EMV®
Contactless Mobile Payment

Payment Card Management

White Paper

Version 1.0
May 2017

Legal Notice

This document summarizes EMVCo's present plans for evaluation services and related policies and is subject to change by EMVCo at any time. This document does not create any binding obligations upon EMVCo or any third party regarding the subject matter of this document, which obligations will exist, if at all, only to the extent set forth in separate written agreements executed by EMVCo or such third parties. In the absence of such a written agreement, no product provider, test laboratory or any other third party should rely on this document, and EMVCo shall not be liable for any such reliance.

No product provider, test laboratory or other third party may refer to a product, service or facility as EMVCo approved, in form or in substance, nor otherwise state or imply that EMVCo (or any agent of EMVCo) has in whole or part approved a product provider, test laboratory or other third party or its products, services, or facilities, except to the extent and subject to the terms, conditions and restrictions expressly set forth in a written agreement with EMVCo, or in an approval letter, compliance certificate or similar document issued by EMVCo. All other references to EMVCo approval are strictly prohibited by EMVCo.

Under no circumstances should EMVCo approvals, when granted, be construed to imply any endorsement or warranty regarding the security, functionality, quality, or performance of any particular product or service, and no party shall state or imply anything to the contrary. EMVCo specifically disclaims any and all representations and warranties with respect to products that have received evaluations or approvals, and to the evaluation process generally, including, without limitation, any implied warranties of merchantability, fitness for purpose or non-infringement. All warranties, rights and remedies relating to products and services that have undergone evaluation by EMVCo are provided solely by the parties selling or otherwise providing such products or services, and not by EMVCo, and EMVCo will have no liability whatsoever in connection with such products and services.

This document is provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in this document. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THIS DOCUMENT.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to this document. EMVCo undertakes no responsibility to determine whether any implementation of this document may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of this document should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, this document may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement this document is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with this document.

Contents

Figures

Tables

1 Scope

This document, *EMV Contactless Mobile Payment – Payment Card Management*, is a replacement for a portion of the 2010 EMVCo document Application Activation User Interface *[AAUI]*. Since the publication of the original AAUI document, the mobile device and mobile payment landscape has changed considerably. Some of the concepts and predictions in the original document have not materialized or have followed a different path. An obvious example is software based payment using Host Card Emulation (HCE), which was not considered as a viable solution when preparing the original document. The original AAUI document only considered payment applets on a secure element: HCE introduces a new environment for hosting Software Card applications. Therefore, EMVCo has decided to split the material in the original document into the following:

- A specification for a PPSE applet and application management on a secure element *[PPSE]*.
- This white paper, which explains EMVCo's current view on the management of contactless applications – whether HCE based or using Secure Elements – for contactless payments.

One of the primary forces behind EMVCo decisions related to contactless payment management on Consumer Devices is to provide flexibility in implementations to meet the needs of particular markets. In certain markets, it may be necessary to support the possibility of multiple contactless applications across multiple Execution Environments (Secure Elements and HCE based) being simultaneously active over the contactless interface. Other markets may not have the same requirement and may anticipate that only the contactless application(s) on a single Execution Environment will be active over the contactless interface at any one time. EMVCo does not dictate that an implementation in a market allow for flexibility; rather, this choice is based on business decisions, the complexity of managing multiple contactless applications, and the functionality available on the Consumer Devices, Wearables and Secure Element(s) hosting the contactless applications.

1.1 Audience

This document is intended for use by entities designing, developing, and implementing a Payment Card Manager (for example, a wallet application), entities developing contactless Payment Applications, entities responsible for the provisioning of those applications, and entities responsible for the presence of the PPSE functionality on the Consumer Device (for example, handset manufacturers, operating system providers, mobile network operators, mobile application developers, smart card application developers, etc.).

1.2 Organisation of Document

This document has the following main sections:

- Section 4, Architecture and Data Mapping

  This section describes the necessary components of a mobile device architecture and the data mapping within these components.

- Section 5, Payment Card Manager Purpose

  This section describes the main purpose of any Payment Card Manager (a Wallet) which is to allow the consumer to choose which of their Payment Cards they wish to use for a contactless payment.

- Section 6, Mobile Application Implementation

  This section provides direction for the implementers and designers of a Payment Card Manager.

2 References

The following documents contain provisions that are referenced in this specification. The latest version shall apply unless a publication date is explicitly stated.

2.1 EMV Documents

EMV documents are available on the EMVCo website:

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

Table 2-1: EMV Documents

Reference	Publication Name
[ENTRY]	Contactless Specifications for Payment Systems: Book B – Entry Point Specification
[PPSE]	PPSE and Application Management for Secure Element
[AAUI]	Application Activation User Interface – Overview, Usage Guidelines, and PPSE Requirements

2.2 External References

Table 2-2: External References

Reference	Publication Name
[ISO/IEC 14443]	Identification cards – Contactless integrated circuit(s) cards – Proximity cards
[NCI]	NFC Forum NFC Controller Interface
[GPCARD C]	Contactless Services – GlobalPlatform Card Specification – Amendment C

2.3 Abbreviations

The abbreviations listed in Table 2-3 are used in this specification.

Table 2-3: Abbreviations

Abbreviation	Description
AAUI	Application Activation User Interface
AID	Application Identifier
APDU	Application Protocol Data Unit
FCI	File Control Information
HCE	Host Card Emulation
NCI	NFC Controller Interface
PPSE	Proximity Payment System Environment
SIM	Subscriber Identity Module
TEE	Trusted Execution Environment
UICC	Universal Integrated Circuit Card

2.4 Definitions

The following terms are used in this specification:

Table 2-4: Definitions

Term	Definition
AAUI	Former terminology used in *[AAUI]*, referring to a Payment Card Manager.
Host Card Emulation	The implementation of software based payment where contactless communication in Card Emulation mode is routed to a mobile application on the Device Host.
PPSE	An application presenting the contactless applications available for conducting a transaction to a Merchant Terminal. The PPSE is the first application selected by a Merchant Terminal, and based on the information provided by the PPSE, the terminal uses the highest priority application it supports to process a contactless payment.
Software Card	The card credentials used for Software-based Mobile Payments and stored within the mobile application rather than in a Secure Element.

