications on the Mobile Device should be granted access to MasterCard assets.

### 5.2.3 Requirement GEN_03 – TSM system identification

The TSM system deployed at the facility SHALL be identifiable with an unique system name and version number representing the code build of all individual software modules and the configuration setup to operate in specific roles within a NFC ecosystem.

Rationale: Each TSM setup is different, and hence it is important to track the TSM system when TSM vendor registers for upgrade or renewal approval.

# 5.3 Requirements for Secure Element Issuers

## 5.3.1 Functional

### 5.3.1.1 Requirement SEI_01 – SE lock and terminate policies

An SEI SHALL have documented policies to determine under which conditions the SEI will lock or terminate a SE on which a personalized MasterCard M/Chip Mobile application instance is residing.

Rationale: By default, SEIs have the ability to remotely lock or terminate a SE that they have issued. However, an unwarranted locking or termination of a SE on which an active MCM application is residing must be prevented.

### 5.3.1.2 Requirement SEI_02 – Instance lock and delete policies

An SEI SHALL describe and comply with documented policies to determine under which conditions the SEI will lock or delete a MCM application instance.

Rationale: By default, SEIs have the ability to remotely lock or terminate any application instance residing on a SE that they have issued. However, an unwarranted locking or termination of an active MCM application must be prevented.

### 5.3.1.3 Requirement SEI_03 - Lock and terminate policies

An SEI SHALL inform MasterCard and the Card Issuer of a MCM application on the policies described in SEI_01 and SEI_02, before any MCM application is loaded on the SE owned by SEI.

Rationale: MasterCard and the Card Issuer need to know the circumstances (if any) under which the SEI will lock or terminate a SE on which a MCM application is present.

### 5.3.1.4 Recommendation SEI_04 – TSD/LPO SD cumulative granted memory

An SEI SHOULD assign the cumulative granted memory to each TSD/LPO SD with AM/DM privilege. See reference [8].

Rationale: Having the cumulative granted memory set for each TSD/LPO SD prevents any actor from exceeding its memory allocation and resulting in denial-of-service to other service providers, sharing the same SE.

### 5.3.1.5 Requirement SEI_05 – Profile identifier for device capability

An SEI SHALL maintain an up-to-date registry of the devices associated with its mobile subscriptions and to provide the pre-agreed identifier of the device capability profile to SDM during eligibility check.

Rationale: SDM depends on SEI to provide accurate device profile identifier to perform eligibility check on mobile device.

#### 5.3.1.6 Requirement SEI_06 – Profile identifier for SE capability

An SEI SHALL maintain an up-to-date registry of all issued SE identifier and share with SDM the pre-agreed identifier of the SE capability profile.

Rationale: SDM depends on SEI to provide accurate SE profile identifier to perform eligibility check on SE.

#### 5.3.1.7 Conditional Requirement SEI_07 – CA certificate retrieval

Condition: Applicable if the TSM with the role as SDM or APSDM has no OTA link to the SE.

An SEI SHALL retrieves the CA certificate to other TSM in the ecosystem prior to confidential initial key setup for Security Domain.

Rationale: SEI has OTA capability and authorized access to CASD in SE.

#### 5.3.1.8 Requirement SEI_08 – Forbidden role as CA

An SEI SHALL NOT assume the role as CA.

Rationale: The CA role is one that mediates between the SEI and Card Issuer, and must be a neutral third-party.

#### 5.3.1.9 Conditional Requirement SEI_09 – UI application binding / unbinding

Condition: Applicable if the mobile device supports the security mechanism - SE access control, see reference [12].

An SEI SHALL provide UI application binding / unbinding from other requesting actor in the ecosystem.

Rationale: SEI has authorized access to ARA-M in SE or ARF if the UICC uses the file-system structure.

#### 5.3.1.10 Recommendation SEI_10 – Rule settings for UI application binding

An SEI SHOULD screen all UI application binding requests from other actor to ensure only rule settings involved SDs and application instances in SE are granted for associated SDM or APSDM. It SHOULD use only the ARA-M for rules setting for centralized control.

