EMV
Contactless Mobile Payment

EMVCo Handset Requirements for Contactless Mobile Payment

Version 1.1
November 2015

© 2010-2015 EMVCo, LLC (“EMVCo”). All rights reserved. Any and all uses of the EMV Specifications (“Materials”) shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at http://www.emvco.com/specifications.cfm.

Revision History

The following changes have been made since the publication of Version 1.0:

Assessment of impact of Host-based Card Emulation on Secure Element based payment application

Deletion of references to deprecated technologies (J2ME and SCWS)

Addition of references to new technologies (SEAC, TEE, MSC and OMA)

Contents

© 2010-2015 EMVCo, LLC (“EMVCo”). All rights reserved. Any and all uses of the EMV Specifications (“Materials”) shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at http://www.emvco.com/specifications.cfm.

1 Definitions

Please refer to [ARCH] for the definition of general terms used in these requirements.

The following are the definitions of specific terms used in these requirements.

Handset
A specific type of Mobile Device. That is, a mobile phone handset.

Payment Application
A payment brand specific application hosted and executed within a Secure Element. This is synonymous to the payment applications present on card products.

Mobile Application
A user interface application that makes use of the inherent capabilities of the Mobile Device (e.g. screen, keypad, wide area network etc.). In most cases this is an application targeted for the device/device platform but could potentially be a SCWS application.

Contactless Terminal
A contactless reader/writer. That is, any device capable of initiating communicating with a contactless enabled card or Handset. In the context of this document the contactless terminal is most likely a Point of Sale (POS) terminal but the more generic term is used as the Handset has no way of ensuring that the contactless terminal is actually a POS.

Authorized mobile application
This document assumes that Handsets being used for Contactless Mobile Payment employ a model that allows mobile applications with different trust/security levels to be deployed to the Handset. This same model will restrict access of certain hardware and Handset functionality to specific authorized mobile applications. An authorized mobile application is a mobile application that has passed the relevant approval process and has been deployed with the relevant privileges allowing it to fulfil the requirements specified herein.

2 Abbreviations, Notations, Conventions, and Terminology

2.1 Abbreviations

Please refer to [ARCH] for the descriptions of abbreviations used in these requirements.

The following are the descriptions of specific abbreviations used in these requirements.

RF	Radio Frequency

3 References

The following documents are referenced in this document. The latest version shall apply unless a publication date is explicitly stated.

3.1 EMV Documents

EMV documents are available on the EMVCo Website:

http://www.emvco.com/specifications.cfm.

[ARCH]	Contactless Mobile Payment Architecture Overview

3.2 External Documents

[HCI]	ETSI TS 102 622 – Technical Specification Smart Cards; UICC - Contactless Front-end (CLF) Interface; Host Controller Interface (HCI) (Release V9.4.0 or later)
[HCE]	Host-based Card Emulation – https://developer.android.com/guide/topics/connectivity/nfc/hce.html
[MSC]	EMV NFC Mobile Security Considerations – EMVCo White Paper on Mobile Security Use Cases and Best Practices Version 1.0
[NCI]	NFC Controller Interface (NCI) Specification Technical Specification NFC Forum™ NCI 1.0 NFCForum-TS-NCI-1.0 2012-11-06
[OMA]	simalliance Open Mobile API specification Version 2.05

[SEAC] GlobalPlatform Device Technology – Secure Element Access Control Version 1.0 May 2012

[SWP] ETSI TS 102 613 – Technical Specification
Smart Cards; UICC - Contactless Front-end (CLF) Interface;
Part 1: Physical and data link layer characteristics (Release V9.3.0 or later)

[TEE] GlobalPlatform Device Technology – Trusted Execution Environment System Architecture Version 1.0
GlobalPlatform Device Technology – Trusted Execution Environment Client API Specification 1.0
GlobalPlatform Device Technology – Trusted Execution Environment Internal Core API Specification Version 1.1

4 Scope

As described in [ARCH], the payment system's contactless payment application(s) are hosted within Secure Elements on a contactless enabled Mobile Device which will require certain services and features from the device (in this case a Handset) to effectively enable and manage contactless payment on such devices. Furthermore, from a payment industry perspective, there is the potential that multiple financial institutions, possibly utilizing the payment applications from multiple payment systems, are simultaneously represented on individual Handsets. In order to streamline and facilitate the large scale deployment of the payment related applications and assets to a wide variety of different Handset models and platforms while at the same time ensuring a consistent consumer contactless mobile payment experience, EMVCo has defined a common basic set of functional requirements for these Handsets.