3 Changes

When the Application Activation User Interface document was originally developed, most Consumer Devices that were enabled to process contactless payment were feature phones that did not specifically cater for a seamless experience when making a payment. Many of these shortcomings have been highlighted in the various documents published over the years by EMVCo and others. While the industry has not necessarily followed the recommendations originally made by EMVCo, the payment experience has improved significantly based on the following:

- Card Emulation Mode – as defined by the NFC Forum – has become the standard for contactless mobile payment.
- The general improvements in Consumer Device processing power, incorporation of new biometric hardware (fingerprint sensors) and new means of user interaction (touchscreens).
- The support in most device platforms – and NFC Controllers therein – of the concepts defined in the NFC Forum's NCI Specifications *[NCI]*.
- The adoption of relevant GlobalPlatform specifications such as Card Specification Amendment C *[GPCARD C]*.

These improvements allow a consumer to easily switch between multiple mobile applications on a device and between the choices offered by mobile applications. This has resulted in implementations that allow payments to be processed in less time and with less consumer interaction.

In addition, the support of HCE on the Android platform in conjunction with the support of Tokenisation and software based payment by EMVCo and the Payment Systems has resulted in a reduction in required business arrangements (as opposed to Secure Elements) and in simplification of the provisioning process. This, along with the introduction of Apple Pay, has resulted in an increased adoption of mobile payment and provided an insight into where and how this space will progress.

Note that in the context of this document, the term HCE refers to the implementation of software based payment where contactless communication in Card Emulation mode is routed to a mobile application on the Device Host. This document does not differentiate between the multiple options for the actual management of software based card credentials, which may involve whitebox cryptography, code obfuscation, TEE, etc.

Another important learning has been that in all cases, payment choice is performed by a wallet-type mobile application, and as such EMVCo no longer considers the possibility of such management occurring on another component. For example, the ubiquitous use of SIM Toolkit or Smart Card Web Server on UICCs has not materialized.

Taking the above into account, the original AAUI document has been split into a technical specification detailing both the requirements of a PPSE and the application management for Secure Elements and this white paper which provides direction for a Payment Card Manager.

4 Architecture and Data Mapping

4.1 Architecture

Figure 4-1 depicts the architecture required to enable a Merchant Terminal to interact with the correct contactless applications based on the consumer's choice. The following components are specific to this document.

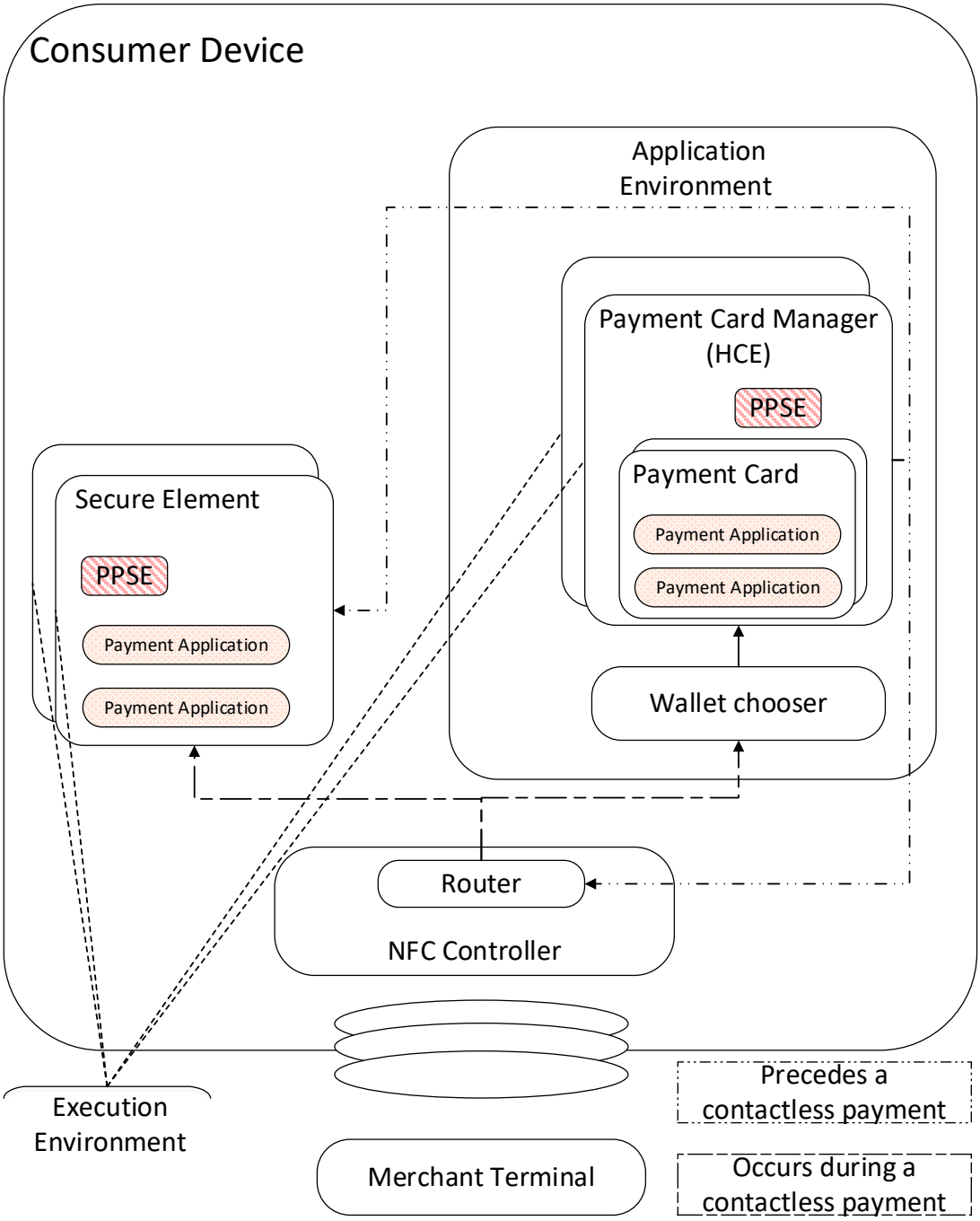
- Payment Card Manager – This component, the basis for this document, is a consumer visible mobile application (for example, a wallet app) resident within the Consumer Device's application environment and used by the consumer to manage which Payment Card(s) will be used for conducting contactless payments. More than one Payment Card Manager may be present on a Consumer Device.
- Payment Card – The consumer visible card(s) within a Payment Card Manager. This is typically the representation of a physical card product within a Payment Card Manager.
- Payment Application – An application selectable over the contactless interface. The Payment Application could be present on a Secure Element in the form of an applet or as a Software Card in the Payment Card Manager. There will be at least one Payment Application associated with a Payment Card, but depending on various factors a Payment Card may be associated with multiple Payment Applications. While out of scope of this white paper, some examples of this one-to-many relationship are:
  - A Payment Card providing options for processing credit or debit transactions each being facilitated by a separately selectable Payment Application.
  - A Payment Card providing options for processing domestic or international transactions each being facilitated by a separately selectable Payment Application.
- Proximity Payment System Environment (PPSE) – An application selectable over the contactless interface. The primary responsibility of the PPSE is communicating the active Payment Application(s) and the respective priorities of the Payment Applications by responding to a Merchant Terminal as specified in *[ENTRY].* The Payment Applications are chosen by the consumer to be used for payment based on the selection of one or more Payment Card(s) within a Payment Card Manager. In this architecture, the PPSE is depicted as an applet on a Secure Element *[PPSE]* or as a Software Card component of the Payment Card Manager.
- NFC Router – A component within the NFC Controller responsible for directing contactless communication to the correct Execution Environment on the Consumer Device.