Rationale: When the SEI grants ARA-C for rule management to more than one actor, there is a possibility that each actor can set rules to grant access to the other actor's application instance in SE.

#### 5.3.1.11 Conditional Requirement SEI_11 – Change notification for mobile subscription identifier/life-cycle state

Condition: Applicable if the SEI is an MNO and uses the UICC for hosting the MCM application in SE.

With reference to [2], an SEI SHALL notify the SDM when:

1. Mobile subscription identifier used for OTI/OTA communication to a device hosting a UICC has changed

2. Mobile subscription is suspended / activated, terminated or restricted.

Rationale: It is important for the SEI to notify the SDM on changes to the mobile subscription identifier or mobile subscription life cycle state so that the SDM can perform the relevant OTI/OTA and backend actions on their information system.

#### 5.3.1.12 Conditional Requirement SEI_12 – SE life-cycle notification

Condition: Applicable if the SEI is a MNO and uses the UICC for hosting the MCM application in SE.

An SEI SHALL notify the SDM when:

1. SE is renewed

2. SE is suspended / activated or terminated

3. Device hosting SE has changed

4. Device hosting SE is either lost or stolen

5. Mobile subscription linked to a device hosting a SE has changed

Rationale: It is important for the SEI to notify the SDM on changes to the state of the SE cycle state so that the SDM can perform the relevant OTI/OTA and backend actions on their information system.

#### 5.3.1.13 Conditional Requirement SEI_13 – Load, Install, extradite and delete of payment application load-file and instances

Condition: Applicable if the SEI grants no CCM privilege to TSD.

The SEI SHALL use the ISD or SSD with AM privilege to load, install and extradite payment application load-file and instances to the APSD during service download or delete payment instance in APSD during service termination.

Rationale: Only ISD or SSD with AM privilege is allowed to perform CCM on behalf of TSD when it has no CCM privilege (see APSDM_02).

#### 5.3.1.14 Conditional Requirement SEI_14 – Authorization to load, install, extradite and delete of payment load-file and instances

Condition: Applicable if SEI_13 is applied.

The SEI SHALL be authorized to initiate the install, extradite and delete of payment load-file and instances from the messaging request of SDM/APSDM. Under no circumstances, the SEI or any other unauthorized entities are allowed to initiate the install, extradite to APSD, or delete of payment instance in APSD.

Rationale: Only authorized SDM/APSDM with secured interface to the SEI is allowed to control and request for the load, install, extradite and delete of payment application load-file and instances for Simple Mode deployment.

### 5.3.2 Security

#### 5.3.2.1 Requirement SEI_15 – Secure messaging for card content management commands

All remote CCM commands (install, extradition, load, delete, and registry-update) involving TSD, APSD, ELF with MCM application code, MCM application instance SHALL be secured with one of:

1. Secure Channel Protocol ‘80’
2. Secure Channel Protocol ‘81’
3. Secure Channel Protocol '02' i=55 over Secure Channel Protocol ‘80’/’81’,
4. Secure Channel Protocol '03' i=00/10 over Secure Channel Protocol ‘80’/’81’

#### 5.3.2.2 Requirement SEI_16 – Minimum security level for card content management commands

All remote CCM commands (install, extradition, load, delete, and registry-update) involving TSD, APSD, ELF with MCM application code, MCM application instance SHALL be established in a secure session with a minimum security level set with C_MAC.

## 5.4 Requirements for Security Domain Managers

### 5.4.1 Functional

#### 5.4.1.1 Conditional Requirement SDM_01 – TSD AID structure for authorized management

Condition: Applicable if a TSD has the Authorized Management privilege.

The TSD AID SHALL be structured as ‘A0 00 00 01 51 54 44 00 00 00 00 00 B2 02 1x 00’, where x is a nibble with hexadecimal value ‘0’ to ‘F’. For every SE, TSD AIDs SHALL be assigned in ascending order, starting with x = ‘0’ and increasing x by 1 for every next TSD. Other AID structure may be allowed at the discretion of MasterCard.

