EMVCo
Contactless Mobile Payment

Application Activation User Interface

Overview, Usage Guidelines, and PPSE Requirements

Version 1.0
December 2010

EMVCo
Contactless Mobile Payment

Application Activation User Interface

Overview, Usage Guidelines, and PPSE Requirements

Version 1.0
December 2010

Contents

Figures

Tables

1 Scope

This document, *EMVCo Contactless Mobile Payment – Application Activation User Interface*:

- describes the components necessary to enable application activation from within an Application Activation User Interface (AAUI) application,
- provides usage guidelines for interacting with components outside the purview of EMVCo, and
- defines the requirements for PPSE behaviour on a Mobile Device.

That is, this document is intended to be the "glue" that connects the various components that make application activation possible, specifying the functionality of the AAUI, defining the interaction with the contactless applications and contactless management entities on the Secure Element and with the Contactless Module, and specifying the PPSE behaviour on the Mobile Device. This document does not detail the functionality of the contactlessef management services of a Secure Element or of the Contactless Module but rather just the interaction between the AAUI and those components.

One of the primary driving forces behind EMVCo decisions related to application management is to provide flexibility in implementations to meet the needs of particular markets. In certain markets, Contactless Payment Terminals may need to support the possibility of multiple contactless mobile payment applications across multiple Secure Elements being active over the antenna interface simultaneously. Other markets may not have the same requirement and may anticipate that only a single contactless mobile payment application on a single Secure Element will be active over the antenna interface at any one time. EMVCo in no way dictates that an implementation in a market allow for flexibility; rather, this choice is based on business decisions, the complexity of managing multiple contactless applications, and the functionality available on the Secure Element(s) hosting the contactless applications.

This document is based on current efforts underway in various standards organizations. As these standards are updated or when new standards are established that apply to this space, EMVCo will publish updated versions of this document.

1.1 Audience

This document is intended for use by entities designing, developing, and implementing a user interface application (for example, a wallet application), entities developing contactless applications, entities responsible for the provisioning of those applications, and entities responsible for the presence of the PPSE functionality on the Mobile Device; for example, handset manufacturers, mobile network operators, mobile application developers, smart card application developers, etc.

1.2 Document Structure

This document is split into the following main sections:

Chapter 1 contains general information that helps the reader understand and use this specification.

Chapter 2 lists related specifications and standards.

Chapter 3 defines new and possibly unfamiliar concepts that are used in this document, and describes conventions used.

Chapter 4 details the purpose of the AAUI and defines two typical use cases to give an example of the consumer experience.

Chapter 5 details the architecture of a Mobile Device that would facilitate an AAUI, and discusses information that should be accessible and possibly configurable by the AAUI.

Chapter 6 provides an overview of AAUI behaviour and the basic interactions between the AAUI and other components on the Mobile Device that facilitate application activation.

Chapter 7 is a more detailed high-level description of the interactions. At this level the document is agnostic as to the actual technologies used for the components (Low-level technical details are contained in Annex A.)

Chapter 8 defines best practices for an AAUI.

Annex A contains the low-level technical details of known components specified by external industry/standards bodies. As additional specifications become available that relate to the AAUI, and as EMVCo determines how such specifications may be used in conjunction with this specification, updated versions of this document will be released.

Annex B contains the low-level EMVCo technical requirements and details for a PPSE implementation on the Mobile Device. As there are potentially multiple options for how and where the PPSE is implemented, updated versions of this document may be released to address different implementations.

Annex C details an alternative for managing application activation when the SECM does not provide an interface that the AAUI can use and the state of contactless applications must be managed through the applications themselves.

Annex D is a glossary of terms and abbreviations used in this specification.

2 References

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

2.1 EMV Documents

EMV®* documents are available on the EMVCo website:

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

[ENTRY]	Contactless Specifications for Payment Systems: Entry Point Specification
[CCPS]	Contactless Specifications for Payment Systems: EMV Contactless Communication Protocol Specification
[ARCH]	Contactless Mobile Payment Architecture Overview

2.2 External References

[SWP]	ETSI TS 102 613: Smart Cards; UICC – Contactless Front-end (CLF) Interface; Part 1: Physical and data link layer characteristics
[GPCARD]	Contactless Services – GlobalPlatform Card Specification v2.2 – Amendment C
ISO/IEC 14443	Identification cards – Contactless integrated circuit(s) cards – Proximity cards
ISO/IEC 18092	Information technology – Telecommunications and information exchange between systems – Near Field Communication – Interface and Protocol (NFCIP-1)

* EMV is a registered trademark in the U.S. and other countries and an unregistered trademark elsewhere. The EMV trademark is owned by EMVCo.

3 Concepts, Notations, and Terminology

3.1 Concepts

This section explains new and possibly unfamiliar concepts that are used in this document. Additional terms and abbreviations are defined in Annex D, Glossary.

3.1.1 Switched On

Switched On describes a state where the Mobile Device is powered up and the user interface (screen, keyboard, etc.) is available for use.

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.

3.1.2 Group

A group is a set of contactless applications consisting of a group head/owner application and one or more member applications. From a consumer point of view, a group could be synonymous with a single product on their Mobile Device that gives them access to multiple contactless services. For example, a group could comprise payment, transit, access, loyalty, etc., 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, only the group head is consumer facing, and actions that affect the group head also affect all the group members.

3.1.3 Always On

Always On describes a state where a contactless application on a Mobile Device is accessible to a contactless terminal as long as the Mobile Device is capable of communicating over the antenna interface – possibly even when the Mobile Device is not Switched On. An application in this state can be equated to a regular contactless card in that the only action required from the consumer to initiate a contactless transaction is the presentment of the Mobile Device to the contactless terminal.

Conversely, if a contactless application is not in an Always On state, the consumer must invoke some action on their Mobile Device to make the application accessible prior to the presentment of the Mobile Device to the contactless terminal.

3.1.4 Mode (External and Internal)

The modes, external and internal, relate to the manner in which the PPSE receives and builds the information that will be provided to a contactless payment terminal.

When External Mode is being used, the AAUI provides the PPSE with the details of the active applications that will be presented to a contactless payment terminal.

When Internal Mode is being used, the PPSE itself will, internally to the Secure Element, collect the details of the active applications from the SECM and build the data to be presented to the contactless payment terminal.

In both Internal Mode and External Mode, the AAUI will interact with the SECM and set the state of the contactless application, based on the decisions of the consumer. However, in some implementations the SECM may allow an application to change its own contactless state, in which case a PPSE configured for Internal Mode could modify its data (to be presented to the contactless payment terminal) based on this application-initiated state change.

While External Mode is suitable for both single Secure Element and multiple Secure Element environments, Internal Mode can only be used when a single Secure Element is active. There is no interaction between Secure Elements that will allow a PPSE to be notified of a state change of an application on another Secure Element or that will allow a PPSE to determine the state of applications on other Secure Elements. Therefore, when multiple Secure Elements are to be simultaneously active, External Mode is the only mode possible.

3.2 Notations

'0' to '9' and 'A' to 'F'	16 hexadecimal characters
AND	Logical AND
*n*b, *nn*b, *nnn*b, ...	Binary values
xx	Any value

3.3 Terminology

SHALL	Denotes a mandatory requirement
SHOULD	Denotes a recommendation
MAY	Denotes an optional feature

4 Purpose and Use Cases

The main purpose of any AAUI is to allow the consumer to make choices as to:

- Which of the available contactless application(s) on their Mobile Device will be accessible over the antenna interface.
- The priority order of these accessible applications.

In addition, an AAUI may allow the consumer to specify different access and priority choices depending on the power state of the device when a contactless transaction is being performed.

This chapter describes use cases for two scenarios that could be provided by an AAUI:

- A single user interface application on the Mobile Device manages a single contactless application on a Secure Element.
- A wallet user interface application on the Mobile Device manages multiple contactless applications on all Secure Elements within the device.

Note: The screens used to depict these use cases are examples only. Please refer to Chapter 8, Best Practices, for more information on the “look and feel” of an AAUI.

4.1 Simple Application Management Use Case

In this example, a single user interface application (a payment product branded application) on the Mobile Device manages a single contactless application on a Secure Element. This simple use case describes a scenario where the consumer, about to make a contactless payment, launches a payment product branded user interface application on their phone and explicitly indicates that they wish to use that payment product to make the contactless payment. Once the consumer has completed this action they present their device to the Contactless Payment Terminal to process the contactless payment transaction.

The screens shown in Figure 4-1 illustrate the basic user interaction involved in this use case. Screen 1 depicts the available handset applications and the consumer's choice to launch their "Issuer Bank" application. Screen 2 depicts the menu available for the "Issuer Bank" application as the consumer chooses to make a payment. Following this choice, screen 3 is displayed and prompts the consumer to present their device to the Contactless Payment Terminal. Once the consumer presents the device, and following the payment processing, screen 4 will inform the consumer that the payment transaction has ended.

Figure 4-1: Use Case 1 Consumer Experience

4.2 Multiple Application Management Use Case

In this example, a wallet user interface application on the Mobile Device manages multiple contactless applications on all Secure Elements within the mobile device. While a wallet type user interface application could manage multiple aspects of the products therein (for example, transaction history, balance enquiry, online banking, etc.), this use case only describes the scenario where the AAUI manages the contactless aspects of the multiple contactless applications.

Unlike the simple use case described in section 4.1, in which there is an explicit consumer choice just prior to making a payment, the consumer does not use this application as part of a contactless transaction but rather uses it to set up their preferences for contactless transactions that will take place in the future. The wallet application is launched in order to set one or more contactless applications to be accessible over the antenna interface in advance of an actual transaction. Therefore the only explicit consumer choice at the time of making a payment transaction is the presentment of the Mobile Device to the contactless terminal. At this point the contactless terminal uses the information provided by the Mobile Device, which reflects the consumer's choices and prioritization, to determine whether one of its own supported terminal side applications will be used to perform a contactless transaction.

The screens shown in Figure 4-2 illustrate the basic user interaction involved in this use case.

Figure 4-2: Use Case 2 Consumer Experience

Screen 1 shows the previously configured consumer contactless application settings where the top three applications (“Trust Bank”, “Fly Airways Bank”, and “MTA Transit”) are accessible to a contactless terminal and available for making contactless transactions in the order listed. The “Trust Bank” application will always be used to make a contactless payment transaction if the payment terminal supports it. If the payment terminal does not support “Trust Bank” but supports “Fly Airways Bank”, then “Fly Airways Bank” will be used. If the terminal is not a payment terminal but a transit terminal that supports neither “Trust Bank” nor “Fly Airways Bank”, then “MTA Transit” will be used.