- Wallet chooser – A platform may provide a feature to allow the consumer to set:
  - which Payment Card Manager(s) will interact with the consumer when a contactless payment transaction occurs
  - [for HCE] which Payment Card Manager(s) will respond to APDU commands received from a Merchant Terminal.

The exact mechanism used by the device platform to achieve the above is out of scope of this document, but could be:

- a requirement that a Payment Card Manager be launched and in the foreground,
- an operating system setting accessible to the user that sets one of many Payment Card Managers as the default, or
- based on a link between an AID received in a SELECT command and a specific Payment Card Manager.

Figure 4-1: Extended Architecture



4.2 Data Mapping

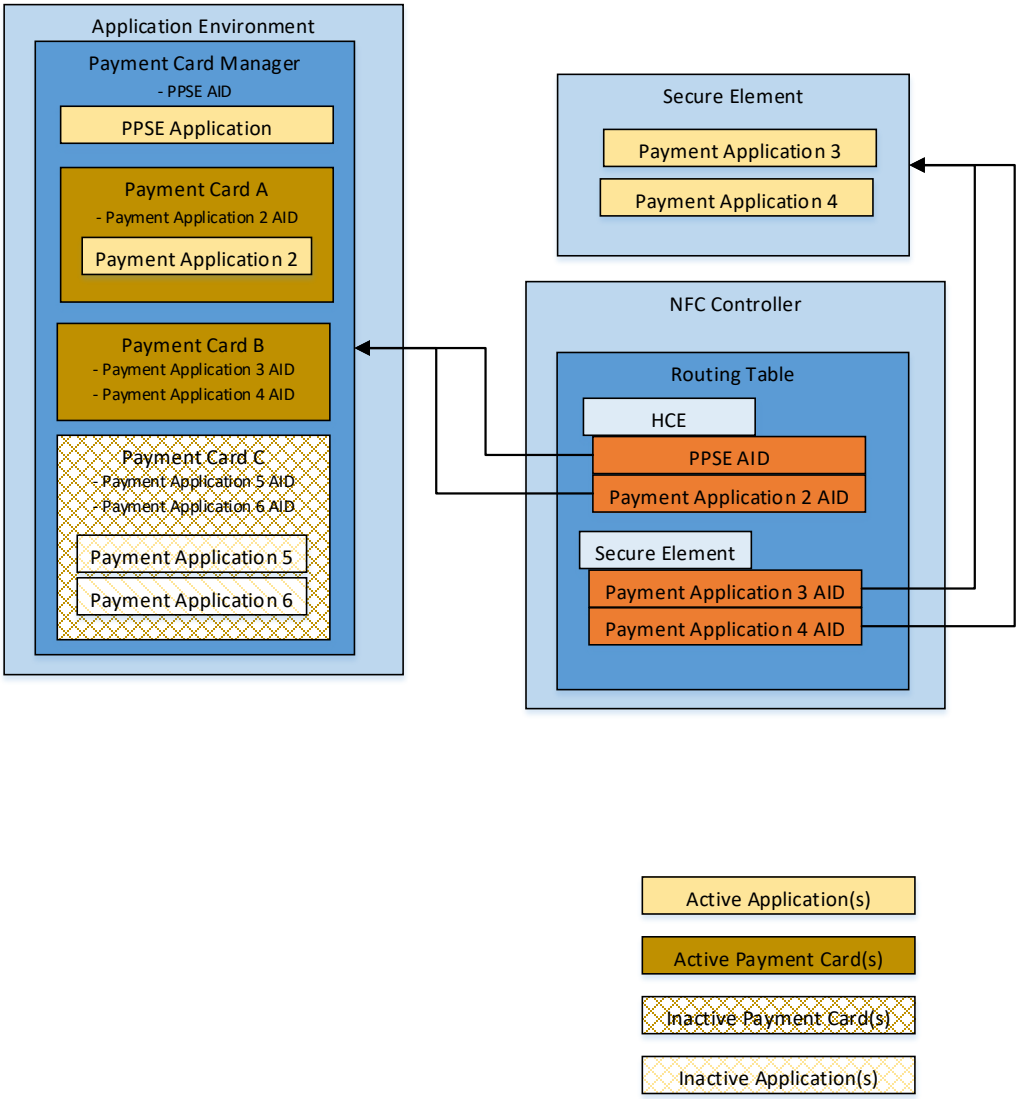
Figure 4-2 lists the types of information that should be accessible and possibly configurable by a Payment Card Manager and indicates how this information may be mapped within the various components of the Consumer Device. The figure depicts a Payment Card Manager with access to the NFC Controller, and possibly one Secure Element present on the Consumer Device. In addition, the figure shows how the NFC Controller will route communication to the relevant Execution Environment whenever EMV level 1 communication is occurring over the NFC interface and based on configuration by the Payment Card Manager.