Rationale: This requirement is in accordance with reference [14].

#### 5.4.1.2 Conditional Requirement SDM_02 – TSD AID structure for delegated management

Condition: Applicable if a TSD has or will get the Delegated Management privilege.

The TSD AID SHALL be structured as ‘A0 00 00 01 51 54 44 00 00 00 00 00 B2 02 2x 00’, where x is a digit (4 bit nibble) with hexadecimal value ‘0’ to ‘F’. For every SE, TSD AIDs SHALL be assigned in ascending order, starting with x = ‘0’ and increasing x by 1 for every next TSD. Other AID structure may be allowed at the discretion of MasterCard.

Rationale: This requirement is in accordance with reference [14].

#### 5.4.1.3 Conditional Requirement SDM_03 – APSD AID structure

Condition: Applicable if an APSD is dynamically created.

The APSD AID SHALL be structured as the concatenation of a 5-byte RID and an 11-byte PIX, in accordance with ISO 7816-5, reference [17]. The RID SHALL be registered by the SDM to identify APSDs associated with an APSDM. The PIX SHALL be assigned by that same SDM, which SHALL use a unique PIX for every APSDM.

Rationale: The SDM can operate as a TSM Hub, interfacing with one or more APSDMs. It is important that the SDM manages the APSD creation with unique AIDs to avoid SD creation failure.

#### 5.4.1.4 Conditional Requirement SDM_04 – TSD/APSD AID structure

Condition: Applicable if a SD is both a TSD and an APSD as defined in this specification.

The SD AID SHALL be structured as a TSD according to SDM_01 or SDM_02.

#### 5.4.1.5 Requirement SDM_05 – TSD acceptance policy for other SD

The application install parameters for the TSD SHALL set as follows:

1. Accepts every SD with AM privilege can extradite instance to that TSD.

2. Only accepts an ancestor SD with AM privilege, or the ISD, can extradite payment load-file to the TSD.

3. Only accepts deletion of associated instances from ISD if TSD has no CCM privilege.

4. Does not accept extradition of associated instances/load-file from any SD if TSD has no CCM privilege.

Rationale: By defining a strict acceptance policy protects the MasterCard asset within its SD in a shared SE environment.

#### 5.4.1.6 Requirement SDM_06 – TSD proximity access over the contactless interface

The TSD SHALL NOT be configured with proximity access over the contactless interface. See reference [8] on contactless interface availability.

Rationale: By restricting proximity access over the contactless interface prevents unauthorized external access of the TSD.

#### 5.4.1.7 Conditional Requirement SDM_07 – Security Domain hierarchy

Condition: Applicable if there is more than one Card Issuer managed by the SDM.

The SDM SHALL create an APSD for each Card Issuer, associated under the TSD. The hierarchy SHALL be setup with minimum 2-tiers of SDs, and is represented at the top by the parent SD, i.e. the TSD associating all the APSDs at the lower tier. All application instances from a Card Issuer SHALL be associated directly under its represented APSD in SE.

Rationale: Having a separate APSD created for each Card Issuer allows them to implement their policy to customize settings for memory management, communication interface access for various deployment scenarios.

#### 5.4.1.8 Conditional Requirement SDM_08 – Ownership of APSDs under the management of SDM

Condition: Applicable if the SDM manages the APSDs and performs the EMV personalization.

The SDM SHALL use a different keyset for each APSD to secure the personalization for different Card Issuers

Rationale: Having a different keyset to secure each Card Issuer personalization script provides a robust security architecture and limit the scope of security breach.

#### 5.4.1.9 Requirement SDM_09 – Card content management capabilities

A SDM SHALL remotely perform CCM on a SE, as specified in reference [5]:

1. Loading of ELF,
2. Installation of payment application instances,
3. Extradition of payment application instance to another SD,
4. Making selectable of application instances,
5. Deletion of payment application instance or ELF,
6. Updating Registry.

Rationale: SDMs will need these functionalities to carry out their responsibilities, as described in this document.