This document is set out to describe and focus on the functional requirements for handsets primarily addressing the following:

- Handset usability to enable consumer management and use of their contactless mobile payments applications/products/device
- Management of Secure Elements which enables discovery and usage of contactless payment applications in a single, or across multiple, Secure Element(s) including the Host-based Card Emulation enabled Handset
- Contactless Module features related to the antenna interface (that is, the interface to contactless payment terminals) and bridging communication between contactless terminals, the device's application processor and any Secure Elements connected to the Contactless Module

A key objective of this document is to promote the development of Handsets according to these requirements so that they can become widely accepted, interoperable and trusted platforms for contactless mobile payments. However, from an acceptance perspective, while EMVCo expects that such Handsets conform to these requirements, EMVCo will only focus on the capabilities of the Handset that are within scope of EMVCo - for example, conformance to [CCPS].

This document does not address the requirements related to:

- The payment system specific payment applications
- The actual Secure Element(s) beyond the very specific interface considerations mentioned above
- The actual payment specific user interface applications and their related functions
- General handset functionality and security
- Handset testing and/or type approval
- Host-based Card Emulation based payment related features

4.1 Target Audiences

This document is intended for:

- Handset manufacturers producing, or planning for the production of, contactless enabled Handsets intending to host EMV based contactless mobile payment products
- Contactless Module (e.g. NFC controller) manufacturers
- Organizations intending to use Handsets for, or in conjunction with, contactless mobile payments (e.g. mobile network operators, issuing banks, transit authorities, etc.)
- Handset application developers
- Payment systems

5 Handset Usability and Payment Product Management

5.1 Application access / Hard / Soft Payment Keys

To enhance the consumer experience with regards to payment, the consumer should be able to launch a preferred payment specific mobile application with as few interactions as possible.

Requirements – Mobile Application Access	
5.1.1.1	The Handset SHOULD provide a quick access method to activate a pre-selected mobile application. *This functionality should be accessible from the highest level of the menu tree (or from the Handset's idle screen), and/or configurable to a hard and/or soft key.*

5.2 Consumer Alerts

To enhance the consumer experience with regards to payment, the consumer may need to be made aware of certain contactless application related occurrences. Some examples of these are:

- A contactless transaction has been initiated and the consumer is alerted of this occurrence
- A contactless transaction has been initiated and continuation of the transaction requires some action (e.g. a confirmation to continue or selection of specific payment card when a conflict is detected) from the consumer
- A contactless transaction has been completed and the consumer is alerted of this occurrence
- A change of Secure Element status is detected when a Secure Element is inserted (or activated) or removed (or made inactive) and the consumer is alerted that their options for payment have increased/decreased

Requirements – Consumer Alerts	
5.2.1.1	Unless the handset has the capability defined in requirement 5.2.1.2 upon receipt of a SELECT command containing a recognized AID over the antenna interface, the Handset SHALL have the capability to launch a predefined mobile application. The launching of the mobile application SHOULD commence immediately on receipt of the SELECT command and while the Handset is still in the proximity of the contactless field.

From a consumer experience point of view, it is important that the launching of the mobile application occur as quickly as possible and is not delayed until after the removal of the Handset from the contactless field. Supporting HCI fulfils this requirement.

5.2.1.2 On receipt of a notification from an application on a Secure Element, the Handset SHALL have the capability to launch a mobile application as defined in the notification.

5.2.1.3 Upon detection of Secure Element insertion or removal, the Handset SHALL have the capability to launch a predefined mobile application.

5.3 Contactless Management

Ideally, activation, user confirmation or user authorization of contactless payment should be facilitated and managed by a relevant authorized mobile application. However, depending on the device manufacturer, similar functionality may also be available at the Handset operating system level which creates the possibility that the consumer may be alerted or prompted to make a choice multiple times during the course of a contactless transaction. If such a Handset functionality exists (e.g. the ability to enable/disable contactless functionality or settings that will require confirmation or the entry of a passcode when a contactless field is detected by the Handset), it must be possible for authorized mobile applications to seamlessly and intuitively override these Handset settings.

The following is a specific example of what these requirements are intended to avoid:

- If, at the Handset system level, a menu option exists indicating that the consumer will be prompted for a passcode each time the Handset enters the proximity of an RF field and the consumer selects this as their preferred option.
- An authorized mobile application managing a payment application is present on the same Handset and requires the entry of a passcode at launch time. (The value of the authorized mobile application passcode will potentially differ from the passcode value used at the Handset system level and each passcode would definitely be managed at a different level).

In this example, if the consumer launches the authorized mobile application with the specific intention of making a contactless payment, they will be prompted for a passcode during the launch sequence of the authorized mobile application and subsequently, when the Handset enters the proximity of the contactless terminal, they will be prompted again to enter a passcode.