The following describes the components and data thereon when viewing Figure 4-2 (see Chapters 5 and 6 for details):

- The NFC Controller needs to know the parameters of the communications protocol of the currently accessible applications in order to successfully interact with a contactless terminal. In the context of this document, it is assumed that the protocol matches that required by EMV Level 1.
- The routing table contains the information needed to route APDU commands received over the NFC interface to the correct Execution Environment. This could be as simple as routing all EMV Level 1 communication to the Execution Environment hosting the Payment Application(s). Alternatively, if the Payment Applications are split amongst Execution Environments, then for each application this includes:
  - The Execution Environment on which the Payment Application is located.

  The example used in Figure 4-2 is based on the consumer indicating that their preferred mechanism of payment is with Payment Card A, and as an alternative, Payment Card B can be used if Payment Card A is not supported by the Merchant Terminal. That is, Payment Card A and Payment Card B are currently accessible for payments while Payment Card C is not currently accessible for payment. The Router will route all PPSE Application and Payment Application 2 commands to the Payment Card Manager itself and all Payment Application 3 and Payment Application 4 commands to the Secure Element. Payment Application 5 and Payment Application 6 are not configured in the Router.
- The PPSE will keep a record of the FCI Template and mirror the information configured to the routing table. Again, for the example used in Figure 4-2, the FCI Template will list directory entries for Payment Application 2, Payment Application 3 and Payment Application 4. There will be no directory entries in the FCI Template for Payment Application 5 or Payment Application 6. The priority of each application in the FCI Template will reflect the choice of the consumer – that is, Payment Application 2 will have the highest priority followed by Payment Application 3 and then Payment Application 4.

Figure 4-2: Data Mapping Diagram



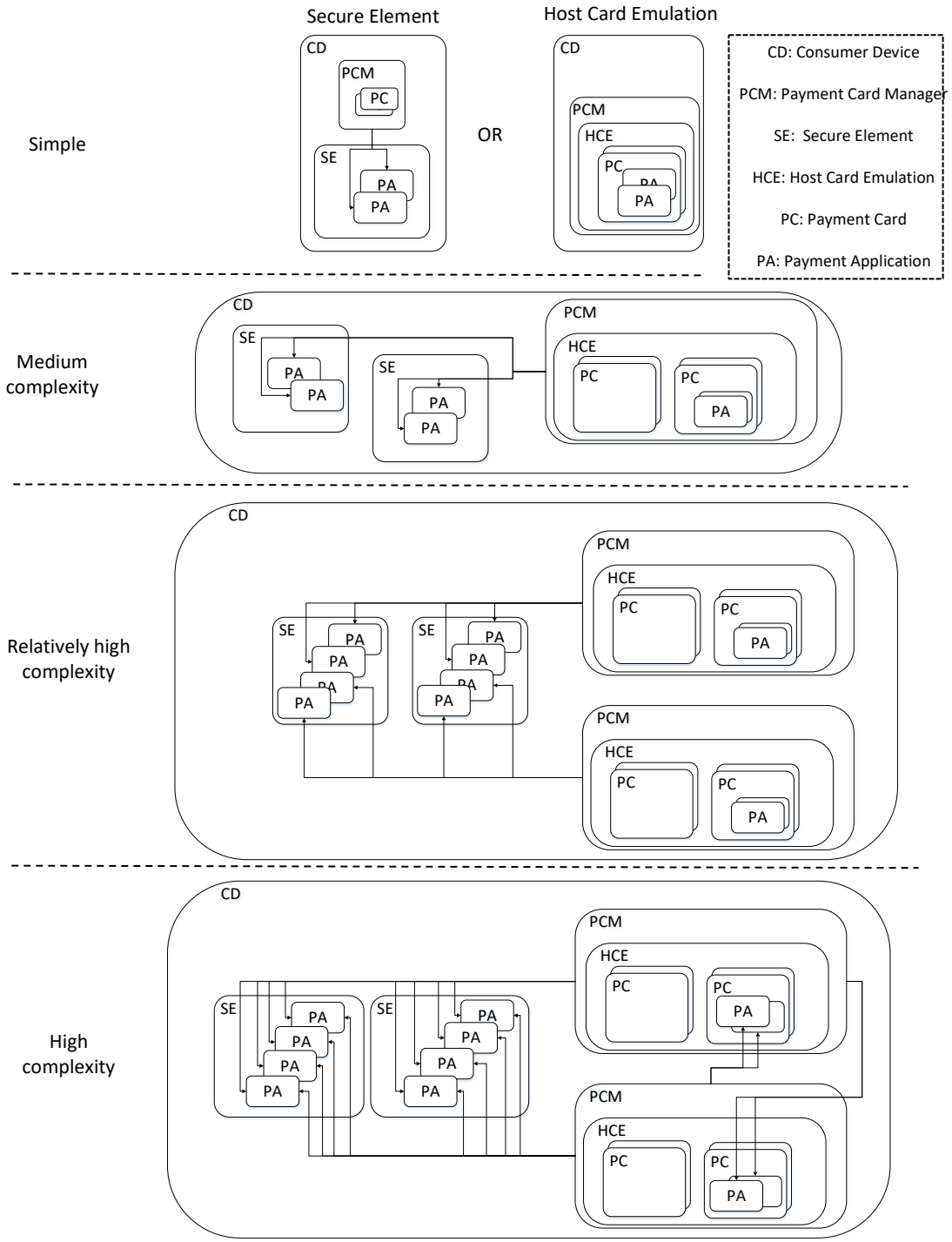
5 Payment Card Manager Purpose

The main purpose of any Payment Card Manager (a Wallet) is to allow the consumer to choose which of their Payment Cards listed in the Payment Card Manager they wish to use for a contactless payment. This choice must result in the associated contactless Payment Applications being accessible over the contactless interface to a Merchant Terminal.

While this management is typically very simple, it can be more complex. Some examples of this possible complexity are described below and depicted in Figure 5-1.

