

**EMV®**

# **Contactless Mobile Payment**

---

## **PPSE and Application Management for Secure Element**

### **Specification**

Version 1.0

May 2017

## Legal Notice

The EMV® Specifications are provided “AS IS” without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. 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 THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV Specifications 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 the EMV Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications 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 these Specifications 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 the EMV Specifications.

# Contents

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction .....</b>   | <b>7</b>  |
| 1.1      | Background .....  | 7         |
| 1.2      | Scope .....   | 7         |
| 1.3      | Audience .....  | 7         |
| 1.4      | References.....   | 8         |
| 1.4.1    | EMV Documents .....   | 8         |
| 1.4.2    | External References.....  | 8         |
| 1.5      | Definitions .....   | 9         |
| 1.6      | Notational Conventions .....                                      | 10        |
| 1.6.1    | Abbreviations.....  | 10        |
| 1.6.2    | Requirements Terminology .....                                    | 11        |
| 1.6.3    | Conventions .....   | 11        |
| 1.7      | Organisation of Document .....                                    | 12        |
| <b>2</b> | <b>Secure Element .....</b>                                       | <b>13</b> |
| 2.1      | The GlobalPlatform Environment (OPEN) .....                       | 14        |
| 2.2      | The PPSE Application.....   | 15        |
| 2.2.1    | PPSE on Mobile Devices .....                                      | 16        |
| 2.3      | Payment Applications.....   | 17        |
| 2.4      | CRS Application .....   | 18        |
| 2.5      | Other Contactless Applications .....                              | 19        |
| <b>3</b> | <b>PPSE Requirements.....</b>                                     | <b>21</b> |
| 3.1      | General Requirements .....  | 21        |
| 3.2      | SELECT Command.....   | 23        |
| 3.2.1    | Command Data .....  | 23        |
| 3.2.2    | Functional Requirements - Device Interface .....                  | 23        |
| 3.2.3    | Functional Requirements – Antenna Interface, External Mode.....   | 25        |
| 3.2.4    | Functional Requirements – Antenna Interface, Internal modes ..... | 27        |
| 3.2.5    | Response Data.....  | 29        |
| 3.3      | PUT TEMPLATE Command .....  | 32        |
| 3.3.1    | Command Data .....  | 32        |
| 3.3.2    | Functional Requirements .....                                     | 34        |
| 3.3.3    | Response Data.....  | 36        |
| 3.4      | GET TEMPLATE Command .....  | 37        |

|                |   |           |
|----------------|---|-----------|
| 3.4.1          | Command Data .....  | 37        |
| 3.4.2          | Functional Requirements .....   | 38        |
| 3.4.3          | Response Data.....  | 39        |
| 3.5            | SET MODE Command.....   | 40        |
| 3.5.1          | Command Data .....  | 40        |
| 3.5.2          | Functional Requirements .....   | 40        |
| 3.5.3          | Response Data.....  | 42        |
| 3.6            | Internal Mode(s) Processing .....   | 43        |
| 3.6.1          | FCI Building Rules.....   | 44        |
| 3.6.2          | Event Processing Rules .....  | 48        |
| 3.6.3          | Conditions of Use for Internal Modes .....  | 50        |
| 3.6.4          | Management of non-payment applications .....  | 51        |
| <b>4</b>       | <b>Secure Element Requirements .....</b>  | <b>52</b> |
| 4.1            | Activating/Deactivating Payment Applications .....  | 52        |
| 4.2            | Managing Priorities .....   | 53        |
| 4.3            | PPSE receipt of events (internal modes only).....   | 54        |
| 4.4            | Informing the Payment Card Manager .....  | 55        |
| <b>Annex A</b> | <b>Parameter Setting for Payment Applications .....</b>   | <b>57</b> |
| A.1            | Installation .....  | 57        |
| A.2            | Personalisation.....  | 60        |
| <b>Annex B</b> | <b>Alternative Activation Mechanism through the Payment Application – SET STATUS command.....</b> | <b>61</b> |
| B.1            | Command Data .....  | 61        |
| B.2            | Functional Behaviour of the Environment .....   | 63        |
| B.3            | Response Data .....   | 63        |
| <b>Annex C</b> | <b>Requirements Mapping Table .....</b>   | <b>65</b> |

## Figures

Figure 2.1: Secure Element Environment and Architecture ..... 14

## Tables

|  |    |
|--|----|
| Table 1-1: EMV Documents .....                                     | 8  |
| Table 1-2: External References .....                               | 8  |
| Table 1-3: Definitions .....                                       | 9  |
| Table 1-4: Abbreviations .....                                     | 10 |
| Table 3-1: PPSE supported instructions .....                       | 21 |
| Table 3-2: SELECT Command Message .....                            | 23 |
| Table 3-3: PPSE Response over the Device Interface .....           | 29 |
| Table 3-4: PPSE Response without an FCI Proprietary Template ..... | 29 |
| Table 3-5: PPSE Response with an FCI Proprietary Template .....    | 30 |
| Table 3-6: SELECT Command Responses .....                          | 31 |
| Table 3-7: PUT TEMPLATE Command Message .....                      | 32 |
| Table 3-8: PUT TEMPLATE Command P1 Usage .....                     | 32 |
| Table 3-9: PUT TEMPLATE Command Data .....                         | 33 |
| Table 3-10: PUT TEMPLATE Command Responses .....                   | 36 |
| Table 3-11: GET TEMPLATE Command Message .....                     | 37 |
| Table 3-12: GET TEMPLATE Command P1 Usage .....                    | 37 |
| Table 3-13: GET TEMPLATE Command Responses .....                   | 39 |
| Table 3-14: SET MODE Command Message .....                         | 40 |
| Table 3-15: SET MODE Command P1 Mode .....                         | 40 |
| Table 3-16: SET MODE Command Responses .....                       | 42 |
| Table A-1: Contactless Protocol Parameters – Installation .....    | 57 |
| Table A-2: User Interaction Parameters – Installation .....        | 58 |
| Table B-1: SET STATUS Command Message .....                        | 61 |
| Table B-2: SET STATUS Command P2 if P1 is '01' .....               | 62 |
| Table B-3: SET STATUS Command P2 if P1 is '02' .....               | 62 |
| Table B-4: SET STATUS Command Responses .....                      | 64 |

# Requirements

|   |    |
|---|----|
| R3.1: General Requirements .....  | 21 |
| R3.2: <b>SELECT</b> Command – Device Interface.....   | 23 |
| R3.3: <b>SELECT</b> Command – Antenna Interface, External Mode /<br>Mobile Device Switched On .....     | 25 |
| R3.4: <b>SELECT</b> Command – Antenna Interface, External Mode /<br>Mobile Device Not Switched On.....  | 26 |
| R3.5: <b>SELECT</b> Command – Antenna Interface, Internal modes /<br>Mobile Device Switched On .....    | 27 |
| R3.6: <b>SELECT</b> Command – Antenna Interface, Internal modes /<br>Mobile Device Not Switched On..... | 28 |
| R3.7: <b>PUT TEMPLATE</b> Command .....   | 34 |
| R3.8: <b>GET TEMPLATE</b> Command .....   | 38 |
| R3.9: <b>SET MODE</b> Command .....   | 40 |
| R3.10: General for Internal Modes.....  | 43 |
| R3.11: FCI Building Rules.....  | 44 |
| R3.12: Event Processing .....   | 48 |
| R4.1: Secure Element Requirements – Activating/Deactivating contactless applications ....               | 52 |
| R4.2: Secure Element Requirements – Managing Priorities.....  | 54 |
| R4.3: Secure Element Requirements – Informing the PPSE .....  | 54 |

# 1 Introduction

## 1.1 Background

EMVCo published the *Application Activation User Interface ([AAUI])* document in December 2010. Since the publication of the original *[AAUI]* document, the mobile device and mobile payment landscape has changed considerably, and some of the concepts and predictions in the original document have not materialized or have followed a different path.

The original *[AAUI]* document was agnostic of the Secure Element Contactless Management (SECM) used for managing contactless applications on a Secure Element, and *GlobalPlatform Card Contactless Services [GPCARD C]* was only considered to be one option for a SECM. Today, *[GPCARD C]* has become the de facto market standard for SECM, and no alternative has emerged. As such, the relevant content specific to *[GPCARD C]* has been extracted from the original *[AAUI]* document and combined with an overview of managing applications on Secure Elements to form this document.

Additionally, over the intervening years, in order to enhance the quality of approved contactless products, EMVCo has refined the test cases applying to Secure Element hosted PPSE applications, and the requirements matching these test cases are reflected herein.

## 1.2 Scope

Requirements detailed herein correspond to those tested by EMVCo for the functional (Level 2) type approval of Secure Elements and PPSE applications for *[GPCARD C]* compliant platforms. They are equivalent to the requirements originally presented in *[AAUI]*, integrate the modifications of the latest applicable Specification Update Bulletins, and are presented slightly differently.

This document should be read in conjunction with the white paper document *[PCM]*.

## 1.3 Audience

This document is primarily intended for use by entities designing, developing, implementing, and testing a PPSE application residing in a Secure Element of the Mobile Device.

It will also be useful to entities developing Payment Applications and Payment Card Manager applications, entities responsible for the provisioning of those applications, and entities responsible for the presence of the PPSE functionality on the Secure Element, e.g. handset manufacturers, operating system providers, mobile network operators, mobile application developers, smart card application developers, etc.

## 1.4 References

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

### 1.4.1 EMV Documents

EMV documents are available on the EMVCo website:

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

**Table 1-1: EMV Documents**

| Reference | Publication Name  |
|-----------|---|
| [AAUI]    | Application Activation User Interface – Overview, Usage Guidelines, and PPSE Requirements                     |
| [Book D]  | Contactless Specifications for Payment Systems: Book D – EMV Contactless Communication Protocol Specification |
| [ENTRY]   | Contactless Specifications for Payment Systems: Book B – Entry Point Specification                            |
| [PCM]     | Payment Card Management White paper   |

### 1.4.2 External References

**Table 1-2: External References**

| Reference       | Publication Name   |
|-----------------|--|
| [GPCARD]        | GlobalPlatform Card Specification  |
| [GPCARD C]      | Contactless Services – GlobalPlatform Card Specification – Amendment C: Contactless Services |
| [ISO/IEC 14443] | Identification cards – Contactless integrated circuit(s) cards – Proximity cards             |

## 1.5 Definitions

The following terms are used in this specification:

**Table 1-3: Definitions**

| Term                 | Definition   |
|----------------------|--|
| AAUI                 | Application Activation User Interface, the former terminology used in <i>[AAUI]</i> , referring to a Payment Card Manager.   |
| Application Group    | A set of contactless applications consisting of a group head application and one or more member applications. From a consumer point of view, a group is synonymous with a single Payment Card on their Mobile Device that gives them access to multiple contactless services. For example, a group could comprise multiple Payment Applications, one of which is designated by the product owner as the group head and the others as members of the group. With regards to application activation and priority changes, only the group head is consumer facing, and actions that affect the group head also affect all the group members.<br><br>See <i>[GPCARD C]</i> for further details about Application Groups. |
| CMP Application      | Contactless Mobile Payment Application, the former terminology used in <i>[AAUI]</i> , referring to a Payment Application.   |
| Payment Application  | A contactless application that performs information exchange and processing needed to perform a contactless payment transaction. It may be hosted in the same Secure Element as the PPSE, or in a different Secure Element, or in the HCE environment.   |
| Payment Card         | A consumer-facing payment service presented to the Consumer as a single product – generally represented by a card visual in a Payment Card Manager.<br><br>A Payment Card may comprise a unique Payment Application, or an Application Group of contactless applications – including at least one Payment Application.   |
| Payment Card Manager | A consumer visible application resident within the Mobile Device's application environment and used by the consumer to manage which – of the possible multiple – Payment Card(s) will be used for conducting contactless payments. More than one Payment Card Manager may be present on a Mobile Device.   |

| Term        | Definition  |
|-------------|---|
| PPSE        | The Proximity Payment Service Environment is the first contactless application selected by a Merchant Terminal presenting the contactless applications available for conducting a transaction.  |
| Switched On | A state where the Mobile Device is powered up and the user interface (screen, keyboard, etc.) is available for use.<br><br>For the purposes of this document, there is only one other applicable Mobile Device power state; that is, where the user interface is not available because the device is not Switched On. For example, power is below the threshold at which the user interface becomes active, the Mobile Device is switched off, or the battery is depleted or removed. |

## 1.6 Notational Conventions

### 1.6.1 Abbreviations

The abbreviations listed in Table 1-4 are used in this specification.