The fourth application (“Issuer Bank”, which is also a payment application) is present on the Mobile Device but is not currently accessible over the antenna interface and will not be used to make a contactless transaction.

However, the consumer has highlighted “Issuer Bank” and on screen 2 the consumer is presented with the option of setting this account to “Always On” [1] (which gives it the same antenna interface accessibility status as the accounts above).

On screen 3, the consumer is informed that making this choice has created a conflict[2] in that “Issuer Bank” and “Trust Bank” are not permitted to be simultaneously accessible over the antenna interface. A potential reason for this conflict could be that these two products, while issued by different banks, are the same payment brand and it is not possible for both products to be simultaneously accessible.[3]

In screen 4, the consumer has chosen to accept this restriction and now has the option to reorder the “Always On” accounts. In screens 5 and 6, the consumer has chosen to give the “Issuer Bank” the highest priority. Additionally, screen 6 shows that “Trust Bank”, while still an available application, is not accessible over the antenna interface and will not be used to make a contactless transaction.

[1] The term “Always On” is only used as an example and is intended to convey to the consumer that an application is always accessible to a contactless reader.

[2] Refer to section 7.4.1 for more information on conflicts.

[3] While not shown in this scenario, another possible reason for such a conflict could be related to a mobile device that supports multiple Secure Elements but only allows a single Secure Element to be active at any one time. In this case, if the “Issuer Bank” application is on one Secure Element and the “Trust Bank” application and the “Fly Airways Bank” application are not on the same Secure Element, then the message on screen 3 would inform the consumer that the “Always On” settings for both “Trust Bank” and “Fly Airways Bank” will be switched off.

5 Architecture

While this document is based on the architecture detailed in *[ARCH]*, in order to enable application activation, specific additional components need to be highlighted. This chapter describes:

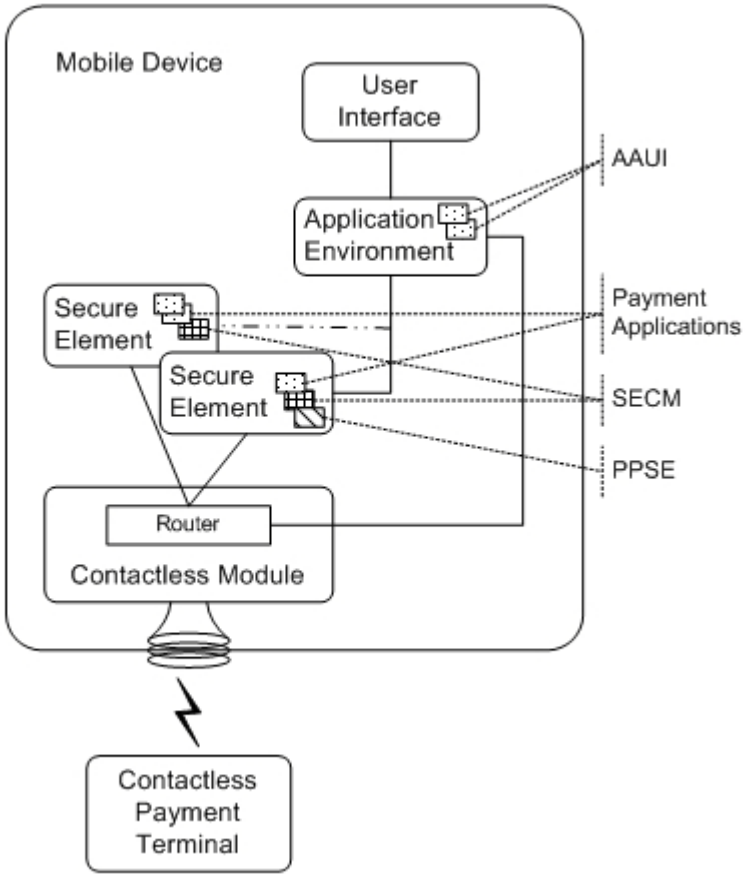
- The extended architecture required to enable application activation.
- The types of information that should be accessible and possibly configurable by an AAUI, and how this information may be mapped within the various components of the Mobile Device.

5.1 Extended Architecture

Figure 5-1 represents the extended architecture required to enable application activation. The following components are specific to this document and have not been fully described in *[ARCH]*. Additional details about the behaviour of these components are provided in the remainder of this book.

- Application Activation User Interface (AAUI) – This component, and the basis for this document, is a consumer visible application resident within the Mobile Device's application environment and used by the consumer to manage the contactless characteristics of one or more contactless mobile payment applications.
  - More than one AAUI may be present on a Mobile Device.
  - An AAUI may reside within a Secure Element.
  - Multiple AAUIs may interact with a single contactless mobile payment application, if the various components implement a certain minimum level of functionality described herein.
- Secure Element Contactless Management (SECM) – An operating system level application of a Secure Element that manages the contactless related characteristics of the contactless applications on that Secure Element.
- Proximity Payment System Environment (PPSE) – An application with the primary responsibility of communicating the active Contactless Mobile Payment Applications and the respective priorities by responding to a Contactless Payment Terminal as specified in *[ENTRY]*. In this architecture, the PPSE is depicted as an application on a Secure Element but it is feasible that it could be hosted elsewhere (for example, within the Mobile Device's application environment or within the Contactless Module).

Figure 5-1: Extended Architecture



5.2 Data Mapping

Figure 5-2 lists the types of information that should be accessible and possibly configurable by an AAUI and indicates how this information may be mapped within the various components of the Mobile Device. The figure depicts an AAUI with access to the Contactless Module, a primary Secure Element, and possibly one or more other Secure Elements present on the Mobile Device. In addition, the figure depicts that the Contactless Module will route communication to the relevant Secure Element whenever communication is occurring over the antenna interface.

The following describes the components and data thereon when viewing Figure 5-2 from the bottom up (further details are provided in the following chapters):

- The Contactless Module needs to know the parameters of the communications protocol of the currently accessible applications in order to successfully interact with a contactless terminal.

  The contactless routing table contains the information needed to route commands received over the antenna interface to the correct contactless application. For each application this includes:

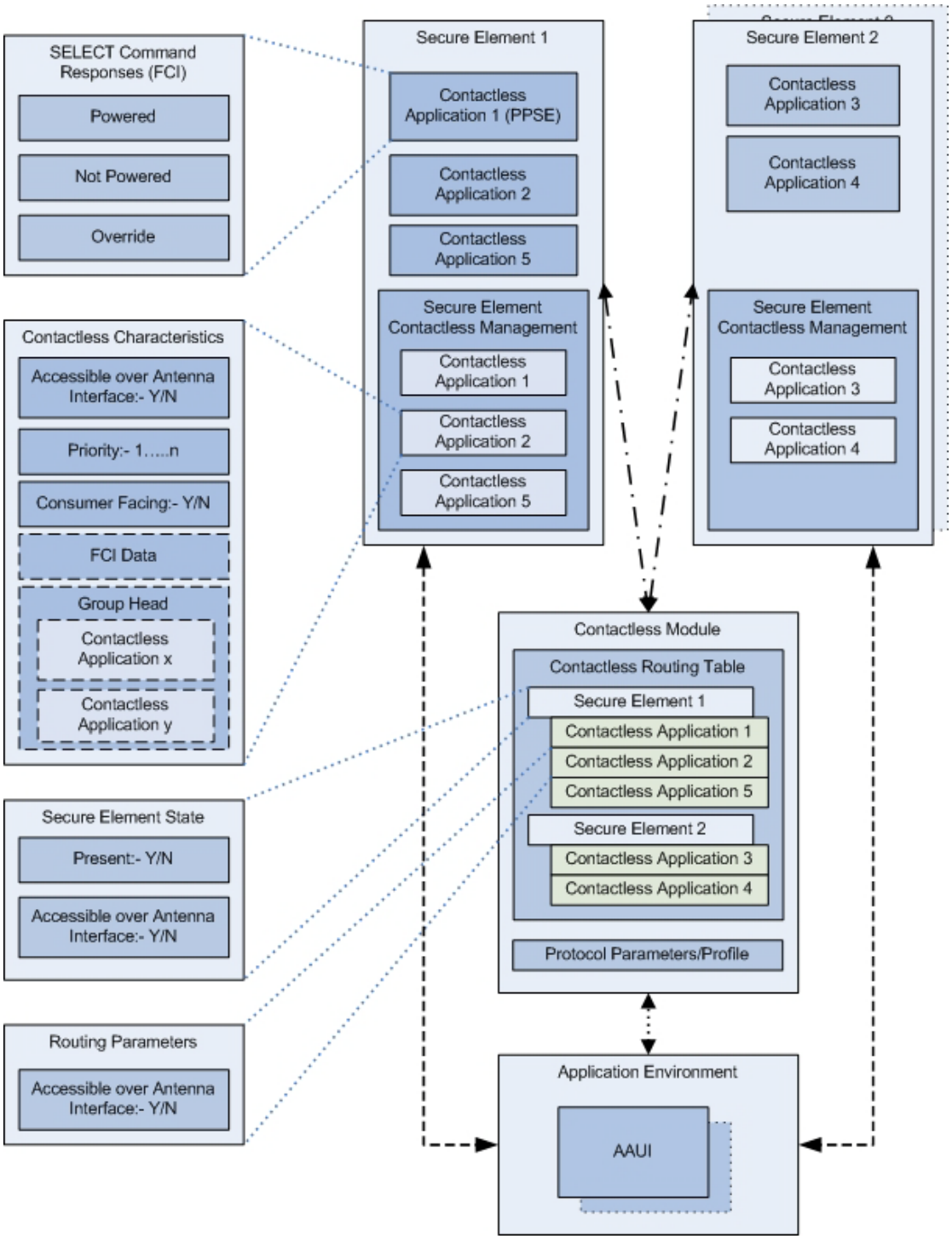
  - The Secure Element on which the application is located.
  - The application's accessibility state over the antenna interface.

- For each Secure Element, the Secure Element Contactless Management scheme contains the contactless relevant information of each contactless application, such as:

  - Whether the application is accessible over the antenna interface.
  - The priority order of the application.
  - Whether the AAUI will present information related to the application to the consumer (that is, whether the application is consumer facing).
  - Potentially the FCI data that will go into the PPSE.
  - Grouping information if the application is a group head.