#### 5.4.1.10 Conditional Requirement SDM_10 – UI application binding/unbinding capabilities

Condition: Applicable if the SEI does not implement centralized management of UI applications binding/unbinding and grants the SDM self-management using the ARA-C.

The SDM SHALL support the binding/unbinding of UI application to associated SD and application instances in SE from requesting APSDM.

#### 5.4.1.11 Recommendation SDM_11 – Script sending capability

A SDM SHOULD provide the script sending functions defined in [2] to enable APSDM without OTA/OTI capability to deliver the application script to the payment application instance in SE.

#### 5.4.1.12 Conditional Requirement SDM_12 – Script content

Condition: Applicable if SDM_11 is supported.

A SDM SHALL NOT stores any scripts in its TSM system once the entrusted scripts are sent successfully on behalf of its requestor.

Rationale: SDM has no further use of the scripts after it is delivered.

#### 5.4.1.13 Recommendation TSM SDM_13 – Memory management

A SDM SHOULD perform memory usage tracking within its TSD.

Rationale: Memory usage tracking is needed to prevent situations in which the loading of an ELF containing MCM application code or the instantiation of a mobile payment application instance from an existing ELF does not succeed due to a lack of available memory on the SE.

#### 5.4.1.14 Conditional Requirement SDM_14 – Service activation

Condition: Applicable if the service is pre-deployed in factory and service activation is only possible through the SDM.

A SDM SHALL activate the payment service when it receives an explicit request from the APSDM after the Cardholder is authenticated with the Card Issuer.

Rationale: A pre-deployed service must remain non-usable till the Cardholder is authenticated through a service activation process.

#### 5.4.1.15 Requirement SDM_15 – Service suspension

For Cardholder request to temporary suspend the payment service or billing issues, SDM SHALL:

1. Remotely lock a payment application using Set Status command defined in [5].
2. Notify the UI application to disable a service to block access to the service.

Rationale: Depending on the reason for service suspension, SE or application lock SHALL be applied.

#### 5.4.1.16 Requirement SDM_16 – Service suspension, verification before instance lock

A SDM SHALL check the identity of the requestor and verify the reason against its service policy before attempting to remotely lock the MCM application instance.

Rationale: Locking an application instance denies the Cardholder the service usage and must be checked legitimately before authorizing an instance lock process.

#### 5.4.1.17 Conditional Requirement SDM_17 – Service suspension, instance lock priority

Applicable if the SDM communicates to the SE via the Admin Agent in mobile device, see reference [13].

A SDM SHALL gotten the lock script ready and push it down immediately to the SE at the next moment when the Admin Agent connects online to the SDM.

Rationale: Locking an application instance through an OTA/OTI channel must be given the highest priority by the SDM to maximize the success rate in the limited time when the UI application goes online and connects to the SDM.

#### 5.4.1.18 Requirement SDM_18 – Service suspension, instance lock retry

A SDM SHALL implement retry policy to send the lock script when previous attempt fails.

Rationale: Locking the instance via OTA/OTI must be repeated till the Card Issuer notifies that the Cardholder account is successfully suspended at the backend.

#### 5.4.1.19 Requirement SDM_19 – Service resumption

For various reasons, a SDM SHALL implement service resumption to:

1. Remotely unlock a SE application using Set Status command defined in [05].

2. Notify the UI application to re-enable a service and reinstate access to the service.

3. Notification to all relevant actors of the ecosystem for backend actions on their information system.

Rationale: A service can be resumed from a suspension and initiated by Card Issuer due to:

1. Previously reported lost/stolen of mobile device was found and reported by Cardholder

2. Resolution of billing issues

3. Cardholder request for reinstatement from a previously temporary suspended payment service.

#### 5.4.1.20 Requirement SDM_20 – Service resumption, verification before instance unlock

A SDM SHALL check the identity of the requesting actor and verify the reason against its service policy before attempting to remotely unlock the MCM application instance from a locked state.