- Simple – A single Payment Card Manager managing one or more Payment Cards (exclusive to this Mobile Payment Application), each linked to one or more Payment Applications in a single Execution Environment (Secure Element or HCE).
- Medium complexity – A single Payment Card Manager managing multiple Payment Cards (exclusive to this Mobile Payment Application), each linked to one or more Payment Applications across multiple Execution Environments.
- Relatively high complexity – Multiple Payment Card Managers managing multiple Payment Cards (each exclusive to this Payment Card Manager) across multiple Execution Environments.
- Highly complex – Multiple Payment Card Managers managing multiple Payment Cards (not exclusive to any particular Payment Card Manager), each linked to one or more Payment Applications across multiple Execution Environments.

Figure 5-1: Complexity Examples



The complexity of each of the examples above is increased if it is deemed necessary for multiple Payment Applications to be simultaneously accessible to a Merchant Terminal.

From an EMVCo perspective, and based on input from stakeholders, the following scenarios are considered to be viable and are described further in this document. Note that this does not exclude other approaches.

- A single Payment Card Manager managing one or more Payment Cards (exclusive to this Payment Card Manager) in a single Execution Environment (HCE or Secure Element).
- A single Payment Card Manager managing multiple Payment Cards (each exclusive to this Payment Card Manager) across two Execution Environments (HCE and a Secure Element).

In both of the above cases, the consumer may have more than one Payment Card Manager installed on their device, but these mobile applications are wholly separate. A device platform that allows the presence of multiple Payment Card Managers will also have a mechanism for configuring which Payment Card Manager will interact with the user when the presentment of the Consumer Device to the Merchant Terminal occurs. This mechanism ensures that the settings described hereafter are controlled by the default or most recently used Payment Card Manager while the other Payment Card Managers, if any, and their respective Payment Applications, are inactive. These two viable scenarios also avoid any issues with the conflicts described in the previous AAUI document.

5.1 Single Execution Environment Use Case

In this example, a single mobile application (a Payment Card Manager) on the Consumer Device manages one or more Payment Cards, and by association one or more Payment Applications. The Payment Application(s) can be present in a Secure Element connected directly to the NFC Controller or present as a Software Card in, and directly managed by, the Payment Card Manager through HCE.

In most implementations using a single Execution Environment, all EMV Level 1 communication from a Merchant Terminal is directed to the single Execution Environment (a Secure Element or, in the case of HCE, a Payment Card Manager on the Device Host).

In the case that all communication is directed to the single Secure Element, it would be a PPSE application on that Secure Element that would be responding to a PPSE SELECT command received from the Merchant Terminal. It is the responsibility of the Payment Card Manager to ensure that the response to the PPSE SELECT command reflects the Payment Card choice of the consumer. This can be done using either External or Internal mode as specified in *[PPSE]*.

In the HCE case where the selection of the PPSE is directed to the Payment Card Manager, it is the responsibility of this Payment Card Manager to ensure that the response to the PPSE SELECT command reflects the consumer's Payment Card choice.

The Single Execution Environment use case is further broken down into the following three separate use cases.

5.1.1 Secure Element and External Mode

This use case assumes that:

- The consumer, through the Payment Card Manager, has chosen the specific Payment Card(s) available for payment at some point in the past or immediately preceding the presentment of the Consumer Device to the Merchant Terminal.
- All EMV Level 1 contactless communication received by the NFC Controller is routed to the single Secure Element.
- The Secure Element has been provisioned with a PPSE supporting External Mode specified in *[PPSE]*.
- The Payment Card Manager is capable of interacting with the PPSE in the Secure Element.
- The Payment Card Manager is also capable of interacting with the Payment Applications and/or the Contactless Registry Service application (as defined in *[GPCARD C]*) in the Secure Element.

The Payment Card Manager ensures that the Payment Application(s) associated with the Payment Card(s) will become known and accessible to a Merchant Terminal in anticipation of the consumer imminently presenting the Consumer Device to a Merchant Terminal. That is:

- The Payment Card Manager “activates” and, if necessary, prioritizes the associated Payment Application(s).
- The Payment Card Manager configures the PPSE to return the correct information to the Merchant Terminal. See section 3.3 in *[PPSE]*.

5.1.2 Secure Element and Internal Mode

This use case assumes that:

- The consumer, through the Payment Card Manager, has chosen the specific Payment Card(s) available for payment at some point in the past or immediately preceding the presentment of the Consumer Device to the Merchant Terminal.
- All EMV Level 1 contactless communication received by the NFC Controller is routed to the single Secure Element.
- The Secure Element supports *[GPCARD C]* and has been provisioned with a PPSE supporting the Internal Mode specified in *[PPSE]*.
- The Payment Card Manager is capable of interacting with the Payment Applications and/or the Contactless Registry Service (as defined in *[GPCARD C]*) in the Secure Element.

The Mobile Payment Application ensures that the Payment Application(s) associated with the Payment Card(s) will become known and accessible to a Merchant Terminal in anticipation of the consumer imminently presenting the Consumer Device to a Merchant Terminal. That is:

- The Payment Card Manager “activates” and, if necessary, prioritizes the associated Payment Application(s). Based on this activation, the FCI Template within the PPSE is built as per section 3.6 in *[PPSE]*.

5.1.3 Host Card Emulation Only

This use case assumes that:

- The consumer, through the current, or default, Payment Card Manager, has chosen the specific Payment Card(s) available for payment at some point in the past or immediately preceding the presentment of the Consumer Device to the Merchant Terminal.
- All EMV Level 1 contactless communication received by the NFC Controller is routed to the Device Host.

The Payment Card Manager builds the FCI Template based on the consumer’s choice. This FCI Template is returned to the Merchant Terminal as the response to a received PPSE SELECT command. For details on how the FCI Template is structured, refer to *[ENTRY]* section 3.3.1.

5.2 Multiple Execution Environments Use Case

This example is an extension of the single Execution Environment examples. In this case, a single mobile application (a Payment Card Manager) on the Consumer Device manages one or more Payment Cards and by association one or more Payment Applications possibly distributed across two Execution Environments. The Payment Application(s) can be present in, and directly managed by, the Payment Card Manager through HCE and can be present in a Secure Element connected directly to the NFC Controller.