- The PPSE will keep a record of FCI responses as instructed by the AAUI. (As this diagram depicts multiple Secure Elements, External Mode is assumed).

Figure 5-2: Data Mapping Diagram



6 AAUI Behaviour

This chapter expands the use cases described in Chapter 4 into flows that show the interaction between the AAUI, the consumer, and various other components on the Mobile Device. Separate flows show how these interactions differ depending on the mode being used.

Figure 6-1 provides the flow for use case 1 using External Mode.

Figure 6-2 provides the flow for use case 1 using Internal Mode.

Figure 6-3 provides the initial flow for use case 2. As this flow is only consumer interaction, it is identical for the External and Internal Modes.

Figure 6-4 is a continuation of the flow from Figure 6-3 and provides the flow in External Mode.

Figure 6-5 is a continuation of the flow from Figure 6-3 and provides the flow in Internal Mode.

6.1 Entities

The flows depict the actions taken by each of the following entities:

- Consumer – Self explanatory.
- AAUI – The user interface application that allows the consumer to manage the use of their contactless applications.
- Contactless Mobile Payment Application – An application that is hosted in a Secure Element and that performs information exchange and processing needed to complete a contactless mobile payment transaction.
- Secure Element Contactless Management – The component responsible for managing the contactless state (accessibility over the antenna interface) and priority usage of accessible contactless applications on a particular Secure Element implementation.
- PPSE – The component that will indicate to a contactless terminal which contactless applications are accessible and in what priority order.
- Point of Sale – A Contactless Payment Terminal.

6.2 Conventions

In the flows:

- A solid connector indicates that the entity performing the action is initiating the subsequent action.
- A broken connector or broken lines indicate that the entity that performed the preceding action does not perform the subsequent action or that the next action may not occur immediately following the preceding action but could possibly occur at some future point.
- Where an action is composed of two steps, these are highlighted with a “1” or “2” on the connector.

Accompanying each flow is an expanded description of the necessary AAUI interactions. These descriptions are simplified, based on the assumption of a simple (and, in the short term, probably most common) Mobile Device configuration consisting of a single available Secure Element. Note that for a Mobile Device configuration where multiple Secure Elements are intended to be simultaneously active, Internal Mode is not possible and External Mode must be supported.

Note: The screens used in these flows are the same as those depicted for the use cases in Chapter 4 and are examples only. Please refer to Chapter 8, Best Practices, for more information on the “look and feel” of an AAUI.

6.3 External Mode Use Case 1 Flow

Figure 6-1 shows the flow for the simple use case described in section 4.1 when operating in External Mode.

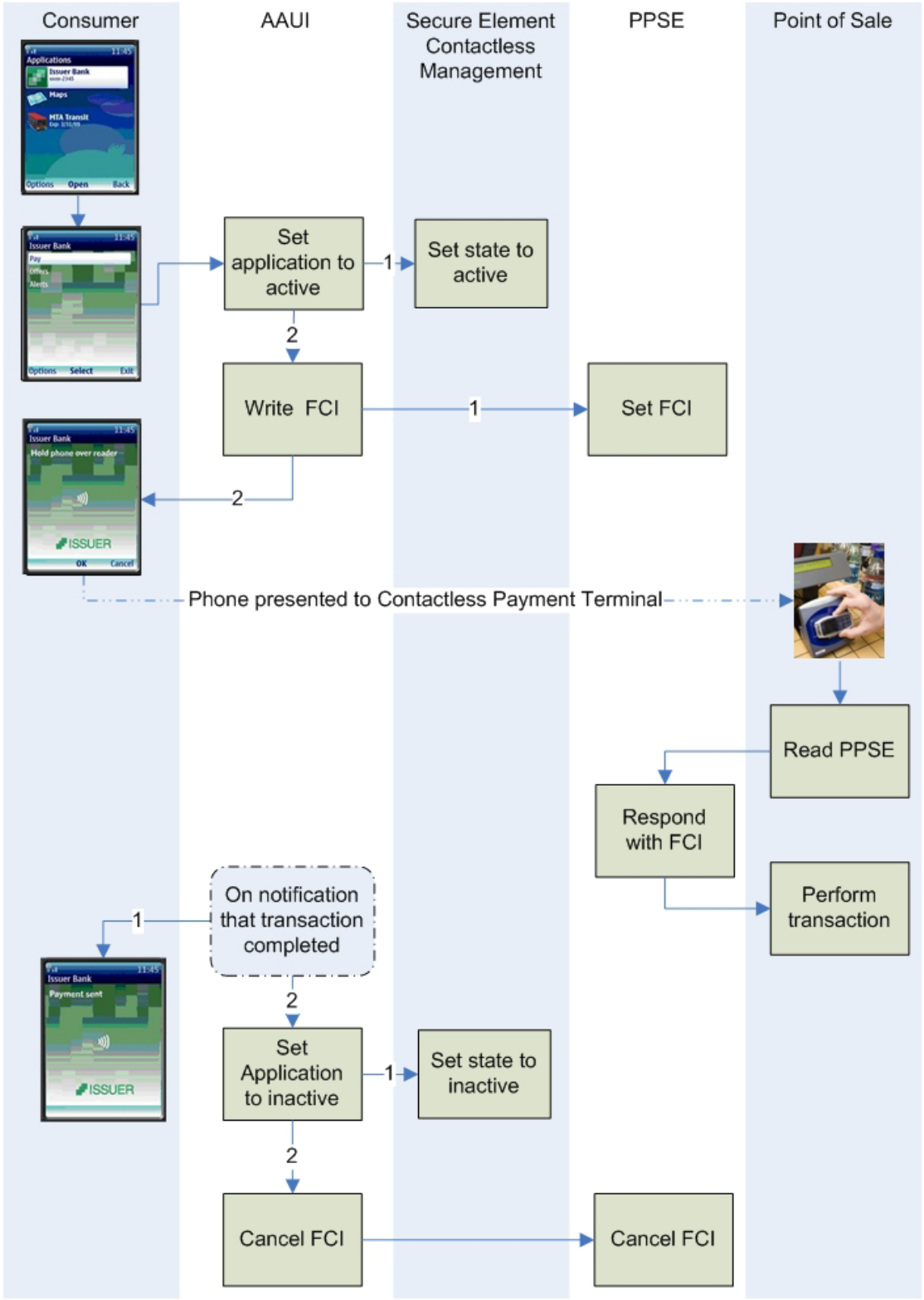
As the flow illustrates, the AAUI ensures that the contactless mobile payment application linked to the “Issuer Bank” will become known and accessible to a Contactless Payment Terminal in anticipation of the consumer imminently presenting the Mobile Device to a contactless terminal. That is:

- The AAUI informs the Secure Element Contactless Management entity for the Secure Element on which the contactless mobile payment application resides to set the state of the application to accessible over the antenna interface.
- The AAUI configures the PPSE to return the correct information to the Contactless Payment Terminal.

On completion of the payment transaction, the AAUI makes the contactless mobile payment application inaccessible to a contactless terminal by reversing the actions above:

- The AAUI informs the same Secure Element Contactless Management entity for the Secure Element on which the contactless mobile payment application resides to set the state of the application to inaccessible over the antenna interface.
- The AAUI configures the PPSE to return whatever information it previously returned to the contactless terminal.

Figure 6-1: External Mode Use Case 1 Flow



6.4 Internal Mode Use Case 1 Flow

Figure 6-2 shows the flow for the simple use case described in section 4.1 when operating in Internal Mode.

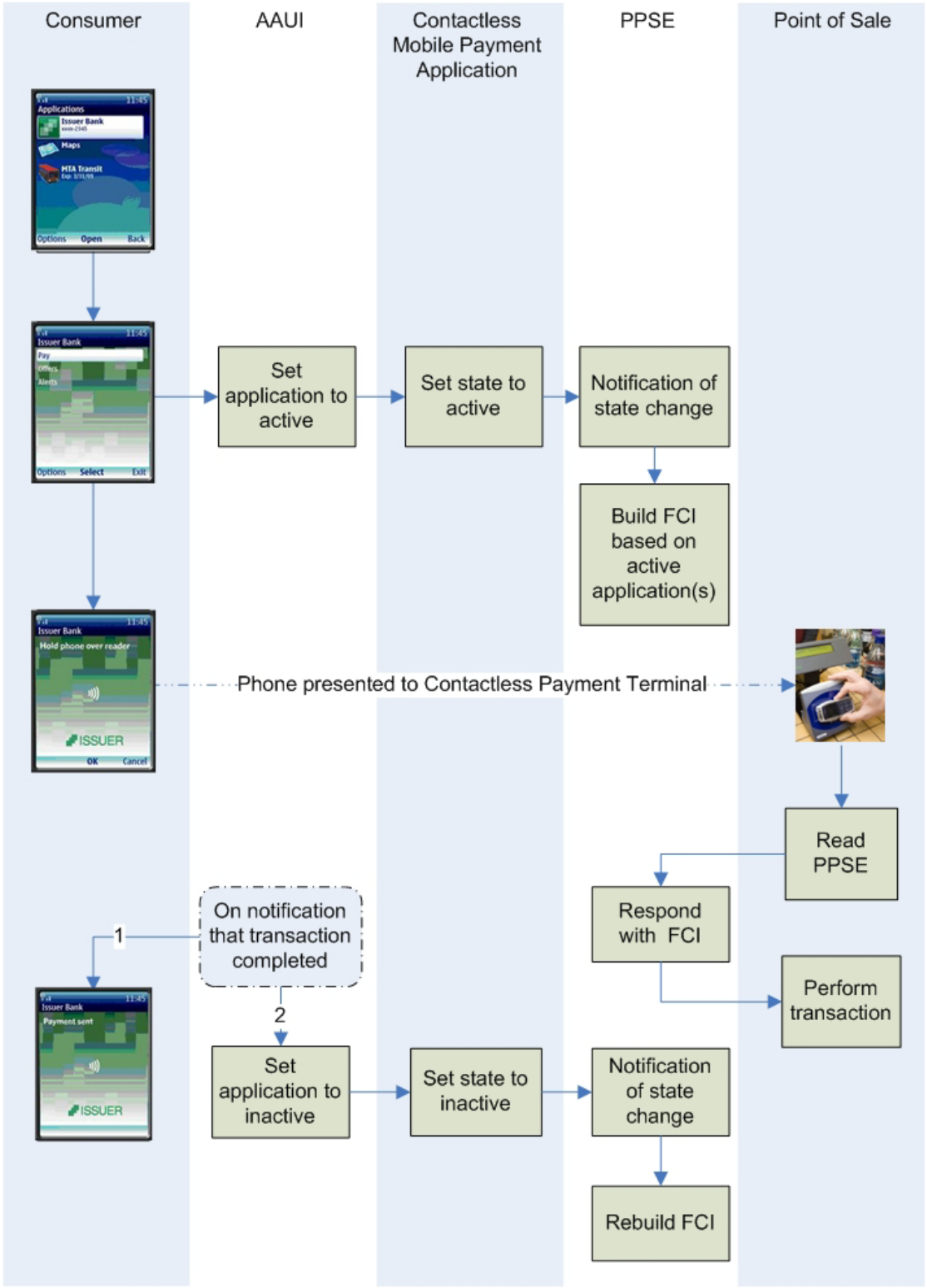
As the flow illustrates, the AAUI ensures that the contactless mobile payment application linked to the “Issuer Bank” will become known and accessible to a Contactless Payment Terminal in anticipation of the consumer imminently presenting the Mobile Device to a contactless terminal. That is:

- The AAUI informs the contactless mobile payment application itself to set its state to accessible over the antenna interface.
- A mechanism internal to the Secure Element allows the PPSE to be informed of the state change and the PPSE to build the information to be returned to the contactless payment terminal.