Rationale: Unlocking an application instance enables the service usage and must be checked legitimately before authorizing an instance unlocking process.

#### 5.4.1.21 Requirement SDM_21 – Service renewal

A SDM SHALL implement service renewal to remotely:

1. Delete an existing MCM application instance.

2. Instantiate a new MCM application instance.

3. Extradite the new instance to an APSD associated with the requesting APSDM.

Rationale: A service renewal is needed for:

1. Soon to expired Cardholder account

2. Replacement of Cardholder account due to security compromise.

#### 5.4.1.22 Requirement SDM_22 – Service termination

A SDM SHALL implement service termination and delete a MCM application instance.

Rationale: A service termination is needed to support:

1. Cardholder initiated request to unsubscribe.

2. Card Issuer initiated request for billing issue with Cardholder.

### 5.4.2 Security

#### 5.4.2.1 Requirement SDM_23 – Secure messaging for card content management commands

All remote CCM commands (install, extradition, load, delete, and registry-update) involving an APSD, ELF with MCM application code, MCM application instance SHALL be secured with one of,

1. Secure Channel Protocol '02' i=55,

2. Secure Channel Protocol '03' i=00 or i=10

#### 5.4.2.2 Requirement SDM_24 – Minimum security level for card content management commands

All remote CCM commands (install, extradition, load, delete, and registry-update) involving an APSD, ELF with MCM application code, MCM application instance SHALL be established in a secure session with a minimum security level set with C_MAC.

#### 5.4.2.3 Conditional Requirement SDM_25 – Pre-shared TSD initial keys

Condition: Applicable if the SDM exchanges pre-shared TSD initial keys with SEI.

After the SEI dynamically creates the TSD, the SDM SHALL replace the initial keys in the TSD with final keys known only to itself, before using the TSD for CCM.

Rationale: The TSD is only secured after the SDM rotates from initial to final secure channel keys.

#### 5.4.2.4 Conditional Requirement SDM_26 – Delivery of TSD key rotation scripts

Condition: Applicable if SDM_25 is applied.

The TSD key rotation script SHALL NOT be delivered through the SEI's OTA/OTI channel.

Rationale: SEI with knowledge of the pre-shared initial keys can intercept the key rotation script and recover the final secure channel keys.

#### 5.4.2.5 Conditional Requirement SDM_27 – Confidential Setup of TSD Initial Secure Channel Keys

Condition: Applicable if the SE is pre-loaded with a CASD and setup with certificates to enable confidential setup of initial secure channel keys.

The SDM SHALL setup the TSD initial secure channel keys using one of the following scenarios provided by UICC Configuration of ref. [3]:

1. Scenario #1 Pull Model using PK scheme
2. Scenario #2 Pull Model using Non-PK scheme
3. Scenario #2.A Push Model with SDM certificate
4. Scenario #2.B Push Model without SDM certificate

Rationale: To ensure SEI who creates the TSD on behalf of SDM will not have access to the TSD.

#### 5.4.2.6 Conditional Requirement SDM_28 – CA certificate verification

Condition: Applicable if the SDM uses the CASD to confidentially setup the TSD.

The SDM SHALL verify the authenticity of the CA public key certificate retrieved from the CASD in SE before using it to confidentially setup the secure channel keys for TSD.

Rationale: Verification of the CA certificate ensures it is valid and not expired.

### 5.4.3 Mobile Device and Assembly Eligibility Checks

#### 5.4.3.1 Requirement SDM_30 – Eligibility checks prior to load or instantiate

A SDM SHALL check that MasterCard has approved both the Cardholder's Mobile Device and the Assembly for use with a MCM application, before starting any of the following processes:

1. Remote loading of an ELF containing MCM application code to a SE,

2. Remote instantiation of a MCM application instance from an existing ELF on a SE.

In the case that the outcome of this check is that MasterCard has not approved one or more of the above components, the SDM SHALL NOT proceed with any of these processes.

If any mobile device component is nonresponsive to eligibility checks, or responds with data that cannot be interpreted by the SDM, then the SDM shall assume the approval status of that component as “not attained approved” and SHALL terminate the provisioning process.