In this use case, the selection of the PPSE is directed to the Payment Card Manager or the Secure Element and it is the responsibility of this Payment Card Manager to ensure that the response to the PPSE SELECT command reflects the consumer’s Payment Application(s) choice.

5.2.1 Host Card Emulation and Secure Element

This use case assumes that:

- The consumer, through the Payment Card Manager, has chosen the specific Payment Card(s) available for payment at some point in the past or immediately preceding the presentment of the Consumer Device to the Merchant Terminal.
- EMV Level 1 contactless communication received by the NFC Controller is routed either to the Device Host or to the single Secure Element based on the manner in which the NFC Controller Routing Table has been configured by the Payment Card Manager.
- The Payment Card Manager is capable of interacting with the Payment Applications and/or the Contactless Registry Service (as defined in *[GPCARD C]*) in the Secure Element.

The Payment Card Manager ensures that the PPSE and the Payment Application(s) will become known and accessible to a Merchant Terminal in anticipation of the consumer imminently presenting the Consumer Device to a Merchant Terminal. That is:

- If necessary, the Payment Card Manager "activates" the associated Payment Application(s) on the Secure Element.
- The Payment Card Manager builds the FCI Template based on the consumer's choice. If the PPSE is hosted on a Secure Element, once built, this FCI Template is transmitted to the PPSE, else, if the PPSE is hosted in the Payment Card Manager, it is returned to the Merchant Terminal as the response to a received PPSE SELECT command. For details on how the FCI Template is structured, refer to *[ENTRY]* section 3.3.1.
- Configure the Router based on the consumer's choice. See section 6.7.

6 Mobile Application Implementation

The following chapter provides direction to the implementers and designers of a Payment Card Manager regarding the functionality that is needed in the application, or may be available to the application, to enable specific features.

6.1 Removable Secure Elements

In the case that a Payment Card Manager manages Payment Cards with associated Payment Applications hosted on a removable Secure Element, there are specific conditions that must be met in the case that the Secure Element is removed and/or replaced.

There should be a platform feature that is able to notify, and trigger the launch of, the relevant Payment Card Manager whenever a removal or insertion of the Secure Element occurs.

The first task of the Payment Card Manager, during its launch cycle, should be to check that the specific Secure Element is still present on the device and that the Payment Applications it manages are still present and manageable. Depending on the consumer's choices, it may be necessary to inform the consumer that a specific Payment Card is no longer available for contactless payment.

6.2 Consumer Management of Payment Cards

While a Payment Card Manager may have additional functionality that is beyond the scope of this document, it is likely that the application will have functionality that:

- Lists the consumer facing Payment Card(s).
- Allows the consumer to choose one or possibly more Payment Card(s) that would enable the associated Payment Application(s) to interact with a Merchant Terminal.
- If allowing the consumer to choose more than one Payment Card to be used for payment, then allows the consumer to prioritize the order in which each would be used. This will enable a Merchant Terminal to interact with Payment Applications according to the consumer's own preferences.

6.2.1 Representation of Payment Cards

The Payment Card Manager should present Payment Card information in an intuitive manner that is clearly recognizable and understandable to a typical consumer.

There are many technical or detailed aspects that are of no interest to the majority of consumers (ISO 14443, Types A and B, PPSE, AIDs, HCE, Secure Element types, etc.). One of the main focuses of this document is to make sure that the consumer does not need to have any knowledge of these. The Payment Card Manager should hide these details from the consumer while still providing the consumer with enough functionality to effectively manage all aspects of their Payment Card(s).

The Payment Card Manager should present only consumer-relevant Payment Card information to the consumer. For example:

- The PPSE is a contactless application and is integral to the correct operation of Payment Applications on a Consumer Device, but there is no need for it to be visible to the consumer or even for the consumer to be aware of its existence.
- A single physical card product being added by the consumer to the Payment Card Manager may result in multiple Payment Applications being provisioned to the Consumer Device and possibly multiple Payment Cards being added to the Payment Card Manager. For a Payment Card linked to several Payment Applications, each with its own unique AID, what is relevant and should be visible to the consumer should represent an identifiable card product rather than the individual Payment Applications that make up the product. The Payment Card Manager should present and allow the consumer to manage the Payment Card while the Payment Card Manager manages the underlying Payment Applications affected.

6.2.2 Prioritizing Multiple Payment Cards

If the Payment Card Manager allows the consumer to choose more than one Payment Cards to interact with a Merchant Terminal, this should be sensible and only allowed if one of the chosen Payment Cards is actually capable of being chosen to conduct a transaction. For example, it may not make sense for two Payment Cards from the same Payment System to be chosen simultaneously. This is especially true when the two Payment Cards are linked to Payment Applications that have the same AID. The consumer should also have a clear indication of which Payment Card will be used if it is supported by the Merchant Terminal. It is not necessary for priorities to be presented to the consumer, but if the user interface allows the consumer to set or order the priority of their Payment Cards, the consumer should be able to discern the relative priority of the Payment Card within the card list.

6.2.3 Payment Card Management

As described in section 6.1, it is at the discretion of the Payment Card Manager owner whether the consumer can only use one Payment Card at a time or whether it is possible to enable more than one Payment Card at a time. The latter provides more leeway for the Merchant Terminal to process a payment if higher prioritized Payment Applications are not supported by the Merchant Terminal. Note that even if the consumer sets only one Payment Card, this card may still present multiple Payment Application options to the Merchant Terminal. If the consumer can indicate that more than one Payment Card could be used for payment, these should be ordered and this same Payment Application order reflected to the Merchant Terminal using priorities in the PPSE FCI Template. Note again that it does not make sense to enable multiple Payment Applications with the same AID as only the very first in the list would ever be used for payment. This limitation should be enforced by the Payment Card Manager.

Managing which Payment Cards could possibly be used for contactless payment is a consumer-controlled function that is based on the current state of the Payment Cards present on the Consumer Device. The Payment Card Manager presents the current view of the Payment Cards it manages to the consumer and allows the consumer to manipulate the settings or characteristics of those cards.