On completion of the payment transaction, the AAUI makes the contactless mobile payment application inaccessible to a contactless terminal by reversing the actions above:

- The AAUI informs the contactless mobile payment application to set its state to inaccessible over the antenna interface.
- The mechanism internal to the Secure Element allows this state change to be communicated to the PPSE so that the information to be returned to the contactless payment terminal can be rebuilt.

Figure 6-2: Internal Mode Use Case 1 Flow



6.5 Initial Flow for Use Case 2

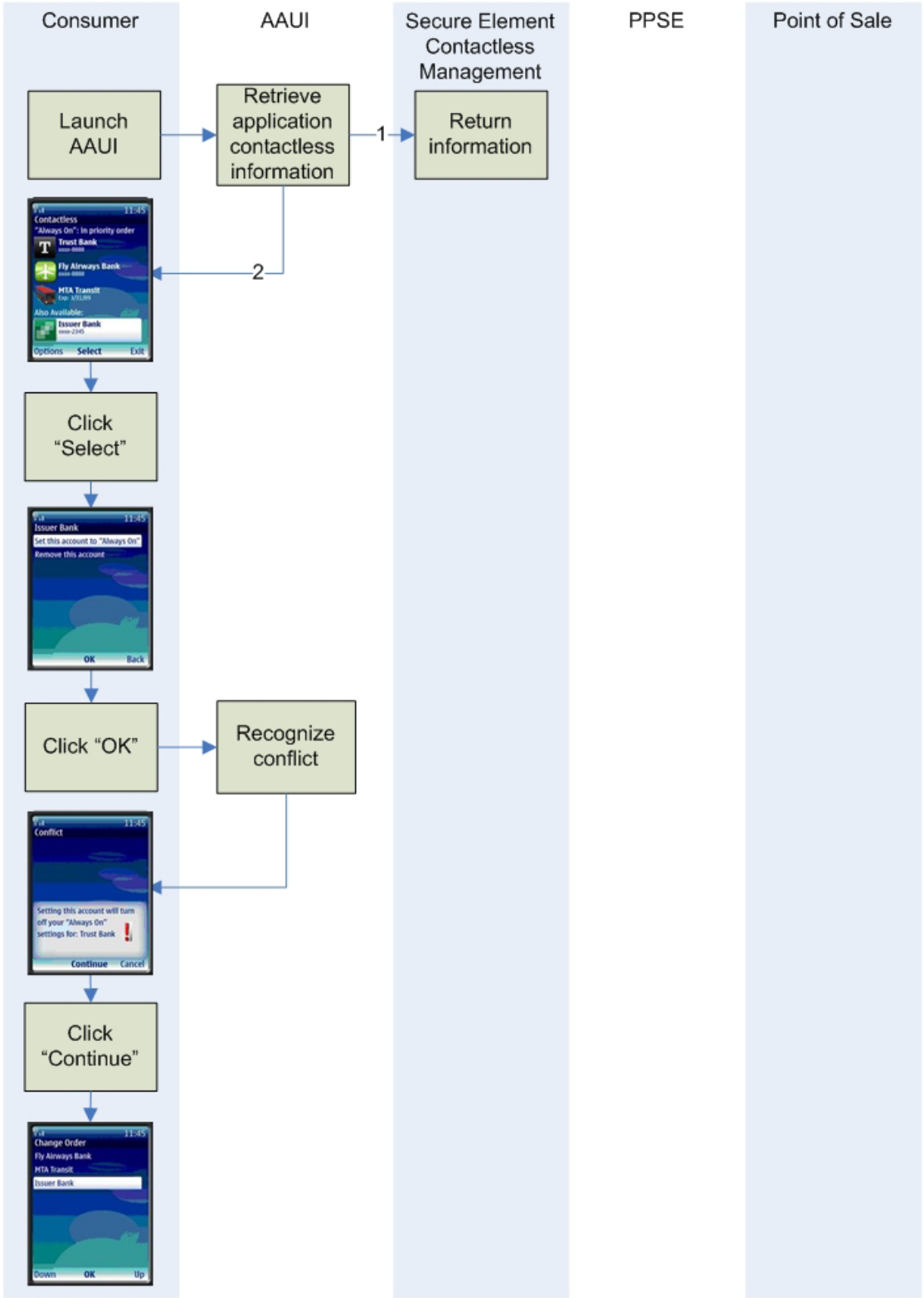
Figure 6-3 shows the initial flow of the consumer interaction for the use case described in section 4.2.

As the flow illustrates, the AAUI has the following initial responsibilities in this use case:

- It must retrieve the information of all the available contactless applications from all of the available Secure Elements.
- It must recognize, and alert the consumer to, the conflict between “Trust Bank” and “Issuer Bank”.

This use case then splits into alternate flows depending on whether External or Internal Modes are being used.

Figure 6-3: Use Case 2 Flow 1 of 2



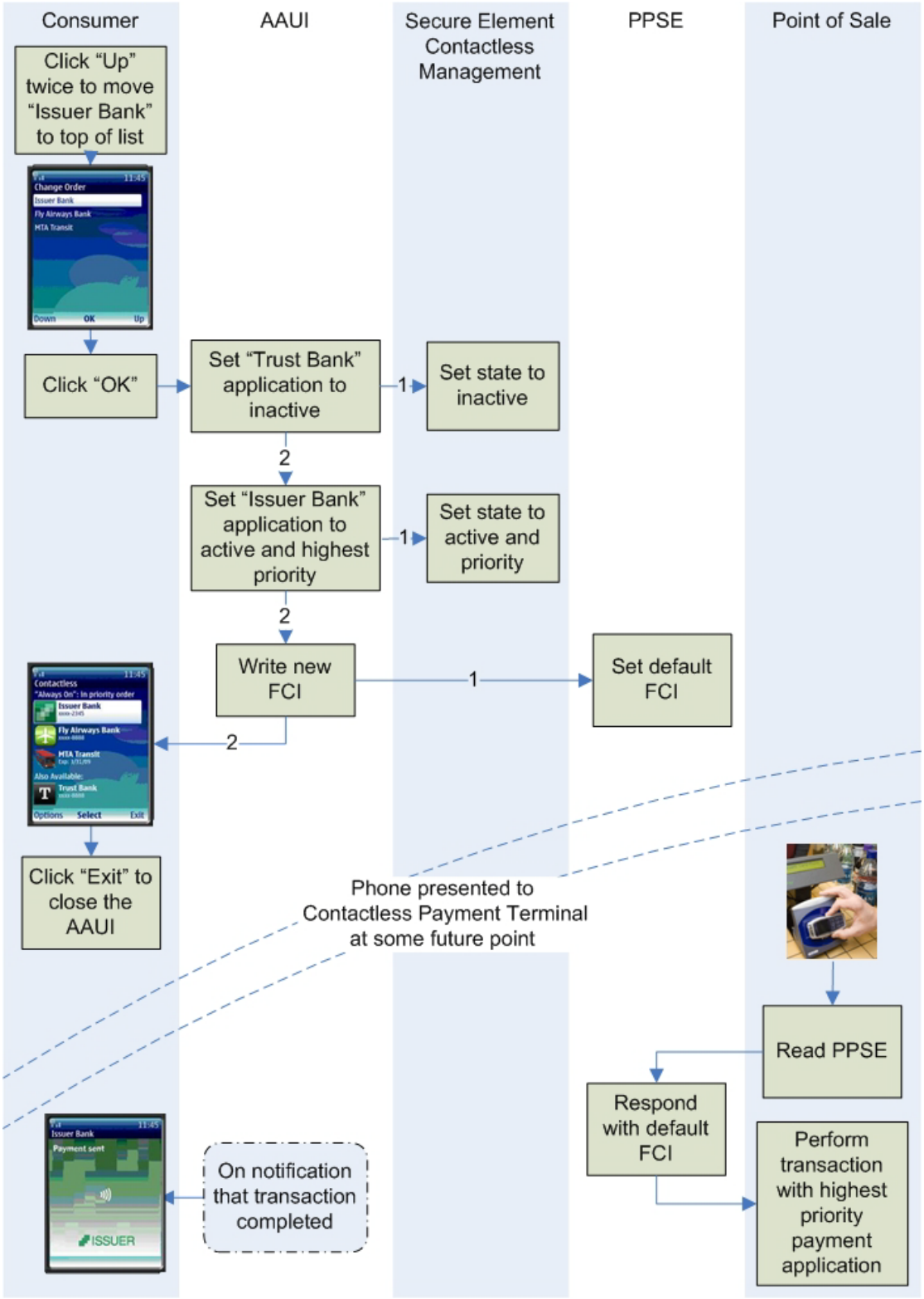
6.6 External Mode Use Case 2 Flow

Figure 6-4 shows the flow (following that illustrated in Figure 6-3) for the use case described in section 4.2, when using External Mode.