**Table 1-4: Abbreviations**

| Abbreviation | Description                           |
|--------------|---------------------------------------|
| AAUI         | Application Activation User Interface |
| ADF          | Application Definition File           |
| AID          | Application Identifier                |
| API          | Application Programming Interface     |
| CREL         | Contactless Registry Event Listener   |
| CRS          | Contactless Registry Services         |
| FCI          | File Control Information              |
| HCE          | Host Card Emulation                   |
| NFC          | Near Field Communication              |
| PPSE         | Proximity Payment System Environment  |

| Abbreviation | Description                           |
|--------------|---------------------------------------|
| SECM         | Secure Element Contactless Management |
| TLV          | Tag, Length, Value                    |
| UICC         | Universal Integrated Circuit Card     |

## 1.6.2 Requirements Terminology

The following (words are used often in this specification and have specific meanings:

### **SHALL**

Defines a product or system capability which is mandatory.

### **MAY**

Defines a product or system capability which is optional or a statement which is informative only and is out of scope for this specification.

### **SHOULD**

Defines a product or system capability which is recommended.

## 1.6.3 Conventions

The following conventions apply:

### **Requirement Numbering**

Requirements in this specification are uniquely numbered with the number appearing next to each requirement: For example:

---

R3.8.2 **If** the GET TEMPLATE command is received over the antenna interface,  
**then** a response of '6985' SHALL be returned.

---

A requirement may have different numbers in different versions of the specifications. Hence, all references to a requirement should include the version of the specification as well as the requirement's number.

Requirements may include informative statements. In this case, the statement is written in the italic font and the verb 'MAY' instead of 'SHALL' is used.

## 1.7 Organisation of Document

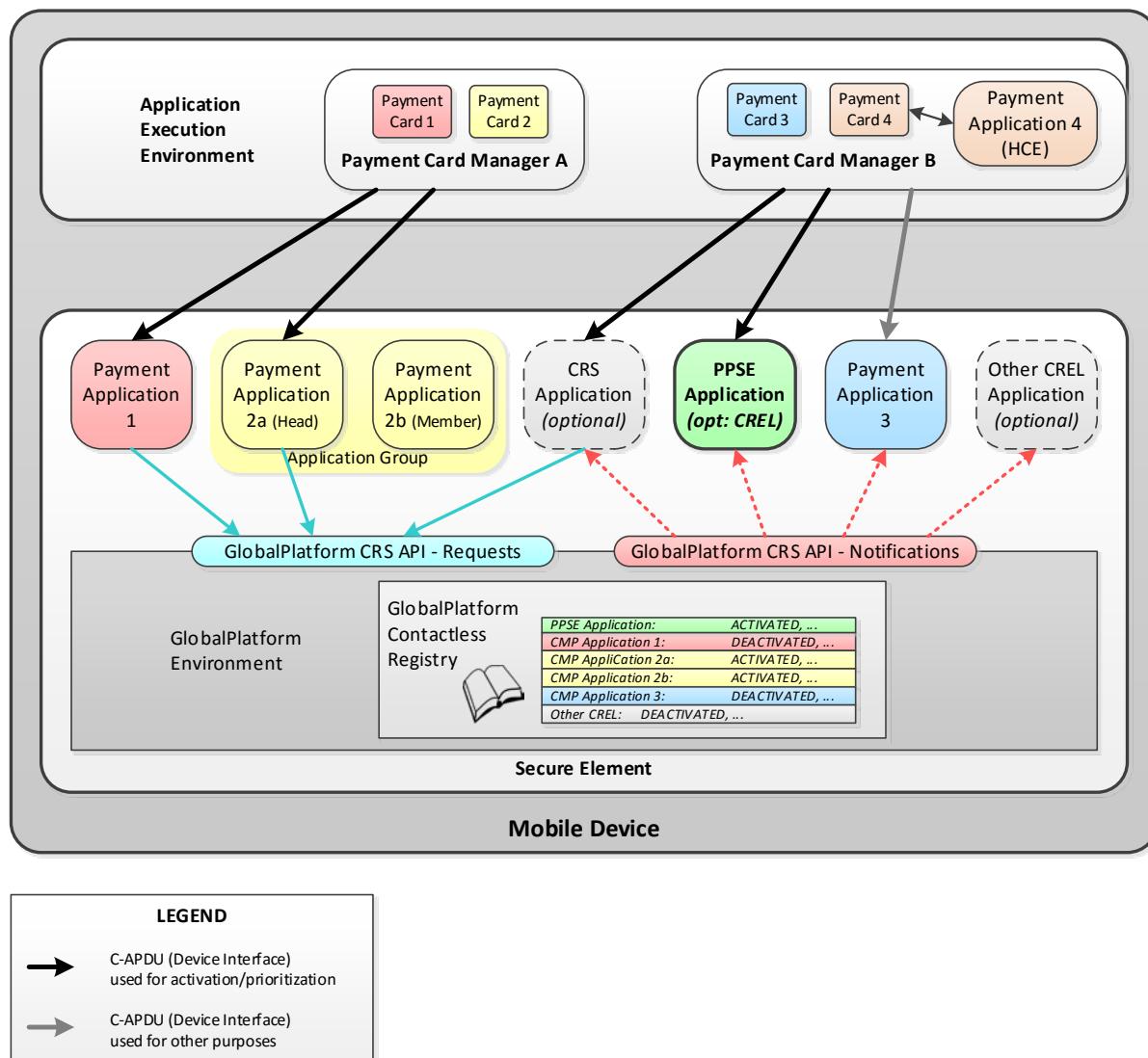
This document contains the following information:

- Chapter 1 contains general information that helps the reader understand and use this specification
- Chapter 2 introduces the architecture of the Secure Element that will host the PPSE Application (applet) and, optionally, Payment Applications (applets)
- Chapter 3 specifies the Secure Element hosted PPSE application, for the three modes (External Mode, Internal Mode and Internal Mode with Mutual Exclusivity Rule)
- Chapter 4 defines the required behaviour of Secure Elements intended to host Payment Applications or the PPSE application
- Annex A details the contactless parameters that must be set for Payment Applications during installation or personalisation
- Annex B proposes an alternative for managing contactless application activation. This alternative can be used when the Payment Card Manager cannot interact with the Secure Element's CRS application. In this case, the Payment Card Manager interacts with each Payment Application to manage the Payment Application's activation state
- Annex C establishes a correspondence between the numbering of requirements in this document and the requirements/sections in the original [AAUJ] and the associated Specification Update Bulletins

## 2 Secure Element

As per the *[PCM]*, the architecture of a device capable of Contactless Mobile Payment is, at minimum, an NFC-capable Mobile Device with an NFC Controller, an antenna, and an application environment hosting one or more Payment Card Managers. In addition, the device requires an Execution Environment capable of hosting a contactless Payment Application. This environment could be the device's own application environment (i.e. for HCE) or a Secure Element (the focus of this document).

A Secure Element in the Mobile Device, such as an embedded Secure Element or a UICC, complies with the GlobalPlatform Card Specifications *[GPCARD]* and, specifically to manage contactless applications, the GlobalPlatform Contactless Services *[GPCARD C]*. In general, *[GPCARD]* enables the loading, installation and management of applications (applets) within the application environment of the Secure Element. Amendment C *[GPCARD C]* enables the management of an application's contactless aspects if these applications are intended for use over the antenna interface of the Secure Element. The PPSE application developed in accordance with this specification is installed in this Secure Element. Likewise, Payment Applications and other applications may also be installed in this Secure Element.

**Figure 2.1: Secure Element Environment and Architecture**

## 2.1 The GlobalPlatform Environment (OPEN)

This document targets Secure Elements complying with [GPCARD] (v2.2 or higher) and [GPCARD C] (v1.0 or higher). The latter provides numerous and highly valuable tools for the management of contactless applications in the Secure Element, such as:

- A Contactless Registry within the GlobalPlatform environment that stores the contactless-related parameters of each contactless application (contactless activation state, selection priority, volatile priority, Application Group parameters, proprietary information, RF parameters, etc.)

Note that GlobalPlatform is deprecating support for volatile priority and as such, while still described herein, its usage is not recommended and it is also being deprecated for the PPSE.

- A Contactless Registry Service (CRS) API enabling applications to read from or write to the Contactless Registry – within the limit of the rights and privileges allocated to such applications
- The possibility for contactless applications – within the limit of their allocated rights and privileges – to receive notifications when the contactless-related parameters for themselves or for other contactless applications change
- The possibility to create Application Groups allowing a single customer-facing contactless service – comprising multiple underlying contactless applications – to be activated and deactivated simultaneously
- The notion of a selectable CRS application allowing a device resident application to manage the activation state and priority of contactless applications in the Secure Element (see section 2.4)
- The notion of Contactless Registry Event Listener (CREL) application(s), enabling privileged applications (CRELs) to be notified when the contactless parameters of related contactless applications change

## 2.2 The PPSE Application

The main purpose of any PPSE is to return File Control Information (FCI) as a response to the selection of the PPSE application over an antenna interface. The content of the FCI contains a single directory entry or a list of directory entries. Note that, in addition to the Payment Application directory entries, other contactless application directory entries may be present in the FCI.

Each Payment Application Directory Entry identifies the following information applicable to the entity selecting the PPSE (typically a Merchant Terminal):

- The Payment Application available for selection (by AID) and use by the Merchant Terminal
- The usage priority of each Payment Application; that is, the lower the value, the higher the priority<sup>1</sup>
- The specific Merchant Terminal application underpinning the product; that is, the kernel to be used to interact with this Payment Application
- Other application-specific data

---

<sup>1</sup> Except that priority '0' means no priority assigned.

All EMVCo contactless payments are required to support the use of the PPSE. The PPSE in a card form factor has traditionally contained a static list of supported Payment Applications, accessible over the antenna interface, personalised with an Issuer-defined prioritisation of each Payment Application, and accessible over the antenna interface in the SELECT command response. The mapping of the PPSE FCI can be found in *[ENTRY]* as well as in section 3.2.5 of this document. For further information regarding the processing of the PPSE FCI by a contactless reader, please refer to *[ENTRY]*.

## 2.2.1 PPSE on Mobile Devices

For Mobile Devices, the PPSE typically contains additional functionality that allows the Payment Application(s) reflected in the PPSE to be dynamically managed by the consumer through a Payment Card Manager. This mobile-specific functionality allows a Payment Card Manager to control the PPSE's SELECT command response depending on the Payment Card choices of the consumer.

Additionally, Payment Applications may be configured to be available (or not) when the Device is not Switched On. Therefore, the SELECT command response could depend on the PPSE's assumption related to whether or not the Mobile Device is Switched On at the time it is presented to a Merchant Terminal.