The following overview is from the point of view of the consumer making changes to their Payment Cards and describes how these changes are propagated across the Consumer Device and can change the contactless characteristics of one or more of their contactless Payment Applications. The following overview describes the process used to ensure that the consumer's choices are respected when a contactless payment transaction occurs.

- A consumer wishing to view or change which Payment Cards are used for contactless transactions launches the Payment Card Manager.

  Alternatively, the Payment Card Manager could be launched based on an action performed by the consumer – for example, the device enters the proximity of a Merchant Terminal. In this case, the choice to make changes could occur prior to the current payment transaction occurring or following a payment transaction.

- The Payment Card Manager displays all the Payment Cards it manages to the consumer.
- The Payment Card Manager allows the consumer to make changes.
- For each change the consumer makes, the Payment Card Manager:
  - Updates the contactless characteristics (prioritization and accessibility state) of the affected Payment Application(s). See section 6.3.
  - If operating in External Mode or for an HCE implementation of the PPSE, updates the PPSE FCI to reflect any changes. See sections 6.4 and 6.5 respectively.
  - Updates any necessary contactless routing to reflect the changes. See section 6.7.

6.3 Payment Application Specific Information

In general, the following information should be available to the Payment Card Manager at any point during or immediately following the provisioning of a new Payment Card:

- AID(s) – The AID(s) of the Payment Application(s) associated with the Payment Card.
- APDU Commands – For Payment Applications hosted on a Secure Element, the manner in which to activate, deactivate and potentially prioritize the Payment Applications' accessibility over the contactless interface. This is typically through a command issued directly to the Payment Application or the Contactless Registry Service as defined in *[GPCARD C]*.
- Directory Entries – When operating in External Mode or for an HCE implementation of the PPSE, the data that must be populated to the PPSE when the contactless Payment Applications linked to the Payment Card are accessible over the antenna interface; that is, the Directory Entry or Directory Entries necessary to build the FCI Template.

6.4 Updating the PPSE

The FCI Template returned to the Merchant Terminal on receipt of the PPSE SELECT command is used by the Merchant Terminal to determine which Payment Application will be used to conduct the current payment transaction.

6.4.1 Secure Element in Internal or External Mode

If using the PPSE on a Secure Element in Internal or External Mode to manage the FCI Template, refer to *[PPSE]*.

As per *[PPSE]*, Internal Mode can only be used when all the Payment Applications are hosted in the same Secure Element as the PPSE. Conversely, Internal Mode cannot be used if a Payment Card Manager is managing Payment Applications across multiple Execution Environments. In this case, the PPSE must be configured to operate in External Mode or the PPSE must be hosted in the Payment Card Manager itself through HCE.

Note that, as with any HCE based application, an HCE based PPSE application will not be selectable by a contactless reader when the Mobile Device is not powered. Thus, if the Payment Card Manager manages Secure Element based Payment Applications that must remain accessible to the Merchant Terminal when the Mobile Device is not powered, the Payment Card Manager must manage a Secure Element based PPSE configured for External Mode. Additionally, for this scenario, there would need to be special processing related to the routing of APDU commands specifically for when the Mobile Device is not powered.

The Payment Card Manager may manage multiple instances of the PPSE application, as long as only one PPSE instance is accessible to the Merchant Terminal at any time.

6.4.2 Host Card Emulation PPSE

When the PPSE functionality is present in the Payment Card Manager [using HCE], it is the responsibility of each Payment Card Manager to build the correct FCI Template. For details on how the FCI Template is structured, refer to *[ENTRY]* section 3.3.1.

Each Payment Card Manager will build the FCI Proprietary Template that reflects the consumer's choices in anticipation of this Payment Card Manager receiving a PPSE SELECT command.

The FCI Proprietary Template is built using the directory entries specified during the Payment Card provisioning process for all the Payment Applications that are intended to be accessible over the contactless interface whenever that Payment Card is chosen to be used for payment.

For each set of applicable Payment Applications, the Payment Card Manager performs the following basic functions:

- Concatenating the directory entries in priority order to build a valid FCI Proprietary Template.
- Inserting the Priority Indicator within each directory entry based on the priority order indicated by the consumer.

In addition, if the resulting FCI Proprietary Template contains a directory entry, or entries, that have no possibility of being accessed over the antenna interface, the Payment Card Manager removes the directory entries for those contactless Payment Applications that would not be accessed. Removing the lower priority directory entries reduces the size of the FCI Proprietary Template and improves the overall transaction execution time.

6.5 Multiple Payment Card Managers and Secure Elements

The presence of multiple Payment Card Managers, each of which interact with the Secure Element, necessitates specific Mobile Device platform prerequisites and additional functionality in the Payment Card Managers themselves. These prerequisites and functionality are key to ensuring synchronization between the consumer's payment choices and the actual state of the Mobile Device when a contactless payment transaction is occurring. Note that this section is specific to Secure Elements, multiple Payment Card Managers and the concept of a default Payment Card Manager. As evidenced by the rest of this document, there are numerous cases where this section would not apply, e.g. when all Payment Applications are HCE based, there is a single Payment Card Manager, there is no notion of a default Payment Card Manager, etc.

From a consumer perspective, there may be an expectation that a specific Payment Card (or specific Payment Cards) should be available for a contactless payment transaction when the consumer has not previously launched a Payment Card Manager. The realization of this expectation is typically handled by a default Payment Card Manager. However, in the case of multiple Payment Card Managers, when a Payment Card Manager, other than the default, is launched, there are steps needed to override the default Payment Card(s). If this new Payment Card Manager is not itself becoming the default, there are steps needed to ensure the reinstatement of the default Payment Card(s).

6.5.1 Device Prerequisites

Only a single Payment Card Manager is active at any one time. The active Payment Card Manager is either the current running mobile application with which the consumer is interacting or the default Payment Card Manager.

To successfully manage default Payment Card(s) the following prerequisites are expected of a Mobile Device platform:

- A Payment Card Manager must be notified when it is becoming active.
- A Payment Card Manager must be notified when it will no longer be active.

While these prerequisites are obvious for the case in which the consumer is launching or closing a Payment Card Manager, they actually apply to the default Payment Card Manager as seen below.