Rationale: Mobile Devices and Assembly components that are not approved by MasterCard are not compliant with all MasterCard requirements regarding functionality and security. Therefore no MasterCard assets must be provisioned to such components.

#### 5.4.3.2 Requirement SDM_31 – Eligibility check on Mobile Device

The SDM SHALL request from SEI the reference identifier of the device profile associated with the Cardholder’s Mobile Device. The profile identifier SHALL be checked for Mobile MasterCard Approved Mobile Devices.

Rationale: Only approved components including Mobile Device, is allowed to be provisioned with MasterCard payment applications and Cardholder data.

#### 5.4.3.3 Requirement SDM_32 – Eligibility check on Secure Element

The SDM SHALL request from SEI the reference identifier of the SE profile associated with the SE in Cardholder’s Mobile Device. The profile identifier SHALL be checked for Approved MasterCard M/Chip Mobile Secure Elements.

Rationale: Only approved SE in Assembly is allowed for contactless payment with MasterCard M/Chip Mobile.

#### 5.4.3.4 Requirement SDM_33 – Approval checks on the payment application

The SDM SHALL ensure that the payment application that is to be provisioned OTA/OTI has been approved as a part of the SE approval, referenced in requirement SDM_32. This SHALL be done before beginning the transfer of the payment application or of any assets to the mobile device.

#### 5.4.3.5 Recommendation SDM_34 – Load and instantiate retry

The SDM SHALL make sure that the if the loading or instantiation process is not completed, the re-attempt must be performed with a new eligibility check.

Rationale: If a long time passes between the moment the eligibility check took place and the moment an ELF is loaded or a MCM application instance is

instantiated, the components used by the Cardholder may have changed. As an example, a SE may have been inserted into another Mobile Device.

#### 5.4.3.6 Requirement SDM_35 – Eligibility check status to APSDM

The SDM SHALL provide eligibility check function for APSDM to query eligibility and approval status of associated Cardholder's Mobile Device and SE.

Rationale: APSDM depends on SDM for eligible check status for approved components during personalization.

## 5.5 Requirements for Application Provider Security Domain Managers

### 5.5.1 Functional

#### 5.5.1.1 Requirement APSDM_01 – Personalization capability

An APSDM SHALL function as a Personalization Bureau for MCM applications. In particular, an APSDM SHALL remotely and confidentially personalize a MCM application instance residing on a SE in a Mobile Device.

Rationale: APSDMs will need these functionalities to carry out their responsibilities, as described in this document.

#### 5.5.1.2 Requirement APSDM_02 – APSD acceptance policy for other SD

The application install parameters for the APSD SHALL set as follows:

1. Accepts an ancestor SD with AM privilege can extradite instance to the APSD if the TSD has AM privilege. Or accepts an SD with DM under an ancestor SD with AM privilege can extradite instance to the APSD if the TSD has DM privilege. Or accepts ISD can extradite instance to the APSD if the TSD has no CCM privilege.

2. Only accepts deletion of associated instances from ISD if TSD has no CCM privilege.

3. Does not accept extradition of associated instances/load-file from any SD if TSD has no CCM privilege.

Rationale: By defining a strict acceptance policy protects the MasterCard asset within its SD and ensures only authorized SDM can operates on the instances associated under the APSD.

#### 5.5.1.3 Requirement APSDM_03 – APSD proximity access over the contactless interface

The APSD SHALL NOT be configured with proximity access over the contactless interface. See reference [8] on contactless interface availability.

Rationale: By restricting proximity access over the contactless interface prevents unauthorized external access of the APSD.

### 5.5.2 Security

#### 5.5.2.1 Recommendation APSDM_04 – Executable load-file authenticity

The authenticity of any ELF containing MCM application code loaded remotely to a SE SHOULD be protected by the DAP or mandated DAP verification mechanism defined in reference [5], if the APSDM uses the SEI to load the ELF.