The PPSE FCI contains the list of Payment Applications available for the Merchant Terminal. Non-payment contactless applications may also be present in the PPSE FCI, provided that these applications are intended to be selected by Merchant Terminals supporting contactless payments, and that these terminals make use of the PPSE for the application selection process. Typically, loyalty or transport applications may be referenced in the PPSE FCI.

This specification focuses on the mechanisms used to populate/configure the PPSE with Directory Entries and how to indicate which Directory Entries are, at a given point in time, returned to the Merchant Terminal. Three mechanisms are defined for achieving this: External Mode, Internal Mode and Internal Mode with Mutual Exclusivity Rule. These modes relate to the manner in which the PPSE application in the Secure Element receives, acts on, and builds the information that will be provided to a Merchant Terminal.

- External Mode – When this mode is being used, the Payment Card Manager provides – directly to the PPSE – the Directory Entry of each Payment Application that will be returned to a Merchant Terminal.

External Mode is suitable for a single Secure Element environment as well as when multiple Execution Environments (Secure Element(s) and/or HCE) are active simultaneously. The Payment Card Manager provides the PPSE with the SELECT command responses to be returned to the Merchant Terminal.

In Figure 2.1, Payment Card Manager B interacts with the PPSE application in External Mode, as seen from the black arrow linking these two entities.

- Internal Mode – When this mode is being used, the PPSE will itself, internally to the Secure Element, collect the details of the active applications from the GlobalPlatform CRS and build the data to be returned to the Merchant Terminal.

Internal Mode implies that the Secure Element platform provides a means for the PPSE to determine which contactless applications are active. The PPSE uses information provided by the GlobalPlatform environment related to these active applications to build the SELECT command response to be returned to the Merchant Terminal. The PPSE also needs to be able to receive notifications of changes to contactless parameters for these applications. To enable this behaviour in the frame of *[GPCARD C]*, the PPSE must be declared as a Contactless Registry Event Listener (CREL) for all Payment Applications.

Internal Mode can only be used when a single Secure Element is active. There is no interaction between Execution Environments (Secure Elements and/or HCE) that will allow a PPSE in this mode to be notified of a state change of an application on another Execution Environment or that will allow a PPSE to determine the state of applications on other Execution Environments. Therefore, when multiple Execution Environments are to be simultaneously active, External Mode is the only mode possible.

In Figure 2.1, Payment Card Manager A uses the PPSE application in Internal Mode, as there is no direct arrow linking these two entities.

- Internal Mode with Mutual Exclusivity Rule – This mode is a variant of Internal Mode and is intended to ensure that no more than one Payment Card can be active at any time. When configured for this mode, the PPSE application behaves as if configured for Internal Mode, but over and above regular Internal Mode, it will deactivate any currently active Payment Application (or Application Group) when it is notified that a new Payment Application (or Application Group) has been activated.

An implementation of the PPSE may support one, two, or three modes and it is the Payment Card Manager that will configure the PPSE to behave in an expected manner.

## 2.3 Payment Applications

Besides the PPSE, the Secure Element may also host contactless Payment Applications. For these Payment Applications, the Payment Card Manager may be able to retrieve contactless specific information, must be able to set the Payment Application's activation state, and (if applicable) must be able to set the Payment Application's selection priority.

A Payment Application corresponds to the technical implementation of a Payment Card service (or part of it, if the Payment Card represents multiple Payment Applications) offered in a Payment Card Manager. During a contactless transaction, it processes the commands received over the antenna interface from the Merchant Terminal. The Payment Application may also receive and process commands over the device interface from a Payment Card Manager.

When the PPSE is configured in either of the internal modes, the Secure Element hosting the PPSE application also hosts all the Payment Applications that are intended to be included in the FCI of the PPSE. Each of these Payment Applications must declare the PPSE application as a CREL.

When the PPSE is configured in External Mode, Payment Applications may be installed in any Secure Element of the mobile device (in the same Secure Element as the PPSE or in a different one), or even in the HCE environment.

Each Payment System defines their own requirements for their Payment Applications. Payment Applications may offer the following contactless management services to Payment Card Managers:

- Activation/deactivation of the Payment Application on the antenna interface (see Annex B)
- Setting or resetting of volatile priority (see Annex B)<sup>2</sup>

When a single Payment Card represents multiple Payment Applications, these Payment Applications should be hosted inside the same Secure Element and should constitute an Application Group, as defined by [GPCARD C].

## 2.4 CRS Application

Depending on deployment choices, the Secure Element will also host a CRS application and may provide an APDU interface to a Payment Card Manager, providing direct access to the CRS. Alternatively, if this APDU interface is not present, the CRS may receive Payment Card Manager requests indirectly through the Payment Applications.

---

<sup>2</sup> The use of volatile priority is deprecated by EMVCo.

If providing a direct APDU interface, this will be a single interface to all Payment Card Managers to manage all underlying Payment Applications installed in the same Secure Element to facilitate the following:

- Global activation/deactivation of the antenna interface for the Secure Element
- Activation/deactivation of each contactless application individually (or as an Application Group) on the antenna interface
- Changing the selection priority for contactless applications
- Setting or resetting of volatile priority for contactless applications<sup>3</sup>
- Retrieval of contactless parameters from the CRS

GlobalPlatform [GPCARD C] proposes a standard implementation of the CRS application. The services listed above are offered by the GlobalPlatform CRS application with the command APDUs GET STATUS and SET STATUS. See [GPCARD C] section 3.11 for further details.

As per the GlobalPlatform specifications, there is at most one CRS application in the Secure Element, and the APDU interface to the CRS application in the Secure Element is optional.

If the CRS application is not available for use through the APDU interface, Payment Card Managers should use the contactless management functionality offered by each Payment Application – a standardized APDU interface is described in Annex B. However, in the absence of an APDU interface to the CRS application, some management functions like changing the selection priority of Payment Applications will definitely be unavailable to Payment Card Managers. When this is the case, the Secure Element configuration should ensure that no more than one Payment Card is active at a given time. This can be achieved by a dedicated Contactless Registry Event Listener (CREL) application, or by the PPSE application itself (see the description for Internal Mode with Mutual Exclusivity Rule).

## 2.5 Other Contactless Applications

Besides Payment Applications, the PPSE and the CRS application, other applications may be present in the Secure Element at the discretion of the Secure Element issuer/manager. These would typically include third-party service provider applications e.g. loyalty, transport, communication, authentication, gaming etc. and are largely out of scope of this document.

Contactless payment may be associated with the processing of loyalty information by the Merchant Terminal. Depending on implementation choices, loyalty applications may or may not be visible to Merchant Terminals in the PPSE FCI.

---

<sup>3</sup> The use of volatile priority is deprecated by GlobalPlatform.

Some Secure Element configurations may include additional, non-consumer-facing applications serving payment purposes. For example, as opposed to using the Internal Mode with Mutual Exclusivity Rule, the Secure Element may host a dedicated CREL application that deactivates the currently active Payment Application when a new Payment Application is activated.

## 3 PPSE Requirements

### 3.1 General Requirements

Table 3-1 summarizes the instructions that are supported by a PPSE application in a Secure Element, based on the currently active mode and depending on the interface on which the instruction is received.

**Table 3-1: PPSE supported instructions**

| Instruction  | Device Interface                 |  |               | Antenna Interface |  |               |
|--------------|----------------------------------|--|---------------|-------------------|--|---------------|
|              | Internal Mode                    | Internal Mode with Mutual Exclusivity Rule | External Mode | Internal Mode     | Internal Mode with Mutual Exclusivity Rule | External Mode |
| SELECT       | Yes                              | Yes  | Yes           | Yes               | Yes  | Yes           |
| PUT TEMPLATE | No                               | No   | Yes           | No                | No   | No            |
| GET TEMPLATE | Yes                              | Yes  | Yes           | No                | No   | No            |
| SET MODE     | If more than 1 mode is supported |  |               | No                | No   | No            |

The following are general functional requirements. Command-specific functional requirements are listed in the following sections.

---

#### R3.1: General Requirements

---

R3.1.1 The PPSE application SHALL be installed with the Contactless Protocol Parameters specified in Table A-1.

R3.1.2 The SELECT command SHALL be accessible over the device interface and over the antenna interface.

---

---

### R3.1: General Requirements

---

- R3.1.3 **If a SELECT command is received and the PPSE application is already selected on another logical channel over the device or antenna interface then the SELECT command SHALL be rejected with an error Status Word<sup>4</sup>.**
- R3.1.4 The GET TEMPLATE command SHALL be supported.  
It SHALL be accessible over the device interface and SHALL NOT be accessible over the antenna interface.
- R3.1.5 The SET MODE command SHALL be supported if the PPSE supports two or three modes.  
**If the SET MODE command is supported, then it SHALL be accessible over the device interface and SHALL NOT be accessible over the antenna interface.**
- R3.1.6 **If the PPSE supports External Mode, then the PUT TEMPLATE command SHALL be accessible over the device interface and SHALL NOT be accessible over the antenna interface.**
- 

---

<sup>4</sup> The actual Status Word value may be platform-dependent but it shall correspond to an error Status Word, i.e. SW different from '9000', '61XX', '62XX' or '63XX'

## 3.2 SELECT Command

The PPSE hosted in a Secure Element can be selected over the device interface as well as over the antenna interface. However, in order to guarantee an atomic session, the PPSE does not support multiple selections simultaneously over the device interface and over the antenna interface (see R3.1.3).

Payment Card Managers using the device interface are thus requested to close the connection with the PPSE application as soon as they have completed their processing with PPSE, even if the Payment Card Manager is still processing other functions, so as to release the PPSE for subsequent selection by a Merchant Terminal or another Payment Card Manager.

### 3.2.1 Command Data

Table 3-2: SELECT Command Message

| Code | Value                            |
|------|----------------------------------|
| CLA  | '00' – '03', '40' – '4F'         |
| INS  | 'A4'                             |
| P1   | '04'                             |
| P2   | '00'                             |
| Lc   | Length of the command data field |
| Data | '2PAY.SYS.DDF01'                 |
| Le   | '00'                             |

### 3.2.2 Functional Requirements - Device Interface

Requirements R3.2 apply to the SELECT command when received over the device interface only. They apply to all three modes.

#### R3.2: SELECT Command – Device Interface

- R3.2.1 **If** a SELECT command is received over the device interface,  
**and** the PPSE application is not active over the antenna interface,  
**then** the PPSE application SHALL become active over the antenna interface.
- R3.2.2 **If** a SELECT command is received over the device interface,  
**then** the PPSE response, constructed as specified in Table 3-3  
SHALL be returned.

---

### R3.2: SELECT Command – Device Interface

---

R3.2.3 **If** any of the following is true:

- the PPSE only supports [External Mode], **or**
- the PPSE was originally configured to support [External Mode] and has never received a SET MODE command, **or**
- the most recently received SET MODE command configured the PPSE to operate in [External Mode],

**then** the value for tag '89' in the PPSE response to the SELECT command SHALL be '01' [External Mode].

---

R3.2.4 **If** any of the following is true:

- the PPSE only supports [Internal Mode], **or**
- the PPSE was originally configured to support [Internal Mode] and has never received a SET MODE command, **or**
- the most recently received SET MODE command configured the PPSE to operate in [Internal Mode],

**then** the value for tag '89' in the PPSE response to the SELECT command SHALL be '02' [Internal Mode].

---

R3.2.5 **If** any of the following is true:

- the PPSE only supports [Internal Mode with Mutual Exclusivity Rule], **or**
- the PPSE was originally configured to support [Internal Mode with Mutual Exclusivity Rule] and has never received a SET MODE command, **or**
- the most recently received SET MODE command configured the PPSE to operate in [Internal Mode with Mutual Exclusivity Rule],

**then** the value for tag '89' in the PPSE response to the SELECT command SHALL be '03' [Internal Mode with Mutual Exclusivity Rule].