Making use of the requirements below will allow the authorized mobile application to disable the prompt for a second passcode and therefore improve the consumer experience.

Requirements – Contactless Management

5.3.1.1 An authorized mobile application SHALL be able to:

- Determine whether the antenna interface is enabled or disabled.
- Enable, and possibly subsequently disable, the antenna interface.

5.3.1.2 If the Handset has a Handset setting to request a confirmation or entry of a passcode when a contactless field is detected, an authorized mobile application SHALL be able to:

- Determine whether such a setting is currently enabled.
- Override, and possibly subsequently re-enable, these setting.

5.4 Presence of a System Icon Indicating Contactless Capability

The consumer should be able to determine whether the Handset is capable of any communication over the contactless antenna by means of a system icon. In most cases this indicator would be in the same “status bar” that contains other connectivity and system indicators such as the current cellular signal strength and the battery power reserve (this is also the same location that the Bluetooth headset symbol is displayed when a headset is paired with the device).

Requirements – System Icon

5.4.1.1 The Handset SHOULD present an indication to the consumer as to whether the device is capable of communication over the antenna interface or not.

5.5 Contactless Mobile Payment in Battery Low /Handset Powered Off Mode

It is not an EMV requirement that a Handset supports the ability to perform a contactless payment transaction when the battery is low or the Handset is powered off. However, if the Handset does support contactless transactions when the battery is low or the Handset is powered off, as there is no means for any mobile application to launch, applications on the Secure Element need to be aware that consumer interaction on the Handset is not possible and take the appropriate action.

Requirements – Power Status

5.5.1.1 The Handset SHALL provide a mechanism that will allow an application on a Secure Element to be aware of the power status of the Handset.

5.6 Consumer Education

The consumer should be aware of the Handset's contactless capability and how best to make use of such.

Requirements – Consumer Education

5.6.1.1 If presentment and orientation of the Handset affects the performance of the contactless communication, the Handset SHOULD have a visual indicator that identifies the position of presentment for the optimized contactless communication.

5.6.1.2 Alternatively, or in addition, documentation SHOULD be provided with the Handset indicating the optimal orientation /position for presentment.

6 Secure Elements

6.1 Single Secure Element

In the case where a Handset supports only one single Secure Element and regardless of whether the Handset is Host-based Card Emulation enabled or not, the following requirements apply.

Requirements –Secure Element

6.1.1.1 The Handset SHALL provide a means to activate and inactivate the communication over contactless antenna to the Secure Element.

6.1.1.2 Access to a Secure Element by mobile applications SHALL be limited to authorized mobile applications only.

6.1.1.3 An authorized mobile application SHALL be able to interact with a Secure Element.

That is, an authorized mobile application must be able to address communication to any application on a Secure Element. This requirement does not imply that the communication will be successful as multiple levels of authorization may be required.

6.1.1.4 An authorized mobile application SHALL be able to manage the accessibility state of the Secure Element (active or inactive) to the antenna interface.

— If a Secure Element is in the inactive state, communication received over the antenna interface SHALL NOT be routed to the Secure Element. An authorized mobile application SHALL still be able to route communication to the inactive Secure Element.

— If a Secure Element is in the active state, communication received over the antenna interface SHALL be routed to the Secure Element. .

6.2 Origin of Secure Element Communication

A Secure Element has a logical architecture that supports two communication interfaces:

- A device or contact interface which enables commands and responses to be exchanged between the Secure Element and the Handset/ authorized mobile applications.
- An antenna interface which enables the exchange of commands and responses between the Secure Element and a contactless terminal via the Contactless Module of the Handset.

Requirements – Origin of Communication

6.2.1.1 Communication routed to a Secure Element by the Handset, or by the Contactless Module of the Handset, SHALL contain a means to indicate its origin.
From the point of view of the Secure Element:

— Communication that has originated over the antenna interface SHALL be identifiable as being received using the contactless protocol (e.g. in a Java Card environment as T=CL).
— Communication that has originated from the Handset, or an authorized mobile application, SHALL be identifiable as being received using a contact protocol (e.g. in a Java Card environment as T=0 or T=1).

6.3 Multiple Secure Elements

In the case where a Handset supports multiple Secure Elements then in addition to the requirements in section 6.1, and where applicable superseding the requirements in section 6.1, regardless of whether the Handset is Host-based Card Emulation enabled or not, the following requirements also apply.