For this use case and as the flow illustrates, the AAUI has the following responsibilities when using External Mode:

- The AAUI informs the Secure Element Contactless Management entity for the Secure Element on which the “Trust Bank” contactless mobile payment application resides to set the state of the application to inaccessible over the antenna interface.
- The AAUI informs the Secure Element Contactless Management entity on the Secure Element on which the “Issuer Bank” contactless mobile payment application resides to set the state of the application to accessible over the antenna interface.
- The AAUI informs the Secure Element Contactless Management entity for the Secure Element on which the accessible contactless applications reside to reorder their priorities as per the consumer’s choice.
- The AAUI builds the FCI based on the accessible contactless applications and their priority order and configures the PPSE with this information.

Figure 6-4: External Mode Use Case 2 Flow 2 of 2



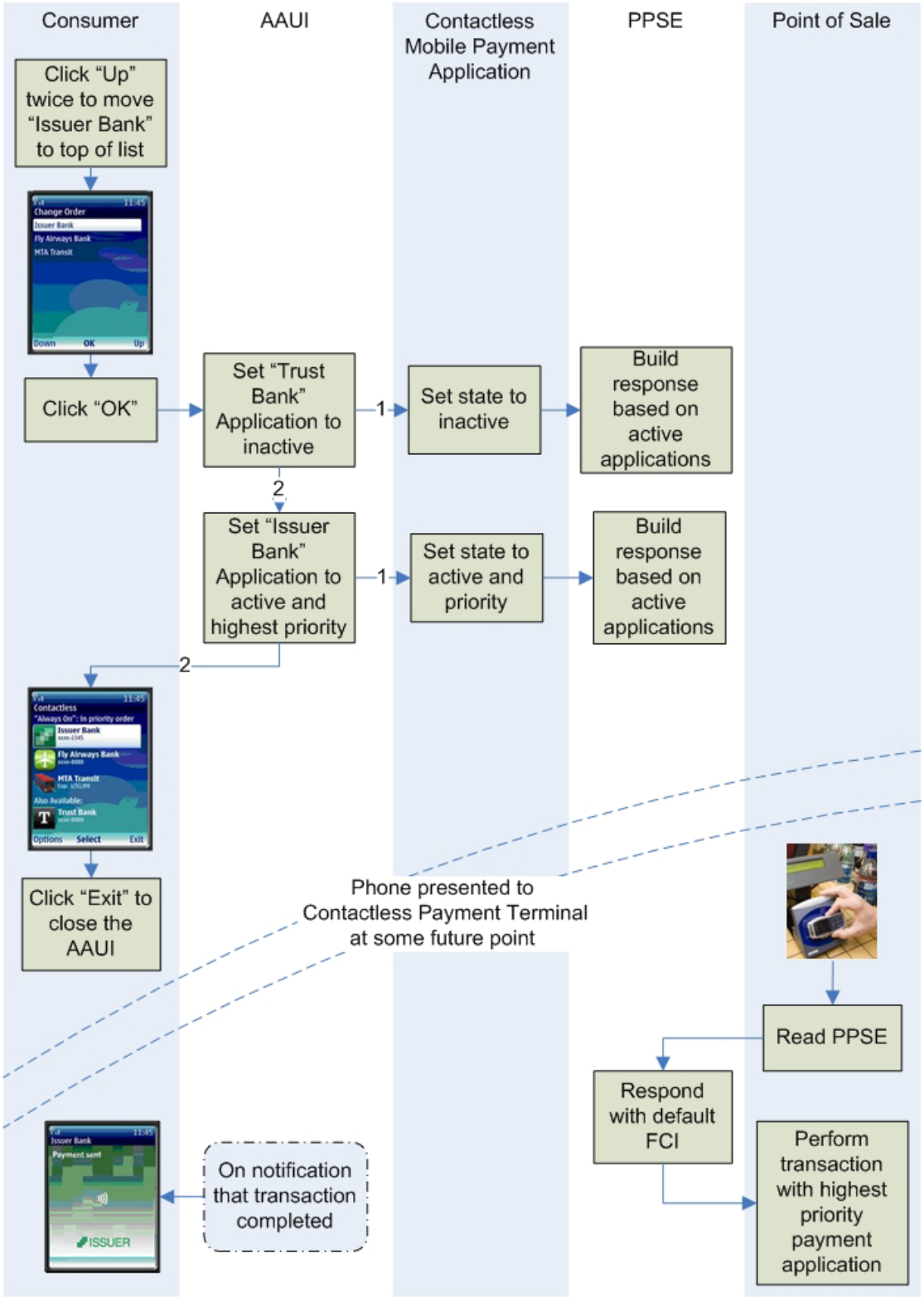
6.7 Internal Mode Use Case 2 Flow

Figure 6-5 shows the flow (following that illustrated in Figure 6-3) for the use case described in section 4.2, when using Internal Mode.

For this use case and as the flow illustrates, the AAUI has the following responsibilities when using Internal Mode:

- The AAUI first informs the “Trust Bank” contactless mobile payment application to set its own state to inaccessible over the antenna interface.
- A mechanism internal to the Secure Element allows the PPSE to be informed of the state change and to build the information to be returned to the contactless payment terminal.
- The AAUI then informs the “Issuer Bank” contactless mobile payment application to set its own state to accessible over the antenna interface.
- A mechanism internal to the Secure Element allows the PPSE to be informed of the state change and to build the information to be returned to the contactless payment terminal.

Figure 6-5: Internal Mode Use Case 2 Flow 2 of 2



7 Contactless Application Activation Management

As demonstrated by the use cases and flows in the preceding chapters, application activation is a consumer-controlled function that is based on the current state of the contactless applications present on the Mobile Device. The AAUI presents the current view of the contactless applications it manages to the consumer and allows the consumer to manipulate the settings or characteristics of those applications.

The main focus of this document is from the point of view of the consumer making changes to the contactless characteristics of one or more of their contactless applications and how these changes are propagated across the Mobile Device. The following is a brief overview of the process used to ensure that the consumer's choices are respected when a contactless operation occurs.

- A consumer wishing to view or change the behaviour of their contactless applications launches the relevant AAUI.
- The AAUI retrieves the contactless characteristics of the contactless applications it manages.
- The AAUI displays all the consumer-relevant contactless application information to the consumer.
- The AAUI allows the consumer to make changes, while highlighting and managing any conflicts that may occur.
- For each change the consumer makes, the AAUI:
    - Updates the contactless characteristics (prioritization and accessibility state) of the affected application(s).
    - In External Mode only, updates the PPSE FCI to reflect any changes.
    - Updates any necessary contactless routing to reflect the changes.

The remainder of this chapter expands on this overview.

7.1 Application-Specific Contactless Information

To make the behaviour described above possible, contactless applications provisioned to Mobile Devices must contain and/or provide their own application-specific contactless information and characteristics to enable an AAUI to function correctly. For example, the AAUI must be able to determine whether the contactless capability of the Mobile Device is enabled.

Similarly, the contactless management scheme (SECM) employed by the Secure Element implementation on which a contactless mobile payment application is being provisioned needs certain information and of course this information may differ depending on the scheme employed.

In general the following basic information should be retrievable by the AAUI at any point following the provisioning of a new contactless application:

- The AID of the application.
- The accessibility state of the application; that is, whether the application is immediately accessible over the antenna interface.
- Whether the application is consumer facing; that is, whether an AAUI will present information regarding this contactless application to the consumer.

  Contactless applications that are not consumer facing include:

  - the PPSE
  - a contactless application that is part of a group of contactless applications but is not the group head
- When operating in External Mode, the data that must be populated to the PPSE when the contactless mobile payment application is accessible over the antenna interface; that is, the directory entry or directory entries necessary to build the FCI. (When operating in Internal Mode, the PPSE will retrieve this information directly from the SECM.)

The following information may also be available and usable by the AAUI depending on the SECM scheme:

- Protocol information, which could be a profile[4] or specific contactless parameters, defining the exact contactless protocol required to ensure the correct operation of the contactless application when communicating with a contactless terminal. The AAUI may use this information to correctly configure the Contactless Module.
- A family identifier indicating under which family this contactless application belongs; for example, whether the contactless application is primarily a payment, transit, identity, or other type of application.
- Consumer-facing graphics, descriptions, links, etc., that may be used by an AAUI to present information related to the contactless application to the consumer.
- Identification of the contactless application that is used to present the list of accessible applications to a contactless terminal. In the case of EMV-based contactless mobile payment applications and this document, this is the PPSE.
- Group information, if multiple contactless applications are bundled together as part of an overall product and only one contactless application—the group head or group owner—is consumer facing.

  Example:

  > A service provider provisions one or more different types of contactless mobile payment applications (credit, debit, international, domestic, pre-paid, purse, etc.) along with one or more different types of contactless transit applications (bus, train, subway, ferry, etc.) and instead of allowing the consumer to manage each individually, these are managed as a group with only one of the group being consumer facing. In this case the consumer would see only one application presented to them in an AAUI but any changes made to this one application would affect all the member applications.

- Whether it is possible for the contactless application to be accessible over the antenna interface when the Mobile Device is not Switched On. The AAUI can use this information to indicate to the consumer which applications will be used when the consumer's device is Switched On and which will be used when the device is not.

[4] As discussed on page 50.

- Whether, when this contactless application is accessible over the antenna interface, one or more other contactless applications should not be. This limitation exists to prevent the operation of one contactless application from interfering with the correct functioning of another.

  Example:

  A non–EMV-based contactless mobile payment application (which does not get listed in the PPSE) may co-exist on a Mobile Device that also hosts EMV-based contactless mobile payment applications. The non–EMV-based application could indicate that the PPSE must not be simultaneously accessible over the antenna interface. This would ensure that if a consumer has indicated that payment should be made with the non–EMV-based application, and the Mobile Device is presented to a contactless payment terminal that supports both EMV-based and non–EMV-based contactless payment, the terminal would transact with the desired application.

7.2 Retrieving Information and Characteristics

The first task of the AAUI during its launch cycle is to retrieve all the relevant information and current contactless characteristics of the contactless applications present on the Mobile Device. As per the system architecture figure in *[ARCH]*, these contactless applications may be hosted in a variety of Secure Elements and the AAUI must retrieve the most up-to-date information on each Secure Element and each contactless application thereon. There are a variety of reasons why this information may have changed since the AAUI was last active, such as:

- Another AAUI has modified the information.
- The state of the contactless application has been modified by the contactless application itself or by some other management application.
- New contactless applications have been provisioned to the device.
- Contactless applications have been deleted from the device.
- A new Secure Element has been inserted or activated.
- A Secure Element has been removed or deactivated.