---

### 3.2.3 Functional Requirements – Antenna Interface, External Mode

Requirements in this section apply when the PPSE is configured to operate in [External Mode], when the SELECT command is received over the antenna interface

- Requirements R3.3 (in the order listed) apply when the Mobile Device is Switched On or when the PPSE is incapable of determining (or does not implement functionality to determine) whether the Mobile Device is Switched On.
- Requirements R3.4 (in the order listed) may apply when the PPSE is capable of determining whether the Mobile Device is Switched On and it is not.

---

#### R3.3: SELECT Command – Antenna Interface, External Mode / Mobile Device Switched On

---

R3.3.1 **If** the most recent PUT TEMPLATE command received had a usage parameter of '05' [Mandatory data only],  
**then** the PPSE response to the SELECT command, constructed as specified in Table 3-4, SHALL be returned.

---

R3.3.2 **If** any of the following is true:

- the PPSE has not received a PUT TEMPLATE command since being configured to operate in [External Mode], **or**
- the most recent PUT TEMPLATE command received had a usage parameter of '06' [Hide], **or**
- the most recent PUT TEMPLATE command received had a usage parameter of '04' [Cancel override] and no [Device Switched On no override] FCI is currently configured,

**then** a response of '6A82' [Application not found] SHALL be returned.

---

R3.3.3 **If** no override is currently set,  
**then** the FCI built on receipt of the most recent PUT TEMPLATE command with a usage parameter of '01' [Device Switched On no override] SHALL be returned.

---

---

### R3.3: SELECT Command – Antenna Interface, External Mode / Mobile Device Switched On

---

R3.3.4 **If** all of the following are true:

- An FCI was built on receipt of the most recent PUT TEMPLATE command with a usage parameter of '03' [Override until cancelled], **and**
- No subsequent PUT TEMPLATE command with a usage parameter of '04' [Cancel override] or '05' [Mandatory data only] or '06' [Hide] has been received, **and**
- The override has not been cancelled due to the Mobile Device being switched off (see R3.4.2).

**then** the FCI built on receipt of the most recent PUT TEMPLATE command with a usage parameter of '03' [Override until cancelled] SHALL be returned.

---

### R3.4: SELECT Command – Antenna Interface, External Mode / Mobile Device Not Switched On

---

R3.4.1 **If** the most recent PUT TEMPLATE command received had a usage parameter of '05' [Mandatory data only],  
**then** the PPSE response to the SELECT command, constructed as specified in Table 3-4, MAY be returned,  
else,

- **If** no [Device not Switched On] FCI is currently configured,  
**then** a response of '6A82' [Application not found] MAY be returned,  
**else**,  
the FCI built on receipt of the most recent PUT TEMPLATE command with a usage parameter of '02' [Device not Switched On] MAY be returned.

R3.4.2 **If** the most recent PUT TEMPLATE command had a usage parameter of '03' [Override until cancelled]  
(and even though no subsequent PUT TEMPLATE command with a usage parameter of '04' [Cancel override] has been received),  
**then** the [Override until cancelled] FCI MAY be cancelled.

---

### 3.2.4 Functional Requirements – Antenna Interface, Internal modes

Similar to [External Mode] (see section 3.3 for details of how these FCI values are set), a PPSE supporting [Internal Mode] or [Internal Mode with Mutual Exclusivity Rule] may support up to three FCI values:

- The PPSE always supports functionality to build the FCI value [Device Switched On no override].
- The PPSE may support functionality to build the FCI value [Device not Switched On] if the platform allows applications to determine whether the device is switched on or off.
- The PPSE may support functionality to build the FCI value [Override until cancelled] if the platform is able to transmit to CREL applications the events notifying a volatile priority change<sup>5</sup>. Such events are only transmitted on Secure Elements supporting [GPCARD C] version 1.1 and 1.2.

Requirements in this section apply when the PPSE is configured to operate in [Internal Mode] or in [Internal Mode with Mutual Exclusivity Rule], when the SELECT command is received over the antenna interface

- Requirements R3.5 apply when the Mobile Device is Switched On, or when the PPSE is incapable of determining (or does not implement functionality to determine) whether or not the Mobile Device is Switched On.
- Requirements R3.6 may apply when the PPSE is capable of determining whether the Mobile Device is Switched On and it is not.

---

#### R3.5: SELECT Command – Antenna Interface, Internal modes / Mobile Device Switched On

---

- R3.5.1 **If** no contactless application has indicated to the PPSE that it is in the active state (that is, FCIs [Device Switched On no override] and [Override until cancelled] are currently empty),  
**then** a response of '6A82' [Application not found] SHALL be returned.
- 

<sup>5</sup> The use of volatile priority is deprecated by GlobalPlatform.

---

**R3.5: SELECT Command – Antenna Interface, Internal modes / Mobile Device Switched On**

---

- R3.5.2 **If** no contactless application is assigned the volatile priority (that is, FCI [Override until cancelled] is currently empty), **and** one or more contactless applications have indicated to the PPSE that they are in the active state (that is, FCI [Device Switched On no override] is currently NOT empty), **then** the PPSE response SHALL contain the FCI [Device Switched On no override].
- R3.5.3 **If** a contactless application is assigned the volatile priority (that is, FCI [Override until cancelled] is currently NOT empty), **then** the PPSE response SHALL contain the FCI [Override until cancelled].
- 

**R3.6: SELECT Command – Antenna Interface, Internal modes / Mobile Device Not Switched On**

---

- R3.6.1 **If** either of the following is true:
- no contactless payment application is in the active state, **or**
  - there are contactless payment applications in the active state, **but** none of these is configured for operation when the Mobile Device is not Switched On (that is, FCI [Device not Switched On] is currently empty),  
**then** a response of '6A82' [application not found] MAY be returned.
- R3.6.2 **If** one or more contactless payment applications that are configured for use when the Mobile Device is not Switched On are in the active state (that is, FCI [Device not Switched On] is currently NOT empty), **then** the PPSE response returned MAY contain the FCI [Device not Switched On].
-

### 3.2.5 Response Data

The PPSE response depends on whether the PPSE is being selected over the device interface (by the Payment Card Manager) or over the antenna interface (by the Merchant Terminal).

The response to a SELECT command received from the Payment Card Manager over the device interface is coded as per Table 3-3.

**Table 3-3: PPSE Response over the Device Interface**

| Tag  | Value        |  | Presence |
|------|--------------|--|----------|
| '6F' | FCI Template |  | M        |
|      | '84'         | '2PAY.SYS.DDF01'   |          |
|      | 'A5'         | FCI Proprietary Template   |          |
|      | '9F08'       | Version Number:<br>• '3130': as per [AAU]<br>• '3131': as per this document  |          |
|      | '89'         | Current Mode:<br>• '01' – External Mode<br>• '02' – Internal Mode<br>• '03' – Internal Mode with Mutual Exclusivity Rule |          |

The response to a SELECT command received over the antenna interface is coded as per:

- Table 3-4 to indicate that the Mobile Device is an EMV-enabled device but no EMV-based contactless applications are to be accessible over the antenna interface, or
- Table 3-5 if at least one EMV-based contactless application is to be accessible over the antenna interface.

**Table 3-4: PPSE Response without an FCI Proprietary Template**

| Tag  | Value        |                  | Presence |
|------|--------------|------------------|----------|
| '6F' | FCI Template |                  | M        |
|      | '84'         | '2PAY.SYS.DDF01' |          |

**Table 3-5: PPSE Response with an FCI Proprietary Template**

| Tag  | Value                    |   | Presence |   |
|------|--------------------------|---|----------|---|
| '6F' | FCI Template             |   | M        |   |
| '84' | '2PAY.SYS.DDF01'         |   | M        |   |
| 'A5' | FCI Proprietary Template |   | M        |   |
|      | 'BF0C'                   | FCI Issuer Discretionary Data                           |          | M |
|      | '61'                     | Directory Entry   |          | M |
|      | '4F'                     | DF Name (AID)   | M        |   |
|      | '50'                     | Application label                                       | O        |   |
|      | '87'                     | Priority indicator                                      | C        |   |
|      | '9F2A'                   | Kernel Identifier                                       | C        |   |
|      | '9F0A'                   | Application Selection<br>Registered Proprietary<br>Data | O        |   |
|      | ...                      |   |          | O |
|      | ...                      |   |          |   |
|      | '61'                     | Directory Entry   |          | O |
|      | '4F'                     | DF Name (AID)   | O        |   |
|      | '50'                     | Application label                                       | O        |   |
|      | '87'                     | Priority indicator                                      | O        |   |
|      | '9F2A'                   | Kernel Identifier                                       | O        |   |
|      | '9F0A'                   | Application Selection<br>Registered Proprietary<br>Data | O        |   |
|      | ...                      |   |          | O |

The response Status Word may contain one of the values shown in Table 3-6.

**Table 3-6: SELECT Command Responses**

| Field | Length | Value       |        |                       |
|-------|--------|-------------|--------|-----------------------|
| SW    | 2      | Status Word |        |                       |
|       |        | Value       | Type   | Meaning               |
|       |        | '6A86'      | Error  | Incorrect P1/P2       |
|       |        | '6A82'      | Error  | Application not found |
|       |        | '9000'      | Normal | Successful processing |

## 3.3 PUT TEMPLATE Command

The PUT TEMPLATE command enables the Payment Card Manager to define one of the FCI Proprietary Templates to be returned in response to a subsequent SELECT command over the antenna interface.

### 3.3.1 Command Data

**Table 3-7: PUT TEMPLATE Command Message**

| Code | Value                            |
|------|----------------------------------|
| CLA  | '80' – '83', 'C0' – 'CF'         |
| INS  | 'D2'                             |
| P1   | Usage – see Table 3-8            |
| P2   | '00'                             |
| Lc   | Length of the command data field |
| Data | FCI Proprietary Template         |
| Le   | Not present                      |

#### Usage (P1)

This parameter indicates when this FCI Proprietary Template is to be used.

**Table 3-8: PUT TEMPLATE Command P1 Usage**

| Code | Meaning                           |
|------|-----------------------------------|
| '01' | Device Switched On no override    |
| '02' | Device not Switched On (optional) |
| '03' | Override until cancelled          |
| '04' | Cancel override                   |
| '05' | Mandatory data only (Delete all)  |
| '06' | Hide                              |

#### Length

If P1 is '04', '05', or '06', then length (Lc) is one ('01').

Otherwise, length (Lc) contains the length of the FCI Proprietary Template.

## Data

If P1 is '04', '05', or '06', then the command data is a single byte of '00'. Otherwise, the data is formatted as per Table 3-9.

**Table 3-9: PUT TEMPLATE Command Data**

| Value  |                               |        | Presence  |                |
|--------|-------------------------------|--------|---|----------------|
| 'A5'   | FCI Proprietary Template      |        | M   |                |
| 'BF0C' | FCI Issuer Discretionary Data |        | M   |                |
| '61'   | Directory Entry               |        | M   |                |
|        |                               | '4F'   | DF Name (AID)                                     | M              |
|        |                               | '50'   | Application label                                 | O              |
|        |                               | '87'   | Priority indicator                                | C              |
|        |                               | '9F2A' | Kernel Identifier                                 | C              |
|        |                               | '9F0A' | Application Selection Registered Proprietary Data | O              |
|        |                               | ...    | O   |                |
| ...    |                               |        | O   |                |
| '61'   | Directory Entry               |        | O   |                |
|        |                               | '4F'   | DF Name (AID)                                     | M <sub>6</sub> |
|        |                               | '50'   | Application label                                 | O              |
|        |                               | '87'   | Priority indicator                                | C              |
|        |                               | '9F2A' | Kernel Identifier                                 | C              |
|        |                               | '9F0A' | Application Selection Registered Proprietary Data | O              |
|        |                               | ...    | O   |                |

<sup>6</sup> Only relevant if the Directory Entry is present.