Requirements –Secure Element(s)

6.3.1.1 The Handset SHALL provide a means to display the list of all available Secure Elements.

6.3.1.2 The Handset SHALL provide a means to activate and inactivate the communication over the contactless antenna to each Secure Element.

6.3.1.3 The Handset SHALL provide a means to route the communication received over the antenna interface to each specific Secure Element.

6.3.1.4 An authorized mobile application SHALL be able to identify all Secure Elements present on the Handset and each Secure Element's current antenna interface accessibility state (active or inactive).

6.3.1.5 An authorized mobile application SHALL be able to determine whether it is possible for more than one Secure Element to be in the active accessibility state simultaneously.

6.3.1.6 An authorized mobile application SHALL be able to interact with all Secure Elements.

That is, an authorized mobile application must be able to address communication to any application on any of the multiple Secure Elements. This requirement does not imply that the communication will be successful as multiple levels of authorization may be required.

6.3.1.7 Where applicable and if more than one Secure Element has been set to the active state, routing of communication received over the antenna interface SHALL be based firstly on the contactless routing table (see section 7.3) and secondly on the priority order of the Secure Element as determined by the Handset/Contactless Module

	manufacturer.

7 Contactless Module

Requirements – Supported Technologies

7.1.1.1 The Contactless Module SHALL support at least one of the following technologies complying with [CCPS]:

- ISO/IEC 14443 Type A
- ISO/IEC 14443 Type B

7.2 Antenna Interface Events

Events are actions or occurrences that become evident to entities that have requested to be alerted when they occur. For example, a currently running mobile application can register to be alerted whenever the Handset senses that it has entered the proximity of a contactless terminal that is attempting to communicate over its antenna interface (that is, the entry of the Handset into the RF field is the event).

Requirements – Contactless events

7.2.1.1 An event SHALL be generated to indicate the entry of the Handset into an RF field.

7.2.1.2 An event SHALL be generated to indicate the removal of the Handset from an RF field.

7.2.1.3 An event SHALL be generated to indicate the receipt of a SELECT command containing a recognized AID over the antenna interface. The event SHALL be generated immediately on receipt of the SELECT command and while the Handset is still in the proximity of the contactless field.

7.3 Command Routing Capability

For Handsets that support multiple Secure Elements and it is possible for more than one Secure Element to be in the active accessibility state, command routing must be possible. In a contactless mobile payment transaction, when a command sequence (starting with an initial SELECT command indicating a specific payment application) is received, the Handset shall be able to route the SELECT and subsequent APDU commands to the Secure Element wherein that payment application is hosted. This is simple in terms of a single Secure Element architecture as all commands are by default routed to that single Secure Element. The added complexity is revealed in a multiple Secure Element environment where multiple applications, possibly even with identical Application Identifiers (AID), could exist in multiple Secure Elements in the

Handset[1]. It is thought that the most appropriate method for APDU command routing would be facilitated through a routing table built into the Contactless Module. It is up to the implementation as to how the routing table would be constructed but some basic requirements shall be fulfilled.

The following example provides a scenario in which such a routing table would be needed as well as an example of what information the routing table would need to maintain.
Imagine a Handset with a Contactless Module connected to 2 Secure Elements (e.g. an embedded secure element and a UICC) each of which hosts a contactless payment application. Assuming the AIDs of the 2 payment applications were different (*x* and *y*), the routing table would need to keep track of each secure elements and the AIDs of the applications thereon. For example:

- UICC contains *x*
- Embedded contains *y*

Whenever a SELECT command is received over the antenna interface, the Contactless Module would need to determine if the AID being selected was *x* or *y* and route the communication to the respective Secure Element.
Now imagine that 2 new contactless payment applications were provisioned to the Handset, one to the UICC and the other to the embedded Secure Element and both had identical AIDs (*z*). At this point the routing table would also need to be updated as such:

- UICC contains *x* and *z*
- Embedded contains *y* and *z*

Now whenever a SELECT command is received over the antenna interface, and the AID being selected is *z*, the Contactless Module has a choice as to where to route the communication and would probably route it to a preferred secure element which highlights a need for an additional parameter in the routing table configurable by an authorized mobile application. That is:

- UICC contains *x* (on) and *z* (off)
- Embedded contains *y* (on) and *z* (on)

Requirements – Contactless Routing	
7.3.1.1	Sufficient information SHALL be maintained in order to be able to route communications received over the antenna interface to the Secure Element hosting the application as indicated by the AID of the most recently received SELECT command. *Communication received over the antenna interface and not preceded by a SELECT command are out of scope of these requirements.*

[1] Where the possibility may exist for an AID in a SELECT command (partial select) to target more than one application at the Secure Element level, the functionality that enables the correct application to be selected is defined by the Secure Element's environment (e.g. GlobalPlatform) and is outside the scope of this document.