The method of retrieving the contactless characteristics and information and Secure Element states is specific to the Contactless Module environment and to the SECM scheme of each Secure Element.

7.3 Presentation to Consumer

After retrieving the necessary information and characteristics of all the contactless applications, the AAUI can then present these to the consumer. Please refer to Chapter 8, Best Practices, for guidelines on how this information is to be presented. The AAUI can present all the contactless applications to the consumer or only those applications that are relevant to the particular AAUI. For example, as can be seen by use case 1 described in section 4.1, a product-specific AAUI may only present and allow manipulation of a single contactless mobile payment application, while a payment focused AAUI may only present, and allow manipulation of, all the available contactless mobile payment applications, leaving the management of non-payment contactless applications to another AAUI.

The implementer of the AAUI determines whether the consumer-facing images, graphics, descriptions, etc., presented to the consumer are those retrieved from the contactless applications themselves, those retrieved from the SECM, those retrieved by some other standard or proprietary means not described in this document, or a combination thereof. However, the rules implied by the characteristics retrieved from the Secure Element should be respected if they are present. For example, contactless applications that have not been flagged as consumer facing are not presented by the AAUI to the consumer. This most likely applies to the PPSE and to contactless applications that are members of a group but not the head or owner of the group.

7.4 Setting Consumer Choice(s)

The AAUI provides the functionality allowing the consumer to modify the contactless characteristics for each of the applications presented. Which characteristics the AAUI allows the consumer to modify may depend on the contactless application itself and the SECM scheme employed by the Secure Element on which each contactless application is hosted. Possibilities include:

- Changing whether a contactless application can be accessed by a contactless terminal that supports that contactless application. That is, if a contactless application is currently accessible over the antenna interface, the consumer can make it inaccessible, or vice versa.
- Prioritising the usage of the contactless applications that are currently accessible over the antenna interface. That is, the consumer prioritizes the order of the accessible applications on their Mobile Device. A contactless terminal will then interact with the highest priority application that is common to both the contactless terminal and the Mobile Device.
- Indicating whether the consumer wants a contactless application to continue working even if the Mobile Device is not Switched On. This is typically useful when the Mobile Device is not able to perform any of its primary functions but is still capable of performing a contactless transaction that does not make use of these primary functions (mainly the user interface).

  This option is possible only if the application provider has indicated that the contactless application is usable when the Mobile Device is not Switched On.

In each of the above cases, the changes made to a group head or group owner apply to all the contactless applications that are part of that group.

Depending on the SECM scheme of the Secure Element upon which each modified application, and/or each application affected by a modification, is hosted, the AAUI provides the necessary information to that SECM entity.

7.4.1 Resolving Conflicts

The AAUI manages and resolves conflicts that may result from the choices made by the consumer. That is, the AAUI ensures that an action made by the consumer does not cause an issue with conducting a contactless transaction or potentially allow a contactless transaction to occur using an incorrect contactless application.

In some cases, conflicts may not be an issue for an AAUI on a specific Mobile Device. For example, a Mobile Device that has a single common contactless technology and applications that seamlessly operate simultaneously from a technology and business point of view could have an AAUI that does not need to address conflicts.

However, there are a number of scenarios that could cause conflicts, such as:

- The antenna interface is disabled when the AAUI is making an attempt to set a contactless application as accessible over the antenna interface.
- A Mobile Device supports multiple contactless technologies or supports contactless applications that use the same technology but require slightly different settings that would prevent one of these applications from working over the antenna interface. One real life example of such a conflict is the slightly different contactless parameter settings used in some payment environments as opposed to some transit environments.
- A Mobile Device supports multiple contactless applications but, from a business point of view, there are settings within the AAUI itself to prevent two competing products being accessible over the antenna interface simultaneously.
- A Mobile Device supports multiple contactless applications but from an operational point of view, there are rules that define that when a particular contactless application is accessible over the antenna interface, one or more of the other contactless applications may not be simultaneously accessible over that same interface.
- A Mobile Device supports multiple Secure Elements but has a Mobile Device level policy that mandates that when a certain Secure Element is active, all other Secure Elements are inactive. EMVCo does not endorse this policy but recognizes that there may be business reasons for such a policy.
- A Mobile Device that supports contactless transactions in low, or no, power mode (that is, when not Switched On) hosts contactless applications that require the presence of a user interface application during contactless processing and so are only intended to be operational when the device is Switched On. In such a case, if the AAUI allows the consumer to specifically modify the characteristics of a contactless application for the event when the Mobile Device is not Switched On, then the contactless applications reliant on the phone being Switched On must be excluded from these operations.

In these cases, the AAUI must identify the conflicts and take actions, possibly with user interaction, to resolve them. Refer to Chapter 8, Best Practices, for guidelines on how conflicts are to be conveyed to the consumer.

7.4.2 Updating the PPSE

External Mode

If the AAUI is implemented to use External Mode, once all the relevant SECM entities have been updated to reflect any consumer initiated modifications, the AAUI configures the PPSE. The AAUI will build the FCI Proprietary Template that reflects the consumer's choices and update the PPSE. (As depicted in the architectures in Figure 5-1 on page 17 and Figure 5-2 on page 19, this document assumes that the PPSE is hosted on a Secure Element.)

The FCI Proprietary Template is built using the directory entries retrieved according to the relevant SECM scheme for all the contactless applications that are intended to be accessible over the antenna interface.

If an AAUI is configuring the Mobile Device for contactless transactions that will occur in the future, for each set of applicable contactless applications, the AAUI performs the following basic functions:

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

In addition, if the resulting FCI Proprietary Template contains a directory entry, or entries, that have no possibility of being accessed over the antenna interface, the AAUI removes the directory entries for those contactless applications that would not be accessed. For example, if multiple directory entries have the same base AID—a base AID being a portion of the full AID—then only the highest priority directory entry with this base AID would ever be selected by a Contactless Payment Terminal. Removing the lower priority directory entries reduces the size of the FCI Proprietary Template and improves the overall transaction execution time.

If the AAUI provides functionality to allow the consumer to set specific contactless applications as accessible over the antenna interface when the device is not Switched On, an FCI Proprietary Template is built to support this device state.

If an AAUI is preparing a single application to be used for a specific upcoming contactless transaction (as per use case 1, described in section 4.1), a temporary Override FCI Proprietary Template is built according to the directory entry for that application.

One or more FCI Proprietary Templates are written to the PPSE according to the manner in which the FCI is intended to be used. That is:

- An FCI Proprietary Template that will be returned when the device is Switched On.
- An Override FCI Proprietary Template to be returned for upcoming imminent contactless transaction(s) and until the AAUI informs the PPSE to stop returning this FCI.
- An FCI Proprietary Template that will be returned when the device is not Switched On.

Specifically for the usage described in the second bullet above, on completion of the contactless transaction(s), the AAUI will indicate to the PPSE that the Override FCI Proprietary Template must no longer be returned over the antenna interface and the regular FCI Proprietary Template(s) are to be returned.

Internal Mode

If the PPSE is configured to use Internal Mode, after any change to the state of a Contactless Mobile Payment Application, the PPSE will be updated based on information known to the SECM and retrievable by the PPSE. (For Internal Mode, the PPSE must be hosted on the currently active Secure Element; that is, the same Secure Element as the currently active Contactless Mobile Payment applications.)

The FCI Proprietary Template is built using the directory entries retrieved according to the relevant SECM scheme for all the contactless applications that are intended to be accessible over the antenna interface.

For each set of applicable contactless applications, the PPSE performs the following basic functions:

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

In addition, if the resulting FCI Proprietary Template contains a directory entry, or entries, that have no possibility of being accessed over the antenna interface, the PPSE removes the directory entries for those contactless applications that would not be accessed. For example, if multiple directory entries have the same base AID—a base AID being a portion of the full AID—only the highest priority directory entry with this base AID would ever be selected by a Contactless Payment Terminal. Removing the lower priority directory entries reduces the size of the FCI Proprietary Template and improves the overall transaction execution time.

If the SECM provides functionality to identify contactless applications as accessible over the antenna interface when the device is not Switched On, the PPSE builds an FCI Proprietary Template to support this device state.

7.4.3 Configure Contactless Router

If a Mobile Device supports only a single Secure Element, there is no need to configure a Contactless Router, as all communication received over the antenna interface is routed to that single Secure Element. However, on devices that support multiple Secure Elements, a necessary feature is the Contactless Router that will be able to route contactless communication to the correct Secure Element.

If only one Secure Element is accessible over the antenna interface at any one time, the routing could be a simple instruction from the AAUI to the Contactless Module to switch all communication over the antenna interface from one Secure Element to another.

If multiple Secure Elements are simultaneously accessible over the antenna interface, routing is more complicated. The Contactless Module compares the AID received in the SELECT command to the AID information in the Contactless Router in order to direct communication to the correct Secure Element. The exact manner in which the Contactless Router is originally configured is outside the scope of this document. However, there is a specific scenario where the AAUI may have to manipulate the Contactless Router based on the consumer's choice of accessible contactless application. In this scenario, a contactless application with the same AID may exist on multiple Secure Elements. If the consumer has indicated a specific application on a specific Secure Element to be accessible over the antenna interface, the AAUI must configure its twin application in the Contactless Router as inaccessible over the antenna interface to avoid the possibility that the incorrect application be used to conduct the contactless transaction.

7.4.4 Setting Protocol Parameters/Profiles

If a Mobile Device supports only a single technology configured to work according to the contactless reader infrastructure where the device would be most likely deployed, there is no need to set protocol parameters. However, on Mobile Devices that allow the technologies they support to be configured depending on the contactless applications that are accessible, it may be necessary to inform the Contactless Module that the technology being used by these contactless applications assumes that certain contactless protocol parameters must be configured in order for a contactless terminal to successfully communicate with the Mobile Device and the consumer's chosen contactless application. Where this is required by the contactless applications and supported by the Contactless Module, the AAUI is responsible for indicating to the Contactless Module what parameter settings are necessary.

As an alternative to multiple individual contactless parameters, some SECM schemes define profiles for some of the most commonly used communication protocols. A specific example of this is the profiles for the EMVCo defined contactless communication protocol.

8 Best Practices

The best practices described in this chapter typically apply to a user interface application (an AAUI) on a Mobile Device that has a relationship to one or more of the contactless applications hosted on the Secure Element on the Mobile Device. While such an application could have additional functionality that is beyond the scope of these best practices, it is likely that the application will have functionality that may:

- List the consumer-facing contactless application(s).
- Allow the consumer to order the contactless applications within that list according to the consumer's own preferences.
- Allow the consumer to prioritize the order in which a contactless terminal will interact with the contactless payment applications according to the consumer's own preferences.