### 3.3.2 Functional Requirements

---

#### R3.7: PUT TEMPLATE Command

---

- R3.7.1 **If** P1 contains a value other than '01', '02', '03', '04', '05', or '06',  
**or** P2 contains a value other than '00',  
**then** a response of '6A86' SHALL be returned.
- If** the PPSE does not support handling for when the device is not Switched On,  
**and** P1 of the GET TEMPLATE command contains a value of '02',  
**then** a response of '6A86' SHOULD be returned.
- R3.7.2 **If** a PUT TEMPLATE command is received over the antenna interface,  
**then** a response of '6985' SHALL be returned.
- R3.7.3 **If** the PPSE is not currently configured to operate in [External Mode],  
**then** a response of '6985' SHALL be returned.
- R3.7.4 **If** the template received in the command data is not formatted as per Table 3-9,  
**then** a response of '6984' SHALL be returned.
- R3.7.5 **If** P1 contains a value of '01' [Device Switched On no override],  
**then** the received command data SHALL become the FCI Proprietary Template for the FCI that would be returned (as a response to the SELECT command over the antenna interface) when no override is currently set.
- Note, that in the case that the PPSE supports handling for when the device is not Switched On, the FCI that would be returned (as a response to the SELECT command over the antenna interface) may contain a different value (see R3.7.7).*
- R3.7.6 **If** P1 contains a value of '02' [Device not Switched On],  
**and** the PPSE is not capable of determining (or does not implement functionality to determine) whether the device is Switched On or not,  
**then** a response of '6985' SHOULD be returned.
-

---

### R3.7: PUT TEMPLATE Command

---

- R3.7.7 **If** P1 contains a value of '02' [Device not Switched On]  
**and** the PPSE is capable of determining whether the device is  
Switched On or not,  
**then** the received command data MAY become the FCI Proprietary  
Template for the FCI that would be returned (as a response to the  
SELECT command over the antenna interface) when the device is  
not Switched On.
- R3.7.8 **If** P1 contains a value of '03' [Override until cancelled],  
**then** the received command data SHALL become the FCI  
Proprietary Template for the FCI that would be returned (as a  
response to the SELECT command over the antenna interface). *This  
FCI is returned over the antenna interface until the override is  
cancelled.*
- Note, that in the case that the PPSE supports handling for when  
the device is not Switched On, the FCI that would be returned (as a  
response to the SELECT command over the antenna interface) may  
contain a different value (see R3.7.7).*
- R3.7.9 **If** P1 contains a value of '04' [Cancel override],  
**then** the current override, if any, SHALL be disabled.
- R3.7.10 **If** P1 contains a value of '05' [Mandatory data only],  
**then** only the DF Name within the FCI Template (see Table 3-4)  
SHALL be returned (as a response to the SELECT command over the  
antenna interface).
- R3.7.11 **If** P1 contains a value of '06' [Hide],  
**then** the PPSE SHALL behave as if it were not present.
- R3.7.12 **If** command data contains an FCI Proprietary Template,  
**then** the length field of the newly constructed FCI Template (tag  
'6F') SHALL reflect the length of the data received in the command  
message in addition to the length of the PPSE's DF Name data  
object.
-

### 3.3.3 Response Data

The response Status Word may contain one of the values shown in Table 3-10.

**Table 3-10: PUT TEMPLATE Command Responses**

| Field | Length | Value       |        |                                 |
|-------|--------|-------------|--------|---------------------------------|
| SW    | 2      | Status Word |        |                                 |
|       |        | Value       | Type   | Meaning                         |
|       |        | '6984'      | Error  | Data invalid                    |
|       |        | '6985'      | Error  | Conditions of use not satisfied |
|       |        | '6A86'      | Error  | Incorrect P1/P2                 |
|       |        | '9000'      | Normal | Successful processing           |

## 3.4 GET TEMPLATE Command

The GET TEMPLATE command enables the Payment Card Manager to retrieve the current FCI settings within the PPSE; that is, the same response data that would be returned in response to a SELECT command over the antenna interface.

The support of the GET TEMPLATE command is mandatory, regardless of the PPSE configuration mode.

### 3.4.1 Command Data

Table 3-11: GET TEMPLATE Command Message

| Code | Value                    |
|------|--------------------------|
| CLA  | '80' – '83', 'C0' – 'CF' |
| INS  | 'D4'                     |
| P1   | Usage; see Table 3-12    |
| P2   | '00'                     |
| Lc   | '00'                     |
| Le   | Absent                   |

#### Usage (P1)

This parameter indicates which of the possible FCI records present in the PPSE is to be returned.

Table 3-12: GET TEMPLATE Command P1 Usage

| Code | Meaning                           |
|------|-----------------------------------|
| '01' | Device Switched On no override    |
| '02' | Device not Switched On (optional) |
| '03' | Override until cancelled          |
| '04' | Device                            |

The response to the GET TEMPLATE command is dependent on the parameter set in P1, as defined in the following requirements.

### 3.4.2 Functional Requirements

---

#### R3.8: GET TEMPLATE Command

---

- R3.8.1 **If P1 contains a value other than '01', '02', '03', or '04',  
or P2 contains a value other than '00',  
then a response of '6A86' SHALL be returned.**  
**If the PPSE does not support handling for when the device is not  
Switched On,  
and P1 of the GET TEMPLATE command contains a value of '02',  
then a response of '6A86' SHOULD be returned.**
- R3.8.2 **If the GET TEMPLATE command is received over the antenna  
interface,  
then a response of '6985' SHALL be returned.**
- R3.8.3 **If P1 contains a value of '01' [Device Switched On and no override],  
then the response command data SHALL contain the FCI that  
would be returned (as a response to the SELECT command over the  
antenna interface) when the device is Switched On, whether or  
not there is a current override FCI.**
- R3.8.4 **If P1 contains a value of '02' [Device not Switched On],  
then the response command data SHOULD contain the FCI that  
would be returned (as a response to the SELECT command over the  
antenna interface) when the device is not Switched On.**
- R3.8.5 **If P1 contains a value of '03' [Override until cancelled],  
but no current override response is available,  
then the response command data SHALL contain an FCI without an  
FCI Proprietary Template (see Table 3-4).**
- R3.8.6 **If P1 contains a value of '03' [Override until cancelled],  
and a current override response is available,  
then the response command data SHALL contain the same FCI that  
would be returned (as a response to the SELECT command over the  
antenna interface) when the device is Switched On.**
-

---

### R3.8: GET TEMPLATE Command

---

R3.8.7 If P1 contains a value of '04' [Device],  
then the response command data SHALL contain the FCI that  
would be returned as a response to the SELECT command over the  
device interface.<sup>7</sup>

---

### 3.4.3 Response Data

Depending on the value of P1 the response command data is formatted as defined in Table 3-4 or Table 3-5.

The response Status Word may contain one of the values shown in Table 3-13.

**Table 3-13: GET TEMPLATE Command Responses**

| Field | Length | Value        |             |                                 |
|-------|--------|--------------|-------------|---------------------------------|
| SW    | 2      | Status Word  |             |                                 |
|       |        | <b>Value</b> | <b>Type</b> | <b>Meaning</b>                  |
|       |        | '6A86'       | Error       | Incorrect P1/P2                 |
|       |        | '6985'       | Error       | Conditions of use not satisfied |
|       |        | '9000'       | Normal      | Successful processing           |

---

<sup>7</sup> This functionality is provided specifically for Mobile Device implementations where the response to the SELECT command is not provided back to the entity selecting the application.

## 3.5 SET MODE Command

The SET MODE command provides a means for an application on the Mobile Device (a Payment Card Manager) to set the mode (External Mode, Internal Mode, or Internal Mode with Mutual Exclusivity Rule) of the PPSE.

### 3.5.1 Command Data

**Table 3-14: SET MODE Command Message**

| Code | Value                    |
|------|--------------------------|
| CLA  | '80' – '83', 'C0' – 'CF' |
| INS  | 'D6'                     |
| P1   | Mode – see Table 3-15    |
| P2   | '00'                     |
| Lc   | Absent                   |
| Le   | Absent                   |

#### Mode (P1)

This parameter indicates the mode of operation of the PPSE.

**Table 3-15: SET MODE Command P1 Mode**

| Code | Meaning                                    |
|------|--|
| '01' | External Mode                              |
| '02' | Internal Mode                              |
| '03' | Internal Mode with Mutual Exclusivity Rule |

### 3.5.2 Functional Requirements

---

#### R3.9: SET MODE Command

---

R3.9.1 **If P1 contains a value other than '01', '02' or '03', then a response of '6A86' SHALL be returned.**

---

R3.9.2 **If the SET MODE command is received over the antenna interface, then a response of '6985' SHALL be returned.**

---

---

### R3.9: SET MODE Command

---

- R3.9.3 **If P1 contains a value of '01' [External Mode],  
and External Mode is not supported by the implementation,  
then a response of '6985' SHALL be returned.**
- R3.9.4 **If P1 contains a value of '02' [Internal Mode],  
and Internal Mode is not supported by the implementation,  
then a response of '6985' SHALL be returned.**
- R3.9.5 **If P1 contains a value of '03' [Internal Mode with Mutual  
Exclusivity Rule],  
and Internal Mode with Mutual Exclusivity Rule is not supported  
by the implementation,  
then a response of '6985' SHALL be returned.**
- R3.9.6 **If P1 contains a value of '01' [External Mode],  
then any current FCI Templates SHALL be reset.**
- R3.9.7 **If P1 contains a value of '03' [Internal Mode with Mutual  
Exclusivity Rule],  
then the PPSE SHALL deactivate all Payment Applications or  
Application Groups that it is aware of.**
- R3.9.8 **If P1 contains a value of '02' [Internal Mode]  
or '03' [Internal Mode with Mutual Exclusivity Rule],  
then the PPSE SHALL rebuild the FCI with the Directory Entry  
information of all its active contactless application(s).**
- See the Functional Behaviour description in Section 3.6.1 for  
further details about how to build the FCI.*
-

### 3.5.3 Response Data

The response Status Word may contain one of the values shown in Table 3-16.

**Table 3-16: SET MODE Command Responses**

| Field | Length | Value       |        |                                 |
|-------|--------|-------------|--------|---------------------------------|
| SW    | 2      | Status Word |        |                                 |
|       |        | Value       | Type   | Meaning                         |
|       |        | '6A86'      | Error  | Incorrect P1/P2                 |
|       |        | '6985'      | Error  | Conditions of use not satisfied |
|       |        | '9000'      | Normal | Successful processing           |

## 3.6 Internal Mode(s) Processing

This section details the manner in which a PPSE configured for Internal Mode or for Internal Mode with Mutual Exclusivity Rule makes use of the CRS API. Unless otherwise specified, all references apply to both modes.

A PPSE capable of being configured for either internal modes must be configured as a CREL application. The `notifyCLEvent()` method provides a means for the GlobalPlatform OPEN to inform a CREL (in this case the PPSE) of contactless state changes to the contactless applications that have identified the PPSE as their CREL application. This method must be implemented by a PPSE supporting both internal modes.

---

### R3.10: General for Internal Modes

---

R3.10.1 The PPSE SHALL expose the `CRELApplication` interface and implement the method `notifyCLEvent()`.