Rationale: With DAP or mandated DAP verification ensures only the approved copy of MCM application code from APSDM's is loaded into the SE.

#### 5.5.2.2 Conditional Requirement APSDM_05 – DAP verification

Condition: Applicable if the DAP Verification mechanism is used.

The APSD SHALL perform the DAP verification.

Rationale: APSDM owns the DAP verification key and is loaded into the APSD.

#### 5.5.2.3 Conditional Requirement APSDM_06 – DAP verification scheme

Condition: Applicable if the DAP verification mechanism or mandated DAP verification mechanism is used.

The scheme used SHALL be one of,

1. The AES scheme specified in section 4.1 of reference [9]. For this scheme, the DAP Verification Key SHALL be a 128-bit AES key.
2. The RSA scheme specified in section C.6.1 of reference [5]. For this scheme, the DAP Verification Key SHALL be a 1024-bit RSA public key.
3. The RSA scheme specified in section 4.2 of reference [10]. For this scheme, the DAP Verification key SHALL be a 2048-bit RSA public key.
4. The ECC scheme specified in section 4.1 of reference [10]. For this scheme, the DAP Verification Key SHALL be a 256-bit ECC public key.

Rationale: This requirement is based on section 3.1.5 of reference [11].

#### 5.5.2.4 Requirement APSDM_07 – Asset security

If MasterCard assets are sent over a remote connection to a SE, their confidentiality, integrity and authenticity SHALL be protected by one of the following secure channel protocols:

1. Secure Channel Protocol '02' with implementation option i = '55' (3 Secure Channel Keys, Initiation Mode Explicit, Pseudo- Random Card Challenge, ICV Encryption for C - MAC Session), as defined in Appendix E of reference [5],
2. Secure Channel Protocol '03' with implementation option i = '00' (Random Card Challenge) or i = '10' (Pseudo-random Card Challenge), as defined in reference [9].
3. Secure Channel Protocol '81' may be supported by the implementation as described in reference [7], with support at least for implementation option '01' (TLS v1.0), and support for the following cipher suites:
    a. TLS_PSK_WITH_3DES_EDE_CBC_SHA
    b. TLS_PSK_WITH_NULL_SHA

Rationale: This requirement is based on section 3.1.2 of reference [11].

#### 5.5.2.5 Requirement APSDM_08 – Minimum security level for personalization/issuer script commands

All remote personalization/issuer script commands for a MCM application SHALL be established with a security level set with C_MAC and C_DECRYPTION during a secure session.

#### 5.5.2.6 Conditional Requirement APSDM_09 – Pre-shared APSD initial keys

Condition: Applicable if the APSDM exchanges pre-shared APSD initial keys with SDM.

After the SDM dynamically creates the APSD, the APSDM SHALL replace the initial keys in the APSD with final keys known only to itself, before using the APSD for personalization.

Rationale: The APSD is only secured after the APSDM rotates from initial to final secure channel keys.

#### 5.5.2.7 Conditional Requirement APSDM_10 – Delivery of APSD key rotation scripts

Condition: Applicable if APSDM_09 is applied.

The APSD key rotation script SHALL NOT be delivered through the OTA/OTI channel owned by the SDM.

Rationale: SDM with knowledge of the pre-shared initial keys can intercept the key rotation script and recover the final secure channel keys.

#### 5.5.2.8 Conditional Requirement SDM_11 – Confidential Setup of APSD Initial Secure Channel Keys

Condition: Applicable if the SE is pre-loaded with a CASD and setup with certificates to enable confidential setup of initial secure channel keys.

The APSDM SHALL setup the APSD initial secure channel keys using one of the following scenarios provided by UICC Configuration of ref. [3]:

1. Scenario #1 Pull Model using PK scheme
2. Scenario #2 Pull Model using Non-PK scheme
3. Scenario #2.A Push Model with APSDM certificate
4. Scenario #2.B Push Model without APSDM certificate

Rationale: To ensure SDM who creates the APSD on behalf of APSDM will not have access to the APSD.