While these best practices could apply to more than one industry, they are targeted towards the payment industry and all examples use EMV-based contactless mobile payment application examples.

8.1 General

An AAUI should make use of the graphical capabilities of the Mobile Device. A purely text-based AAUI is strongly discouraged and is outside the scope of these best practices.

8.2 Representation of Payment Applications

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

Anyone who has been involved in the contactless industry even briefly knows that there are many technical or detailed aspects that are of no interest to the majority of consumers (ISO 14443, Types A and B, PPSE, AIDs, Secure Element types, etc.). One of the main focuses of this document is to make sure that the consumer does not need to have any knowledge of these. The AAUI should hide these details from the consumer while still providing the consumer with enough functionality to effectively manage all aspects of their contactless applications.

The AAUI should present only consumer-relevant contactless payment information to the consumer. For example:

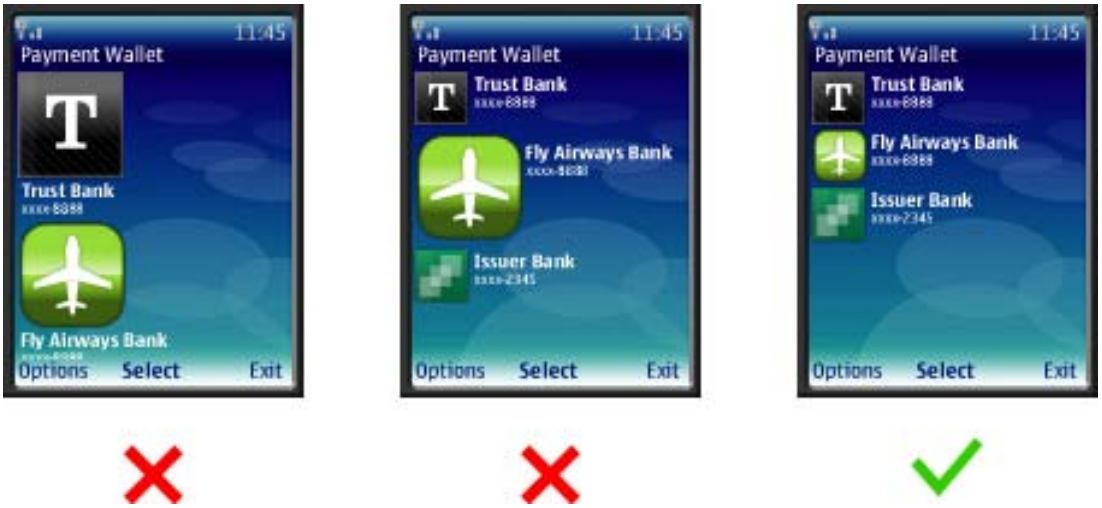
- The PPSE is a contactless application and integral to the correct operation of contactless mobile payment applications on a Mobile Device, but there is no need for it to be visible to the consumer or even for the consumer to be aware of its existence.
- A contactless product may consist of several contactless applications, each with its own unique AID. For the consumer, what is relevant and should be visible is the product rather than the individual applications that make up the product. The AAUI should present and allow the consumer to manage the product while the application manages the underlying applications whenever the consumer's actions affect the product.

8.3 Listing Products and Applications

When listing multiple applications:

- The list should be in the order chosen by the consumer. That is, the consumers preferred[5] application should be highest in the list. If the consumer has not indicated a preference for an application, the order of the applications is at the discretion of the AAUI.
- Each application in the list should have an equal amount of display real estate and a reasonable number of applications should be visible on any single screen.

Figure 8-1: Listing Contactless Capable Products and Applications



While the screen images in Figure 8-1 are purely illustrative, from a best practices point of view, each application listed should contain the following:

- An application provider's defined graphical icon representing the branding of the payment product that is recognizable to the consumer.
- An application provider's defined description of the payment product that is recognizable to the consumer.

[5] Please note that preferred should not be confused with priority.

- Priority is the order in which contactless applications are prioritized for use over the antenna interface.
- Preference is the order in which products are presented to the consumer from a user interface point of view.

Depending on the size of the display available to the AAUI and how the implementation provides further information, additional indicators such as a contactless indicator, priority indicator, Secure Element indicator, and power indicator could either be present together with the icon and description or could be secondary information. Secondary information might be displayed:

- When the application's focus is on within the list,
- When the application is selected, or
- As part of a secondary menu.

8.3.1 User Control

Consumers should be able to reorder their applications in the application list according to their own preferences.

Some consumers prefer to use a more personal description for certain of their payment products. To accommodate this preference, an AAUI may provide the capability for the consumer to modify the payment product's description.

8.4 Contactless Indicators

There are two contactless indicators that may be visible to a consumer. The first is most likely at a device level and its presence, or lack thereof, would indicate to the consumer whether the device is capable of any communication over the antenna interface. In most cases this indicator would be in the same “status bar” that contains other connectivity and system indicators such as the current cellular signal strength and the battery power reserve (this is also the same location that the Bluetooth headset symbol is displayed when a headset is paired with the device). If an AAUI obscures the status bar, it is the responsibility of the AAUI itself to manage this indicator. That is, there should an indication (most likely making use of the same symbol that would have been visible in the status bar) of the current contactless capability of the device itself. Ideally, the presence or absence of an indicator should indicate to the consumer whether the device is currently capable of communication over the contactless antenna.

The second indication, while linked to the first, is at the application level rather than the device level. Its purpose is to provide the consumer with a means to easily determine whether each of their contactless applications is accessible over the antenna interface. This state relates to whether the application is currently capable of responding to commands from an external contactless terminal over the antenna interface (that is, whether the application is accessible or inaccessible). While there are multiple ways to represent this, the consumer should be able to easily distinguish between contactless applications that are accessible and those that are not. Some examples of how this could be represented are:

- Use an indicator similar to the one used in the status bar in the actual application list to identify which applications are accessible.
- Use highlighting to differentiate accessible and inaccessible applications.
- List accessible applications separately from inaccessible applications.

The implementer of the AAUI determines whether accessible applications should be distinguished from inaccessible applications when the contactless capability of the Mobile Device is not enabled.

The initial accessibility state of a contactless application is determined either during the initial provisioning of the contactless application to the Mobile Device or by consumer configuration during the initial setup of the application.

8.4.1 User Control

The ability for the consumer to manage the contactless capability of the device itself is at the discretion of the Mobile Device manufacturer. Ideally this ability should not be present at the device level, as it could interfere with settings within the AAUI. An AAUI managing contactless applications should ensure (during its launch cycle) that the contactless capability of the device is currently enabled and if not, either enable it (and warn the consumer that the capability is being enabled) or indicate to the consumer that the AAUI cannot function correctly if contactless capability is not enabled. The implementer of the AAUI determines whether the application can continue to function correctly even though contactless communication is not enabled or whether to shut down.

Consumers should have the capability to manage the accessibility state of their contactless applications. That is, the consumer should be able to set an application that is currently accessible to inaccessible and vice versa. There are a variety of reasons that a consumer may wish to manage this state, especially when there are multiple applications on their device. For example, if the consumer has both personal and business contactless accounts available on their Mobile Device, they may want the personal card to be accessible for most transactions but when travelling on business may wish to make their personal card inaccessible and make their business card accessible. But even if a consumer only has one contactless account on their phone, the consumer may still wish to set the state to inaccessible, setting it to accessible immediately preceding a contactless transaction and resetting it to inaccessible immediately following the contactless transaction. While switching an application from accessible to inaccessible is a simple operation, the switching of an inaccessible application to accessible may affect the other applications that are currently accessible. There are a variety of reasons why certain applications cannot be simultaneously accessible, as described in section 7.4.1.

Whatever the reason, the consumer should be informed whenever an action will adversely affect a currently accessible application and be given the option to confirm or end the current action.

8.5 Priority Indicators

The priority indicator is used in the case where it is possible for a contactless terminal to communicate with more than one of the accessible applications on the Mobile Device. It is not necessary for priorities to be presented to the consumer but if the user interface allows the consumer to set/order the priority of their applications, the consumer should be able to discern the relative priority of the applications within the application list. The implementer of the AAUI determines how this is communicated to the consumer, but the following are a few suggested examples:

- Order
- Numbered

8.5.1 User Control

The consumer should have the capability to manage and reorder the priorities of their contactless applications. The implementer of the AAUI determines whether the consumer can manage accessible applications only or inaccessible applications as well. The AAUI and the underlying functionality on the Mobile Device will manage the final prioritization of the applications as presented to the contactless terminal.

8.6 Secure Element Indicators

If the Mobile Device has the capability to support multiple Secure Elements and the AAUI itself is capable of managing the possibility of multiple contactless applications residing on these multiple Secure Elements, the consumer may be provided with an indication as to which Secure Element each contactless application resides upon. This could be similar to phone book entries which on some devices are differentiated by an indicator identifying whether the entry is stored in the SIM or within the handset memory. The implementer of the AAUI determines exactly how, and if, this is communicated to the consumer.

8.6.1 User Control

The consumer may have the ability to activate/deactivate individual Secure Elements.

8.7 Power Indicator

The power indicator may be displayed if the following are true:

- At least one of the consumer-facing contactless applications is capable of working even if the Mobile Device is not Switched On.
- The AAUI gives the consumer the option of managing whether each such application will work when the Mobile Device is not Switched On.

The implementer of the AAUI determines exactly how, and whether, this is communicated to the consumer.

8.7.1 User Control

The consumer may have the ability to choose whether a contactless application that is capable of running when the Mobile Device is not Switched On shall be permitted to do so. (The consumer may wish to use certain applications when the Mobile Device is Switched On but some specific other application for the rare case when the Mobile Device is not Switched On.)

8.8 Power User Profiles

An AAUI may provide the capability for the consumer to create a number of profiles (for example a business profile, travel profile, personal profile, etc.). This is of course only relevant to “power users” who have multiple contactless products and frequently change the characteristics of these products.

Annex A Specifications – Usage Guidelines

This annex is focused on specifications published by external bodies. As additional publications become available that relate to this document, EMVCo will release updated versions or amendments to this document.

Based on the currently available external publications, this annex provides:

- Details of the manner in which an AAUI may potentially interface with components based on such publications.
- Details of the manner in which the PPSE, an SECM, or a Contactless Mobile Payment application could potentially interact with each other based on such publications.