---

R3.10.2 On invocation of the `notifyCLEvent()`,  
**if** the PPSE Application is not currently active over the antenna interface,  
**then** the PPSE application SHALL become active over the antenna interface.

---

Note that for proper functioning of the PPSE (configured for either internal modes), contactless applications intended to be presented in the PPSE FCI (i.e. all Payment Applications and possibly other contactless applications such as loyalty) must have their contactless parameters set adequately in the GlobalPlatform Contactless Registry.

This includes:

- Declaring the PPSE AID as a CREL.
- Populating the `INFO_DISCRETIONARY_DATA` with the data elements necessary for the expected processing of the PPSE as specified in this section.

See Annex A for further details regarding the setting of an application's contactless parameters.

### 3.6.1 FCI Building Rules

A PPSE may support functionality to build up to three FCI values:

- Device Switched On no override – This FCI is always supported.
- Device not Switched On – This FCI may be supported by the PPSE if the platform allows the PPSE to determine whether the device is Switched On. This determination is achieved by checking whether the device's user interface is currently available or not (see `getHostDeviceUserInterfaceState()`).
- Override until cancelled – This FCI should be supported if the platform is able to notify the PPSE that a volatile priority change event has occurred. Such events and notifications are available on Secure Elements supporting [GPCARD C] version 1.1 and 1.2<sup>8</sup>.

---

#### R3.11: FCI Building Rules

---

R3.11.1 The PPSE SHALL maintain an FCI [Device Switched On no override] presenting all active applications.

This FCI SHALL be returned when the Mobile Device is Switched On and when no Payment Application currently has the Volatile Priority.

*This FCI MAY also be returned when the Mobile Device is not Switched On.*

---

<sup>8</sup> The use of volatile priority is deprecated by GlobalPlatform.

---

### R3.11: FCI Building Rules

---

R3.11.2 If the PPSE is capable of determining whether the Mobile Device is Switched On,  
**then** the PPSE SHOULD maintain a separate FCI [Device Not Switched On] excluding active applications that require that the Mobile Device be Switched On to process a contactless payment transaction.

This FCI MAY be returned when the PPSE detects that the Mobile Device is not Switched On.

*The indication of whether to include/exclude a Payment Application in this FCI can be retrieved from the INFO\_DISPLAY\_REQUIREMENT of the application's GPCLRegistryEntry.*

- *A value of zero indicates that the Directory Entry should not be populated to this FCI and is only populated to the FCI to be returned when the Mobile Device is Switched On.*
- *A value other than zero indicates that the Directory Entry should be populated to both this FCI and may be populated to the FCI to be returned when the Mobile Device is Switched On.*

---

R3.11.3 When creating or updating the FCI value(s), the PPSE SHALL retrieve the Directory Entry (or Entries) information of applications for which it is a CREL from the INFO\_DISCRETIONARY\_DATA of each active application's GPCLRegistryEntry.

GPCLRegistryEntry objects SHALL be considered in the order as returned by the method `getNextGPCLRegistryEntry()` so as to take into account each application's prioritisation order as described in sections 4.2 and 4.3.

---

R3.11.4 Application Priority Indicator:

For each retrieved Directory Entry, the PPSE SHALL include a Priority TLV in the Directory Entry.

If there are multiple Directory Entries retrieved,  
**then** the first entry from the first returned GPCLRegistryEntry SHALL be given the highest priority '01' and each successive entry (first from the same GPCLRegistryEntry, if any, and then from the subsequent GPCLRegistryEntry, if any) SHALL be given a continually lesser priority.

---

### R3.11: FCI Building Rules

---

#### R3.11.5 Length of Base AID:

For each retrieved Directory Entry that contains a Length of Base AID data object, the PPSE SHALL check whether any other of the previously retrieved Directory Entries (that is, with a higher priority) contains a matching AID. This match is based on a byte-by-byte comparison starting from the left most byte of the AID up to the value of the Length of Base AID.

If there is at least one match among the Directory Entries with a higher priority than the current Directory Entry,  
then the current Directory Entry SHALL be stripped from the template<sup>9</sup>.

Following this check,  
if the current Directory Entry has not been stripped from the template,  
then the Length of Base AID data object (tag, length and value) SHALL itself be stripped from this Directory Entry.

---

#### R3.11.6 Apart from the behaviour described in the two preceding requirements (for inclusion of the Application Priority Indicator data objects and removal of the Length of Base AID data objects), and allowing for a possible overflow as described in the following requirement, all retrieved Directory Entry data objects SHALL be present in Directory Entries populated to the FCI Proprietary Template.

---

#### R3.11.7 The PPSE SHALL be able to present a minimum of 8 Directory Entries to the contactless reader.

If the concatenated Directory Entries result in more than 229 bytes,  
and thus cannot fit into a single R-APDU,  
then the PPSE SHALL remove from the list of entries those that cause the overflow, starting from those with the least highest priority indicator.

---

<sup>9</sup> The rationale for the base AID is that a contactless payment terminal will only interact with the highest priority application even if multiple applications with the same base AID are listed by the PPSE. Therefore, as an optimization of the PPSE, any lower priority application indicating a Length of Base AID, and matching one or more other applications to be listed, can be removed from the list.

---

### R3.11: FCI Building Rules

---

R3.11.8 ~~(Deprecated) If the platform is able to send priority change notifications to the PPSE, and an application is assigned temporarily the Volatile Priority, then the PPSE SHALL build a separate FCI [Override Until Cancelled].~~

~~This FCI SHALL be returned when the Mobile Device is Switched On (or when the PPSE is not capable of determining if the Mobile Device is Switched On) until the relevant application is no longer assigned the Volatile Priority.~~

~~This FCI is based on the following information, in this order:~~

- ~~1. Volatile Part: The INFO\_DISCRETIONARY\_DATA of the application receiving the Volatile Priority. Note that it may contain several Directory Entries if this application is an Application Group Head and may be in the activated or deactivated state.~~
- ~~2. Persistent Part: The INFO\_DISCRETIONARY\_DATA of the active contactless applications.~~

~~For both the volatile and persistent parts see requirements R3.11.3 to R3.11.6 above for details on how to build this FCI with the following caveats:~~

- ~~• For the volatile part, the activated/deactivated state is not taken into account.~~
- ~~• If the application being granted the Volatile Priority is a Payment Application, then all Payment Application Directory Entries must be excluded from Persistent Part. Applications having an Application Family Identifier (INFO\_FAMILY\_IDENTIFIER) with a value of '20' or Applications without an Application Family Identifier are considered to be Payment Applications. Applications with an Application Family Identifier with a value other than '20' are considered to be non-Payment Applications.~~

### 3.6.2 Event Processing Rules

#### R3.12: Event Processing

- R3.12.1 On receipt of a notification that the contactless state of a Payment Application has been set to ACTIVATED, the PPSE SHALL rebuild the FCI [Device Switched On no override] as described in section 3.6.1. *The PPSE MAY rebuild the FCI [Device Not Switched On], if applicable.*

*This notification is the notifyCLEvent( ) indicating the affected target application with an event parameter of EVENT\_ACTIVATED.*

- R3.12.2 **If** the PPSE is configured for [Internal Mode with Mutual Exclusivity Rule],  
**then** on receipt of a notification that the contactless state of an application has been set to ACTIVATED, the PPSE SHALL deactivate the Payment Application (or Application Group) that is currently activated, if any.

Applications having an Application Family Identifier (INFO\_FAMILY\_IDENTIFIER) with a value of '20' or applications without an Application Family Identifier are considered to be Payment Applications and SHALL be deactivated. Applications with an Application Family Identifier with a value other than '20' are considered to be non-Payment Applications and SHALL not be deactivated.

- R3.12.3 On receipt of a notification that a previously activated application is no longer activated, the PPSE SHALL rebuild the FCI [Device Switched On no override] as described in section 3.6.1.  
*The PPSE MAY rebuild the FCI [Device Not Switched On], if applicable.*

*This notification is the notifyCLEvent( ) with a parameter of EVENT\_CREL\_REMOVED, EVENT\_DEACTIVATED, EVENT\_DELETED, EVENT\_GROUP\_MEMBER\_REMOVED, EVENT\_LOCKED, or EVENT\_NON\_ACTIVATABLE.*

If this notification results in no directory entries being present in the FCI, the PPSE SHALL behave as if it were not present.

---

### R3.12: Event Processing

---

- R3.12.4 On receipt of a notification that an activated application has been assigned the highest or lowest selection priority, the PPSE SHALL rebuild the FCI [Device Switched On no override], as described in section 3.6.1. *The PPSE MAY rebuild the FCI [Device Not Switched On], if applicable.*

*This notification would be the notifyCLEvent( ) with a parameter of EVENT\_SELECTION\_PRIORITY\_HIGHEST, or EVENT\_SELECTION\_PRIORITY\_LOWEST. This notification, supporting these parameters, is available on Secure Elements supporting [GPCARD C] from version 1.1.*

- R3.12.5 **(Deprecated)** ~~On receipt of a notification that an application in state ACTIVATED or DEACTIVATED has been assigned the Volatile Priority, the PPSE SHALL build the FCI [Override Until Cancelled] as described in section 3.6.1.~~

~~This notification would be the notifyCLEvent( ) with a parameter of EVENT\_VOLATILE\_SELECTION\_PRIORITY\_SET. This notification is available on Secure Elements supporting [GPCARD C] version 1.1 and 1.2.~~

- R3.12.6 **(Deprecated)** ~~On receipt of a notification that the Volatile Priority has been reset for an application, the PPSE SHALL erase/invalidate the FCI [Override Until Cancelled].~~

~~This notification would be the notifyCLEvent( ) with a parameter of EVENT\_VOLATILE\_SELECTION\_PRIORITY\_RESET. This notification is available on Secure Elements supporting [GPCARD C] version 1.1 and 1.2.~~

- R3.12.6 **(Deprecated)** ~~[GPCARD C] specifies that the Volatile Priority is discarded when the Secure Element is reset or powered on.~~

~~Upon detection that the card has been reset or powered on, the PPSE SHALL erase/invalidate the FCI [Override Until Cancelled], if present.~~

---

---

### R3.12: Event Processing

---

R3.12.7 On receipt of a notification that the Application Discretionary Data of an active application has changed, the PPSE SHALL rebuild the applicable FCIs.

*This notification would be the notifyCLEvent( ) with a parameter of EVENT\_DISCRETIONARY\_DATA.*

---

## 3.6.3 Conditions of Use for Internal Modes

### Secure Elements supporting [GPCARD C] version 1.0.1

On earlier platforms, CREL applications are not notified of changes in selection priority, thus there is no mechanism in for the PPSE to reliably determine the relative priorities when multiple Payment Applications (or Application Groups) are active at one time.

The use of Internal Mode must be limited to systems where the selection priority of Payment Applications does not affect the behaviour when Payment Application selection by a Merchant Terminal occurs. This implies that only a single Payment Application (or Application Group) be active at one time. The system design must ensure that this is the case, for example, by relying on the Payment Card Manager to correctly activate and deactivate applications, or by configuring the PPSE for Internal Mode with Mutual Exclusivity Rule.

For deployments supporting the prioritisation of multiple Payment Applications (or Application Groups) active at one time, the PPSE must be used in External Mode, with the Payment Card Manager explicitly configuring the FCI response of the PPSE and the priorities of applications therein.

### Secure Elements supporting [GPCARD C] version 1.1 and above

On such platforms, CREL applications are notified of changes in selection priority, and as such, the restriction mentioned for [GPCARD C] Version 1.0.1 above does not apply. The PPSE configured for either internal mode can trigger a refresh and reorder of priorities in its FCI responses when it receives a notification of a priority change for a Payment Application for which it is a CREL.