7.3.1.2 An authorized mobile application SHALL be able to configure the routing information within the Contactless Module indicating which Secure Element takes precedence if there is a conflict.

That is, if the AID contained in the SELECT command is a match for contactless applications on multiple Secure Elements.

7.4 Contactless Proximity Antenna

The antenna utilized by the Handset is a key component in ensuring that Contactless Mobile Payment is interoperable with the contactless payment infrastructure. The Handset is required to pass the EMVCo Level 1 testing as defined by [CCPS].

7.5 Contactless Module Configuration

An authorized mobile application shall be able to effectively manage the contactless capabilities of the Handset depending on its own specific functional requirements. For example:

— Define the contactless communication routing for a set of contactless applications,

— Manage the contactless technologies for efficient use by those applications, and,

— Disable contactless communication when it is itself communicating with a secure element using contact communication.

To do so, an authorized mobile application needs to be:

- Aware of the specific capabilities of the Contactless Module
- Able to configure the Contactless Module appropriately.

Requirements – Configuration

7.5.1.1 An authorized mobile application SHOULD be able to determine the following capabilities of the Contactless Module:

— Supported contactless technologies

— Contactless routing capabilities and setting

— Details of the supported Secure Elements

7.5.1.2 An authorized mobile application SHALL be able to query the current antenna interface state. That is:

— In an RF field

— Not in an RF field

— Currently routing communication between the antenna interface and a Secure Element

7.5.1.3 An authorized mobile application SHALL be able to instruct the Contactless Module to switch the antenna interface on and off.

That is, a Handset whose antenna interface has been switched off will not respond to polls from contactless terminals.

- If the authorized mobile application provides a time period indicating how long the interface should be on/off, the Contactless Module SHALL revert to its previous state on expiration of the time period.
  That is, if the authorized mobile application has not reset the Contactless Module to its previous state within that time period.

7.5.1.4 An authorized mobile application SHOULD be able to configure the Contactless Module for a particular contactless technology if it supports more than one.

For example, if a Handset is capable of listening to polls for technologies other than those defined in [CCPS], it should be possible for an authorized mobile application managing EMV based payment applications to configure the Handset to only listen for one or more specific technologies. This could potentially improve the performance of the contactless payment transaction.

8 APPENDIX: Implementation Specific Requirements

The requirements in this Appendix are extensions to the requirements stated in the body of the document and apply to specific known technical implementations for the technology platform. That is:

- NFC Controller
- Secure Element Access Control
- Trusted Execution Environment

The requirements are stated for each of the technologies supported:

8.1 NFC Controller

These requirements apply to a controller on an NFC Forum Device supporting Card Emulation mode.

Requirements – Contactless Module is an NFC Controller	
8.1.1.1	An authorized mobile application SHALL be able to configure the listen cycles of the NFC Controller in Card Emulation mode.
8.1.1.2	The NFC Controller SHALL NOT respond to polls for multiple technologies in a single listen cycle.
8.1.1.3	If the NFC Controller is implemented to interact with a UICC as a Secure Element, it SHALL interface with the UICC using the Single Wire Protocol and Host Controller Interface as defined in: — [SWP] — [HCI]

8.2 Secure Element Access Control

This requirement applies to Handsets supporting single or multiple Secure Elements.

Requirement – Secure Element Access Control	
8.2.1.1	If SEAC is supported it SHALL be implemented as defined in: [SEAC]

8.3 Trusted Execution Environment

The Trusted Execution Environment (TEE) provides a safe area of the device to protect assets and execute trusted code. TEE resides alongside the Execution Environment (REE) and complements traditional security environments such as Secure Element.

This requirement applies to Handsets supporting the GlobalPlatform Trusted Execution Environment technology.

Requirement – Trusted Execution Environment	
8.3.1.1	If TEE is supported it SHALL be implemented as defined in: [TEE]

8.4 NFC Mobile Security Considerations

EMVCo recognizes that NFC enabled mobile handsets introduces new security considerations and published the white paper providing with a set of EMVCo security best practices.

Requirement – Mobile Security Best Practices	
8.4.1.1	The mobile handset design SHOULD follow the recommendations as provided in: [MSC]

8.5 Open Mobile API

simalliance defined the Open Mobile API specification enabling mobile applications to have access to different Secure Elements such as SIMs or embedded SEs.

Requirement – Open Mobile API	
8.5.1.1	The mobile handset SHALL support the API as provided in: [OMA]

<<< END OF DOCUMENT >>>