#### 5.5.2.9 Conditional Requirement APSDM_12 – CA certificate verification

Condition: Applicable if the APSDM uses the CASD to confidentially setup the APSD.

The APSDM SHALL verify the authenticity of the CA public key certificate retrieved from the CASD in SE before using it to confidentially setup the secure channel keys for APSD.

Rationale: Verification of the CA certificate ensures it is valid and not expired.

#### 5.5.2.10 Conditional Requirement APSDM_13 – Delivery of personalization/issuer script via SEI or SDM's OTA/OTI channel

Condition: Applicable if the APSDM does not have the OTA/OTI capability to deliver its personalization script to the SE remotely.

The scripts SHALL contain application specific only, such as personalization or issuer scripts.

Rationale: SE management commands sent via the script sending causes de-synchronization between TSMs managing the life cycle of the SE.

### 5.5.3 Mobile Device and Assembly Eligibility checks

#### 5.5.3.1 Recommendation APSDM_15 – Personalization retry

An APSDM SHALL make sure that if the personalization is not completed, the re-attempt SHALL be performed with a new eligibility check. See requirement SDM_35.

Rationale: If a long time passes between the moment the eligibility check took place and the moment a M/Chip Mobile application instance is personalized, the components used by the Cardholder may have changed. As an example, a Secure Element may have been inserted into another Mobile Device.

### 5.5.4 Issuer Scripts Delivery

#### 5.5.4.1 Requirement APSDM_16 – Script delivery time limit

An APSDM SHALL ensure that the issuer script is delivered to the intended MCM application within a certain amount of time, starting from the moment the APSDM received the request from the Card Issuer. This amount of time SHALL be no longer than 60 seconds under normal operational conditions (i.e. not under failure or breakdown conditions).

Rationale: The contents of the issuer script are very specific to the exact internal state of a MCM application. In general, if a payment transaction (or any other action) is performed in the time between the moment the Card Issuer prepares the issuer script and the moment the script arrives at the application, the script will fail. Therefore the time that elapses between the triggering of an issuer script and the moment it is delivered to the application must be a short as possible.

#### 5.5.4.2 Requirement APSDM_17 – Script delivery failure

If the APSDM does not succeed in delivering the issuer script (including retries) to the MCM application within the maximum amount of 60 seconds, the APSDM SHALL NOT make any further attempt to deliver the script, and the APSDM SHALL warn the Card Issuer that the Issuer Script could not be delivered.

## 5.6 Requirements for Link Platform Operators

### 5.6.1 Conditional Requirement LPO_01 – LPO SD creation by SEI

Condition: Applicable if the SEI dynamically creates the LPO SD for SDM or APSDM to operate an OTA link to the SE.

The LPO SD SHALL be confidentially setup using a CASD.

Rationale: SDM or APSDM operating an LPO relies on SEI's OTA channel to deliver the final SCP80/SCP81 secure channel keys. The only mode of confidential setup of the LPO SD is through the use of CASD, see reference [3].

### 5.6.2 Conditional Requirement LPO_02 – LPO SD creation by SE Manufacturer

Condition: Applicable if the SE Manufacturer pre-creates the LPO SD for SDM or APSDM to operate an OTA link to the SE.

The LPO SHALL perform key rotation through its own OTA channel before operating as an OTA link to SE for the use of SDM or APSDM.

Rationale: The LPO SD is only secured after the LPO performed the key rotation.

### 5.6.3 Recommendation LPO_03 – LPO capable of card content management

Condition: Applicable if the LPO SD is granted Authorized Management or Delegated Management by the SEI to perform CCM.

The secure channel keys responsible for CCM SHALL be different from the secure channel keys used for transport security. The new keys SHALL be injected after LPO_02 is applied.

### 5.6.4 Requirement LPO_04 – LPO SD proximity access over the contactless interface

The LPO SD SHALL NOT be configured with proximity access over the contactless interface. See reference [8] on contactless interface availability.

Rationale: By restricting proximity access over the contactless interface prevents unauthorized external access of the LPO SD.