### 3.6.4 Management of non-payment applications

Unless otherwise specified in the requirements, the PPSE configured in either of the internal modes should consider any contactless application for which it is a CREL as a Payment Application, regardless of the presence or value of the Application Family Identifier in the CRS parameters of this application. Note that the Application Family Identifier is an optional parameter for contactless applications, including for Payment Applications (see Table A-2).

If, for proprietary reasons, the PPSE working in either internal modes adopts a different behaviour from the above recommendation, the following rules apply:

- Contactless applications without Application Family Identifier, or having an Application Family Identifier with value '20', are considered to be Payment Applications and shall be managed by the PPSE as specified in this section.
- The manner in which the PPSE manages contactless applications with Application Family Identifiers other than the value '20' is out of scope of this specification. These applications may be managed by the PPSE as specified in this section.

## 4 Secure Element Requirements

Regardless of whether it hosts a PPSE application or not, a Secure Element aimed at hosting one or more Payment Applications must be designed and configured to support the management of these Payment Applications by the Payment Card Manager, that is:

- Enabling contactless activation and deactivation of contactless applications
- Potentially (depending on the version of [GPCARD C]) enabling selection priority and override priority changes
- When the Secure Element hosts a PPSE application configured for either internal modes, notifying the PPSE application of the changes applied to Payment Applications
- Optionally, providing information about the Payment Application to the Payment Card Manager

Note that a Secure Element supporting [GPCARD C] is expected to comply with the requirements expressed in this section.

### 4.1 Activating/Deactivating Payment Applications

To reflect the consumer's choice of Payment Card(s), the Payment Card Manager shall be able to change the availability state of the PPSE application and Payment Applications on the antenna interface in the Secure Element.

---

#### R4.1: Secure Element Requirements – Activating/Deactivating contactless applications

---

R4.1.1 A Secure Element SHALL provide at least one of the following means for Payment Card Managers to activate contactless applications on the antenna interface:

- A GlobalPlatform CRS application supporting the SET STATUS command as per [GPCARD C] section 3.11
- A CRS application supporting a proprietary APDU for activation
- The CRS application accepting self-activation requests (see [GPCARD C] section 3.9.1) from Payment Applications that support the alternate activation mechanism described in Annex B
- The support of Contactless Self-Activation Privilege (as per [GPCARD C] section 7.2) for Payment Applications using the alternate activation mechanism described in Annex B

---

#### R4.1: Secure Element Requirements – Activating/Deactivating contactless applications

---

R4.1.2 A Secure Element SHALL provide at least one of the following means for Payment Card Managers to deactivate contactless applications on the antenna interface:

- A GlobalPlatform CRS application supporting the SET STATUS command as per [GPCARD C] section 3.11
  - A CRS application supporting a proprietary APDU for deactivation
  - The platform accepting self-deactivation requests from Payment Applications that support the alternate activation mechanism described in Annex B
- 

R4.1.3 A Secure Element SHALL support Application Groups as per [GPCARD C] section 3.7.

*This allows the activation/deactivation of the full Application Group upon explicit activation/deactivation of the head application only.*

---

## 4.2 Managing Priorities

Some Payment Card Managers may enable the consumer to activate several Payment Cards simultaneously. When this is the case, the consumer is offered the possibility to modify the priority order of these Payment Cards.

This activation and prioritisation of multiple Payment Cards requires that the Secure Element provide an interface that will enable the management of priorities of the Payment Applications hosted in the Secure Element.

---

#### R4.2: Secure Element Requirements – Managing Priorities

---

R4.2.1 A Secure Element that enables multiple Payment Applications (or Application Groups) to be active simultaneously SHALL provide at least one of the following means for Payment Card Managers to change the selection priority of Payment Applications (see [GPCARD C] section 6.2):

- A GlobalPlatform CRS application supporting the SET STATUS command as per [GPCARD C] section 3.11
  - A CRS application supporting a proprietary APDU for prioritizing applications
- 

### 4.3 PPSE receipt of events (internal modes only)

When the PPSE application is configured for either internal modes, it will have been declared as the CREL application for Payment Applications as described in Annex A.1. On receipt of contactless events, the PPSE retrieves information from the CRS in order to update its FCI template values.

The Secure Element is therefore expected to:

- broadcast contactless related events associated to Payment Applications to the PPSE application.
- allow the PPSE application to access the registry information of Payment Applications.

---

#### R4.3: Secure Element Requirements – Informing the PPSE

---

R4.3.1 A Secure Element SHALL support the CREL notification mechanism described in [GPCARD C] section 3.10.2

---

---

#### R4.3: Secure Element Requirements – Informing the PPSE

---

R4.3.2 A Secure Element SHOULD support at a minimum GlobalPlatform contactless API v1.2 (*[GPCARD C]* v1.1) so as to propagate the following events to CREL applications:

- EVENT\_SELECTION\_PRIORITY\_HIGHEST
- EVENT\_SELECTION\_PRIORITY\_LOWEST

*Note that if these events are not supported, the PPSE cannot handle the simultaneous activation of multiple Payment Applications (or Application Groups). When this is the case, the PPSE should be configured for Internal Mode with Mutual Exclusivity Rule.*

---

R4.3.3 A Secure Element SHALL allow CREL applications to retrieve the registry entry of each application (that declared it as a CREL) and the ability to read the content of the entry. See *[GPCARD C]* section 3.8.2

---

## 4.4 Informing the Payment Card Manager

To function correctly, a Payment Card Manager needs to be aware of certain information and contactless characteristics of the Payment Applications.

While it is expected that the Payment Card Manager can access this information through other methods (for instance, by connecting to a remote management server), this information may also be available from the Secure Element, either from the CRS application or in a proprietary manner from the Payment Applications directly.

When the Secure Element supports [GPCARD C] and hosts a GlobalPlatform CRS application (see [GPCARD C], section 3.11), Payment Card Managers can use the GET STATUS command of the GlobalPlatform CRS application to retrieve the GlobalPlatform Contactless Parameters of Payment Applications. Typically, the following contactless parameters can be retrieved for contactless applications:

- The AID of the application.
- Application Lifecycle State: Provides the contactless accessibility state of the application; that is, whether the application is immediately accessible over the antenna interface.
- Display Required Indicator: Whether it is intended for the contactless application to be accessible over the antenna interface when the Mobile Device is not Switched On<sup>10</sup>.
- Display Control Template: Whether the application is consumer facing; that is, whether a Payment Card Manager will present information regarding this contactless application to the consumer.<sup>11</sup>
- Application Discretionary Data: Contains the data that is intended to be populated to the PPSE when the Payment Application is accessible over the antenna interface; that is, the directory entry or directory entries necessary to build the PPSE FCI template.
- Selection Priority: The order in which Contactless Applications will be considered during partial selection over the antenna interface. This will also indicate the order of presentation of the Payment Application in the PPSE FCI template when the PPSE is operating in Internal Mode.
- Application Family Identifier: Identifies the family this application belongs to (See Table 12 of [ISO/IEC 14443]). A value of '20' identifies the financial family.
- Application Group Head, Application Group Membership List: if multiple contactless applications are bundled together as part of an overall Payment Card product and only one contactless application—the Application Group head—is consumer facing.
- List of declared CREL Applications. For Payment Applications, this should at least identify the PPSE.

Refer to [GPCARD C], section 3.11 for further details of the GET STATUS command.

As per the [GPCARD C], information and characteristics are provided to the Secure Element during the install or personalisation process of the contactless application. Refer to Annex A for more details on how to set these parameters for Payment Applications.

---

<sup>10</sup> The Payment Card Manager can use this information to indicate to the consumer which applications can only be used when the consumer's device is Switched On and which can be used when the device is not Switched On

<sup>11</sup> Contactless applications that are not consumer facing include the PPSE as well as contactless applications that are part of an Application Group of contactless applications but are not the Application Group head

## Annex A Parameter Setting for Payment Applications

To enable their successful management by the Secure Element, the Payment Card Manager, and the PPSE, Payment Applications hosted in a [GPCARD C] Secure Element must populate their GlobalPlatform Contactless Registry Entry appropriately.

Contactless parameters can be set:

- Either during installation of the Payment Application, through the System Specific Parameters of the INSTALL command
- Or during the personalisation of the Payment Application, using application-specific DGI(s) (Data Grouping Identifier)

Whether the contactless information and characteristics are provided during installation or personalisation is an implementation choice.

### A.1 Installation

Table A-1 defines the structure of the Contactless Protocol Parameters that must be present in the System Specific Parameters of the INSTALL command.

**Table A-1: Contactless Protocol Parameters – Installation**

| Content |      |                                 |  | Presence        |
|---------|------|---------------------------------|--|-----------------|
| 'A0'    | 'OE' | Contactless Protocol Parameters |  | Mandatory       |
|         | 'A2' | '0C'                            | Contactless Protocol Parameter Profile | Mandatory       |
|         |      | 'A0' '04' '80' '04' '3230'      |  | Protocol Type A |
|         |      | 'A1' '04' '80' '04' '3230'      |  | Protocol Type B |

As the Contactless Protocol Parameters reference a profile, it is assumed that this profile '3230' ("20") has already been predefined in the Secure Element to support [Book D] Type A and Type B. A Contactless Protocol Parameter Profile cannot be personalised; therefore it must be provided during installation. See [GPCARD C] for further details regarding the Contactless Protocol Parameters Profile.

Table A-2 defines the structure of the User Interaction Parameters that may be present in the System Specific Parameters of the INSTALL command. If these parameters are not present in the INSTALL command, they should be personalised to the application as described in Annex A.2 below.

**Table A-2: User Interaction Parameters – Installation**

| Content |        |  |   | Presence  |
|---------|--------|--|---|---|
| 'A1'    | '##'   | User Interaction Parameters                  |   | Mandatory   |
| 'A1'    | '88'   | '01'   | 'xx'  | Display Required Indicator                                    |
|         | '87'   | '01'   | '20'  | Application Family Identifier                                 |
|         | '7F20' | '##'   | Display Control Template                    |   |
|         | 'A0'   | '##'   | Application Group head                      |   |
|         |        | '4F' '##' 'xx...xx'                          |   | Group head AID  |
|         | 'A1'   | '##'   | Add to Application Group Authorization List |   |
|         |        | '4F' '##' 'xx...xx'                          |   | Group member's AID  |
|         |        | ...  |   |   |
|         |        | '4F' '##' 'xx...xx'                          |   | Group member's AID  |
| 'A3'    | '10'   | Add to CREL Application AID List             |   |   |
|         |        | '4F' '0E'<br>'325041592E5359532E4444463031'  |   | AID of<br>PPSE  |
| 'A6'    | '##'   | Application Discretionary Data <sup>14</sup> |   |   |
|         |        | 'BF0C'                                       | '##'  | FCI Data  |
|         |        |  | '61'  | '##' Directory Entry  |
|         |        |  |   | '4F' '##'<br>'xx...xx'  |
|         |        |  |   | ADF Name  |
|         |        |  |   | Optional  |
|         |        |  |   | '9F2A' '##'<br>'xx...xx'                                      |
|         |        |  |   | Kernel<br>Identifier as<br>per<br>[ENTRY].                    |
|         |        |  |   | '9F0A' '##'<br>'xx...xx'                                      |
|         |        |  |   | Application<br>Selection<br>Registered<br>Proprietary<br>Data |
|         |        |  |   | Optional  |

<sup>12</sup> Required if this application is a member of an Application Group. Mutually exclusive with 'A1'.

<sup>13</sup> Required if this application is an Application Group head. Mutually exclusive with 'A0'.