6.5.2 Payment Card Managers

When a Payment Card Manager is notified that it is becoming active, it performs the following operations:

- If the PPSE used by the Payment Card Manager is hosted on the Secure Element (as opposed to within the Payment Card Manager itself through HCE), activate, choose and configure (if applicable) the operating mode of the PPSE (External Mode, Internal Mode or Internal Mode with Mutual Exclusivity Rule). See section 3.5 of *[PPSE]*.
- For the Payment Application(s) it manages, and that are hosted within the Secure Element, activate and, if applicable, prioritize the Payment Applications according to the consumer's choice of Payment Card(s). See *[GPCARD C]* or Annex B of *[PPSE]*.
- If the PPSE is configured to operate in External Mode, set the FCI Proprietary Template (Device Switched On no override) according to the consumer's choice of Payment Card(s). See section 3.3 of *[PPSE]*.
- If applicable, it is also possible to set the FCI Proprietary Template (Device not Switched On) according to the consumer’s choice of Payment Card(s). See section 3.3 of *[PPSE]* and section 6.8 of this document.
- Conditionally, depending on the Mobile Device platform, configure the AID of the PPSE and the AIDs of the newly active Payment Applications in the router of the NFC Controller. See section 6.7.

When a Payment Card Manager is notified that it will no longer be active, it performs the following operation:

- Deactivate the Payment Application(s) it manages and that are hosted within the Secure Element. See *[GPCARD C]* or Annex B of *[PPSE]*.

6.6 Host Card Emulation Application Selection

In addition to building the FCI Template for the PPSE processing, in the HCE use case, the current or default Payment Card Manager is also responsible for correctly responding to SELECT Commands received from a Merchant Terminal. While most Merchant Terminals will respect the PPSE and only select the Payment Applications present in FCI Template, it is possible that some older terminals may not. While the underlying platform may reject specific unexpected SELECT commands based on its own mechanism, it is still the responsibility of the Payment Card Manager to process unanticipated SELECT commands. That is, the Payment Card Manager should:

- Return the correct Status Word ('6A82') when receiving a SELECT Command for a contactless application that is not recognized or has not been chosen by the consumer as suitable for payment.
- Anticipate partial selection. The Payment Card Manager should make the best attempt to respond appropriately to partial selection commands while still respecting the consumer's Payment Card choice.

6.7 Routing of APDU Commands

Depending on the capabilities of the device and the number of supported Execution Environments, it may be necessary that the NFC Controller's Listen Mode Routing Table (Router) be configured to accurately reflect the consumer's Payment Card choice.

Additionally, if there are multiple Execution Environments on the device [for HCE] there also may be a need to configure elements of the device platform to direct APDU commands received from the NFC Controller to the correct Execution Environment. As various device platforms handle this configuration in a platform specific manner, the description of this configuration is out of scope of this document.

6.7.1 Single Execution Environment on Device

If a Consumer Device supports only a single Execution Environment, there is no need to configure the Router as all EMV Level 1 communication received over the NFC interface is routed to that single Execution Environment. As per the use cases in Chapter 5 this routing would be either to the Secure Element or to the Device Host (for HCE).

6.7.2 Multiple Execution Environments

On devices that support multiple Execution Environments, the Router is a required feature of the device's NFC Controller that will be able to route EMV Level 1 communication to the correct Execution Environment based on the consumer's Payment Card choice.

6.7.2.1 Payment Application(s) on Single Execution Environment

If the consumer's Payment Card choice is linked to contactless applications that are all hosted on a single Execution Environment, the routing could be a simple instruction to the NFC Controller to direct all EMV Level 1 communication to that single Execution Environment.

6.7.2.2 Payment Cards across Multiple Execution Environments

If the consumer's Payment Card choice is linked to contactless applications that are hosted on multiple Execution Environments, routing is slightly more complicated. An NFC Controller will compare the AID received in the SELECT commands to the AID information in the Routing Table in order to direct communication to the correct Execution Environment. The Payment Card Manager must therefore ensure that the Router is configured with the necessary contactless application AIDs, each pointing to the specific Execution Environment hosting that contactless application.

6.7.2.3 Special Consideration

There is a possible scenario to be considered when configuring the Router.

The exact manner in which the Router is initially configured and kept updated is out of scope of this document. However, there could be a scenario where the Payment Card Manager may have to perform specific manipulation of the Router based on the consumer's Payment Card choice and the accessible contactless application(s). In this scenario, two contactless applications with the same AID may exist in multiple Execution Environments. If the consumer's Payment Card choice is intended to result in a specific instance of a contactless application being accessible over the antenna interface, the Payment Card Manager must ensure that the chosen contactless application, pointing only to the correct Execution Environment, is present in the Router.

6.8 Mobile Device Not Switched On

In specific Mobile Device and Execution Environment configurations, it may be possible for contactless transactions to occur when the Mobile Device is not Switched On. The main use case for this is in the event that the device's battery is depleted to the point that the device platform has powered off the device.

This behaviour is typically enabled on Mobile Device configurations incorporating a Secure Element (HCE most likely requires that the Mobile Device be switched on for contactless transactions to occur). As can be seen from *[PPSE]*, this can be enabled using Internal Mode (which is out of scope of this white paper) or External Mode. A Payment Card Manager using a PPSE on a Secure Element in External Mode can optionally allow consumers to choose which eligible Payment Card(s) will be available for contactless payments when their device is not switched on. The following are a few examples:

- The affected Payment Applications can be configured to process, or are capable of processing, a contactless payment transaction without requiring any interaction from the consumer on the Mobile Device.
- At least one Payment Application is hosted in the Secure Element.

It is also up to the Payment Card Manager to determine how and when this choice of eligible Payment Card(s) would be made. For example:

- The Payment Card Manager should be the default.
- Have a specific setting and explanation of the choice being made during Payment Card selection.
- Be aware of the device's battery capacity, and based on a low battery notification, query the consumer as to whether they want to select a specific eligible Payment Card to be used until such time that the device's battery capacity is no longer low.

Payment Card Managers enabling this setting should inform the consumer that making this choice may change the manner in which contactless payments will occur. For example, as the device will not be switched on, it is not possible for the Payment Card Manager to prompt the consumer for any input prior to a payment occurring or for the Payment Card Manager to provide any indication of progress during, or following, the payment.