<sup>14</sup> Contains the data that must be populated to the PPSE when the Payment Application is to be accessible over the antenna interface; that is, the directory entry or directory entries necessary to build the FCI.

| Content |                          |   | Presence    |
|---------|--------------------------|---|-------------|
|         | '81' '01' 'xx'           | Length of base AID <sup>15</sup>                  | Optional    |
| ...     |                          |   |             |
| ...     |                          |   |             |
| '61'    | '##'                     | Directory Entry                                   | Conditional |
|         | '4F' '##'<br>'xx...xx'   | ADF Name  | Mandatory   |
|         | '9F2A' '##'<br>'xx...xx' | Kernel Identifier                                 | Optional    |
|         | '9F0A' '##'<br>'xx...xx' | Application Selection Registered Proprietary Data | Optional    |
|         | '81' '01' 'xx'           | Length of base AID                                | Optional    |
| ...     |                          |   |             |
| ...     |                          |   |             |

Note: Because the PPSE is not a Payment Application and is not a consumer-facing application, there are no User Interaction Parameters provided during its installation.

---

<sup>15</sup> If present, this indicates that this directory entry must be removed if a higher priority application being presented by the PPSE has the same base AID. Refer to Requirement R3.11.5 for details about the Length of base AID processing.

## A.2 Personalisation

If the User Interaction Parameters described in Table A-2 are provided to the Payment Application during personalisation, the application must populate its `GPCLRegistryEntry` within the CRS in the following manner:

Extract the following information from the buffer containing the personalised data, and set each by invoking the `setInfo( )` method.

- The Application Discretionary Data (tag 'A6') with an `info` parameter of `INFO_DISCRETIONARY_DATA`.
- The Display Required Indicator (tag '88') with an `info` parameter of `INFO_DISPLAY_REQUIREMENT`.
- The Application Family Identifier (tag '87') with an `info` parameter of `INFO_FAMILY_IDENTIFIER`.

If this application is intended to be a member of an Application Group, extract the AID of the intended Application Group head (tag 'A0') and provide it as a parameter on the invocation of the `joinGroup( )` method.

If this application is an Application Group head, extract the AID of each Application Group member (tag 'A1') and provide each separately as a parameter on the invocation of the `addToGroupAuthorizationList( )` method.

Extract the AID of the PPSE and other CREL applications, if any (tag 'A3'), and for each AID provide it as a parameter on the invocation of the `addToCRELApplicationList( )` method.

## Annex B Alternative Activation Mechanism through the Payment Application – SET STATUS command

This annex details an alternative command to the CRS application's SET STATUS command for managing application activation. This command is intended for [GPCARD C] Secure Elements where the CRS application is not available to the Payment Card Manager and it is therefore necessary to manage the state of contactless applications through the Payment Applications themselves. The ability of an application to support this command depends on the platform configuration on which the application is being hosted, and any necessary privileges. Note that this annex assumes that the platform complies with [GPCARD C].

The following SET STATUS command may be supported by a Payment Application. If supported, it enables a Payment Card Manager to indicate a contactless state change to the contactless application itself. EMVCo does not require that Payment Applications support this command; refer to individual Payment System specifications to determine if a specific Payment Application supports it.

### B.1 Command Data

Table B-1: SET STATUS Command Message

| Code | Value  |
|------|--|
| CLA  | '80' – '8F', 'C0' – 'CF', 'E0' – 'EF'                                      |
| INS  | 'F0'   |
| P1   | '01' – Availability State [over the antenna interface]                     |
|      | '02' – Activate and Set Priority [for application selection] <sup>16</sup> |
| P2   | State  |
| Lc   | 'xx' <sup>17</sup>   |
| Data | Command Template <sup>17</sup>   |
| Le   | '00' <sup>17</sup>   |

<sup>16</sup> The use of volatile priority is deprecated by both GlobalPlatform and EMVCo. Actual support by Payment Applications is at the discretion of each Payment System specification for their Payment Application.

<sup>17</sup> Presence and actual value for Lc, Command Data and Le is at the discretion of each Payment System specification for their Payment Application.

## State (P2)

If P1 has a value of '01' [Availability State], this parameter indicates the availability state of this contactless application over the antenna interface, per Table B-2:

**Table B-2: SET STATUS Command P2 if P1 is '01'**

| Code | Meaning     |
|------|-------------|
| '00' | DEACTIVATED |
| '01' | ACTIVATED   |

If P1 has a value of '02' [Activate and Set Priority], this parameter is used to set the override priority of this application for a single imminent transaction or for future transactions. The override priority order is set/reset for this contactless application, per Table B-3:

**Table B-3: SET STATUS Command P2 if P1 is '02'**

| Code | Meaning                  |
|------|--------------------------|
| '02' | Assign Override Priority |
| '82' | Reset Override Priority  |

## Command Data

If present, the command data contains a Template that is either empty or contains application-specific TLV-coded data objects, such as an authentication TLV-coded data object.

## B.2 Functional Behaviour of the Environment

### Behaviour

If P1 contains a value of '01' [Availability State], then the following behaviour is expected:

- If P2 contains a value of '01' [ACTIVATED], this application should become active over the antenna interface.
- If P2 contains a value of '00' [DEACTIVATED], this application should become inactive over the antenna interface.

If P1 contains a value of '02' [Activate and Set Priority], then the following behaviour is expected<sup>18</sup>:

- If P2 contains a value of '02' [Assign Override Priority], this application should become active over the antenna interface and should be given the highest priority for the duration of the next contactless transaction. Following this transaction, this application should return to its previous state and priority.
- If P2 contains a value of '82' [Reset Override Priority] and this application is currently assigned the override priority (that is, no contactless transaction has occurred since the override priority was assigned), this application should return to its previous state and priority.

## B.3 Response Data

The presence of Response Data is optional. If present, the content of the Response Data is Payment Application specific.

The response Status Word may contain one of the values shown in Table B-4:

---

<sup>18</sup> The use of volatile priority is deprecated by both GlobalPlatform and EMVCo. Actual support of volatile priority by Payment Applications is at the discretion of each Payment System specification for their Payment Application.

**Table B-4: SET STATUS Command Responses**

| Field | Length | Value       |        |                                 |
|-------|--------|-------------|--------|---------------------------------|
| SW    | 2      | Status Word |        |                                 |
|       |        | Value       | Type   | Meaning                         |
|       |        | '6A86'      | Error  | Incorrect P1/P2                 |
|       |        | '6985'      | Error  | Conditions of use not satisfied |
|       |        | '6982'      | Error  | Security status not satisfied   |
|       |        | '6A81'      | Error  | Function not supported          |
|       |        | '6984'      | Error  | Application not activated       |
|       |        | '9000'      | Normal | Successful processing           |

## Annex C Requirements Mapping Table

Requirements expressed in this document are equivalent to the requirements and recommendations presented in [AAUI]; they integrate the modifications of the latest applicable Specification Update Bulletins and are presented slightly differently.

In order to ease the reading and the follow-up of test cases between both documents, the table below establishes a mapping between each requirement of this document and the corresponding requirement or section in [AAUI] or in related Specification Update Bulletins.

Note:

- The presence of the sign '\*' indicates that the requirement has been updated in this specification.
- The presence of the sign '‡' indicates that what was originally a requirement is now optional or recommended.
- Strikethrough indicates that the requirement is deprecated.

| <b><i>Requirement in this document</i></b> | <b><i>Equivalence in [AAUI] document or in Specification Update Bulletins</i></b> |
|--|---|
| R3.1.1                                     | -   |
| R3.1.2                                     | B.2.1.1   |
| R3.1.3                                     | SB166 Second Edition - Section 2  |
| R3.1.4                                     | B.2.1.2*  |
| R3.1.5                                     | B.2.1.3‡  |
| R3.1.6                                     | B.2.1.4*  |
| R3.2.1                                     | -   |
| R3.2.2                                     | B.3.1.1   |
| R3.2.3                                     | B.3.1.2   |
| R3.2.4                                     | B.3.1.3   |
| R3.2.5                                     | -   |
| R3.3.1                                     | B.3.2.4   |
| R3.3.2                                     | B.3.2.5   |
| R3.3.3                                     | B.3.2.6   |
| R3.3.4                                     | B.3.2.7   |
| R3.4.1‡                                    | B.3.2.8   |
| R3.4.2‡                                    | B.3.2.9   |

| <b>Requirement in this document</b> | <b>Equivalence in [AAUI] document or in Specification Update Bulletins</b> |
|-------------------------------------|--|
| R3.5.1                              | B.3.3.10   |
| R3.5.2                              | B.3.3.11*  |
| R3.5.3                              | B.3.3.11*  |
| R3.6.1 <sup>‡</sup>                 | B.3.3.12*  |
| R3.6.2 <sup>‡</sup>                 | B.3.3.13*  |
| R3.7.1                              | B.3.1.14*  |
| R3.7.2                              | B.3.1.15   |
| R3.7.3                              | B.3.1.16   |
| R3.7.4                              | B.3.1.17   |
| R3.7.5                              | B.3.1.18*  |
| R3.7.6 <sup>‡</sup>                 | B.3.1.19   |
| R3.7.7 <sup>‡</sup>                 | B.3.1.20   |
| R3.7.8                              | B.3.1.21*  |
| R3.7.9                              | B.3.1.22   |
| R3.7.10                             | B.3.1.23*  |
| R3.7.11                             | B.3.1.24   |
| R3.7.12                             | B.3.1.25   |
| R3.8.1                              | B.3.1.26*  |
| R3.8.2                              | B.3.1.27   |
| R3.8.3                              | B.3.1.28   |
| R3.8.4 <sup>‡</sup>                 | B.3.1.29   |
| R3.8.5                              | B.3.1.30   |
| R3.8.6                              | B.3.1.31   |
| R3.8.7                              | B.3.1.32   |
| R3.9.1                              | B.3.1.33*  |
| R3.9.2                              | B.3.1.34   |
| R3.9.3                              | B.3.1.35   |
| R3.9.4                              | B.3.1.36   |
| R3.9.5                              | -  |
| R3.9.6                              | SB166 Second Edition - Section 4   |

| <b>Requirement in this document</b> | <b>Equivalence in [AAUI] document or in Specification Update Bulletins</b> |
|-------------------------------------|--|
| R3.9.7                              | -  |
| R3.9.8                              | SB166 Second Edition - Section 4   |
| R3.10.1                             | Annex A.1.3 (second sentence)  |
| R3.11.1                             | -  |
| R3.11.2 <sup>#</sup>                | Annex A.1.3 (second bullet)*   |
| R3.11.3                             | SB119 Second Edition - Section 1*  |
| R3.11.4                             | SB119 Second Edition - Section 1*  |
| R3.11.5                             | A.1.2.2 / SB119 Second Edition - Section 2*                                |
| R3.11.6                             | Annex A.1.2.2 *  |
| R3.11.7                             | SB166 Second Edition - Section 8*  |
| <del>R3.11.8</del>                  | SB166 Second Edition - Section 3*  |
| R3.12.1                             | Annex A.1.3 (first bullet)*  |
| R3.12.2                             | -  |
| R3.12.3                             | Annex A.1.3 (third bullet)*  |
| R3.12.4                             | SB166 Second Edition - Section 3*  |
| <del>R3.12.5</del>                  | SB166 Second Edition - Section 3*  |
| <del>R3.12.6</del>                  | SB166 Second Edition - Section 3*  |
| R3.12.7                             | SB166 Second Edition - Section 3*  |
| R4.2.1                              | -  |
| R4.2.2                              | -  |
| R4.2.3                              | -  |
| R4.3.1                              | -  |
| R4.4.1                              | -  |
| R4.4.2                              | -  |
| R4.4.3                              | -  |