A.1 GlobalPlatform

The GlobalPlatform Card Specifications Committee has published an amendment to GlobalPlatform Card Specifications 2.2 which specifies the functionality of a CRS (Contactless Registry Service), which is an SECM entity.

The CRS is a GlobalPlatform service (that is, an OPEN extension exposing a set of APIs) responsible for the management and maintenance of the contactless applications on the GlobalPlatform Secure Element. The CRS Application is a selectable application that uses these APIs and is accessible to applications on Mobile Devices over the device interface. (The CRS Application is not accessible or selectable over the antenna interface. The intention is to limit accessibility to the CRS Application to authorized applications on the Mobile Device alone.) The CRS APIs are used to correctly configure the CRS during installation, personalization, and/or application management. These APIs can also be used by the PPSE – when configured in Internal Mode – to be notified of changes to Contactless Mobile Payment applications that have indicated that the PPSE is their Contactless Registry Event Listener (CREL). The PPSE can then use the CRS APIs to build the list of active applications to be returned to a Contactless Payment Terminal.

The contactless characteristics for each contactless application present on a GlobalPlatform Secure Element are maintained in the CRS of that same Secure Element.

All the commands in this annex are for informative purposes only and *[GPCARD]* is the definitive reference. The following notation is used:

- 'x' – indicates a value that is unknown or could vary depending on the context used.
- '##' – indicates a length that is dependent on the subsequent data.

A.1.1 Install/Personalization Information

As described in section 7.1, in order for an application loaded to a GlobalPlatform Secure Element to be managed by the CRS, the CRS needs to be aware of certain information and contactless characteristics of the application. As per the GlobalPlatform specification, information and characteristics are provided to the CRS during the install or personalization process of the contactless application. Table A.1 lists the GlobalPlatform-defined TLV fields that have a potential impact on the behaviour of a Contactless Mobile Payment Application. (These do not apply to the PPSE.)

Table A.1: Payment Application – CRS Contactless Characteristics

Tag	Description	
'A0'	Protocol Type A Template	
	'80'	EMV-specific – Indicates that the application is selectable when the device is communicating over the antenna interface as per ISO 14443 Type A as defined in *[CCPS]*. '3230' indicates version 2.0 of the CCPS specification.
'A1'	Protocol Type B Template	
	'80'	EMV-specific – Indicates that the application is selectable when the device is communicating over the antenna interface as per ISO 14443 Type B as defined in *[CCPS]*. '3230' indicates version 2.0 of the CCPS specification.
'87'	Application Family Identifier – Identifies the family this application belongs to. (See Table 12 of ISO 14443-3.) '20' identifies the financial family.	
'88'	Display Required Indicator – Indicates whether an application is only intended to run in conjunction with a user interface application. A value of '01' indicates that the application does not require a display and '00' indicates that the application requires a display.	
'7F20'	Display Control Template. This template contains information that could be displayed to the consumer from within a user interface application. The template is only relevant if the application is intended to be visible to the consumer within a user interface application and is a standalone application or is a group head.	
	'6D'	Application Image Template. This template contains an image and optional image encoding data. (See *[GPCARD]*, section 3.2.)

Tag	Description		
		'5F44'	Application Image. An image intended to clearly identify this application to the consumer. (See *[GPCARD],* section 3.2.) The image may be presented by a user interface application.
		...	Possibly image encoding data
	'5F50'	URI. A URI to a site that will provide more details of the application to the consumer. (See *[GPCARD],* section 3.2.) The URI can be displayed as a hyperlink by a user interface application.	
	'5F45'	Application Display Message. Text that will clearly describe this application to the consumer. The first byte of this value indicates the message encoding format of the subsequent data. (See *[GPCARD],* section 3.2.) The message can be presented by a user interface application.	
'A2'	Application Group Head – Only relevant if the application is a member of a group. This template will identify the application's group head.		
	'4F'	The AID of this application's group head	
'A3'	Application Group – Only relevant if application is a group head. This template contains a list of the potential members of the group.		
	'4F'	The AID of a group member	
	...		
	'4F'	The AID of a group member	
'A4'	CREL Application AID List – Only relevant if the application is a standalone application or a group head. This list identifies the PPSE and other CREL applications, if any.		
	'4F'	The AID of the PPSE: '325041592E5359532E4444463031'.	
	…		
'A5'	Policy Restricted Application(s) – Relevant only if there is a specific application that is not intended to be accessible whenever this application is accessible.		
	'4F'	ADF Name (AID) – AID of the restricted application	

Tag	Description			
'A6'	Application Discretionary Data – Data that is discretionary to this type of application. EMV specifies the following content for this data and the application owner may specify additional data			
	'BF0C'	FCI Data		
		'61'	Directory Entry of the highest priority Application	
			'4F'	ADF Name (AID) – AID of the highest priority application in this list
			'9F28'	Kernel Identifier as per Entry Point
			'81'	Length of base AID. If present, this indicates that this entry can be removed if a higher priority application being presented by the PPSE has the same base AID.
			…	
		…		
		'61'	Directory Entry of the lowest priority Application	
			'4F'	ADF Name (AID) – AID of the lowest priority application in this list
			'9F28'	Kernel Identifier as per Entry Point
			'81'	Length of base AID. If present, this indicates that this entry can be removed if a higher priority application being presented by the PPSE has the same base AID.
			…	
	…			

Table A.2 and Table A.3 define the structure of the Contactless Protocol Parameters and User Interaction Parameters that will be present either in the System Specific Parameters of the INSTALL command or in an application-specific DGI (Data Grouping Identifier) used to populate the CRS registry entries defined in Table A.1. Whether the contactless information and characteristics are provided during installation or personalization is an implementation choice.

Table A.2: Contactless Protocol Parameters

Content					Presence
'A0'	'12‘	Contactless Protocol Parameters			Mandatory
	'A2'	'10'	Contactless Protocol Parameter Profile		Mandatory
		'A0' '06' '80' '04' '33323330'		Protocol Type A	Mandatory
		'A1' '06' '80' '04' '33323330'		Protocol Type B	Mandatory

Table A.3: User Interaction Parameters

Content						Presence
'A1'	'##'	User Interaction Parameters				Mandatory
	'88'	'01'	'xx'	Display Required Indicator		Optional
	'87'	'01'	'20'	Application Family Identifier		Optional
	'7F20'	'##'	Display Control Template			Conditional[6]
		'6D'	'##'	Application Image Template		Optional
			'5F44' '##' 'xx...xx'		Application Image	Optional
			…			
		'5F50' '##' 'xx...xx'			URI	Optional
		'5F45' '##' 'xx...xx'			Display Message	Optional
	'A2'	'##'	Application Group Head			Conditional[7]
		'4F' '##' 'xx...xx'			Group head AID	Mandatory
	'A3'	'##'	Application Group			Conditional[8]
		'4F' '##' 'xx...xx'			Group member’s AID	Mandatory
		…				
		'4F' '##' 'xx...xx'			Group member’s AID	Conditional
	'A4'	'10'	CREL Application AID List			Mandatory

[6] Required if the application is a standalone application or a group head.

[7] Required if this application is a member of a group. Mutually exclusive with 'A3'.

[8] Required if this application is a group head. Mutually exclusive with 'A2'.

Content						Presence
	'4F' '0E' '325041592E5359532E4444463031'				AID of PPSE	Mandatory
'A6'	'##'	Application Discretionary Data				Mandatory
		'BF0C'	'##'	FCI Data		Mandatory
			'61'	Directory Entry		Mandatory
				'4F' '##' 'xx...xx'	ADF Name	Mandatory
				'9F28' '##' 'xx...xx'	Kernel Identifier.	Optional
				'81' '01' 'xx'	Length of base AID	Optional
				…		
			…			
			'61'	Directory Entry		Conditional
				'4F' '##' 'xx...xx'	ADF Name	Mandatory
				'9F28' '##' 'xx...xx'	Kernel Identifier	Optional
				'81' '01' 'xx'	Length of base AID	Optional
				…		
		…				

A.1.1.1 Populating the GPCLRegistryEntry

If the information described above is provided to the contactless mobile application during personalization, the application must populate its **`GPCLRegistryEntry`** within the CRS in the following manner:

- Extract the following information from the buffer containing the personalized data, and setting each by invoking the **`setInfo()`** method.
  - The data from tag 'A6' (Application Discretionary Data) with an `info` parameter of `INFO_DISCRETIONARY_DATA`.
  - The data from tag '88' (Display Required Indicator) with an `info` parameter of `INFO_DISPLAY_REQUIREMENT.`
  - The data from tag '87' (Application Family Identifier) with an `info` parameter of `INFO_FAMILY_IDENTIFIER.`
  - The data from tag '6D' (Application Image Template) with an `info` parameter of `INFO_LOGO.`
  - The data from tag '5F50' (URI) with an `info` parameter of `INFO_URI.`
  - The data from tag '5F45' (Display Message) with an `info` parameter of `INFO_DISPLAY_MESSAGE.`
- If this application is intended to be a member of a group, as indicated by tag 'A2', extract the AID of the intended group head and provide it as a parameter on the invocation of the **`joinGroup()`** method.
- If this application is a group head, as indicated by tag 'A3', extract each AID listed under this tag and provide each separately as a parameter on the invocation of the **`addToGroupAuthorizationList()`** method.
- Extract the AID of the PPSE, as indicated by tag 'A4', and provide it as a parameter on the invocation of the **`addToCRELApplicationList()`** method.

Note that specifically for the PPSE implemented for a GlobalPlatform Secure Element, there are no contactless information or characteristics provided during installation or personalization.

A.1.2 Usage of the CRS Application

This section describes how an AAUI could potentially interface with the CRS Application.

A.1.2.1 Retrieve Contactless Applications and Characteristics

As described in section 7.2, the AAUI retrieves the information of the available contactless applications of all the Secure Elements present on a Mobile Device. The following describes how this is achieved if the Secure Element is a GlobalPlatform implementation.

A particular function of the CRS allows the AAUI to determine what changes, if any, have occurred regarding the contactless applications and their parameters. This allows the AAUI to keep its own record of the contactless applications and to retrieve information regarding only new contactless applications and/or those that have recently changed. Alternatively, the AAUI could by default always retrieve all information.

In either case, the first step is always to select the CRS application.

The SELECT command for the CRS is detailed in Table A.4.

Table A.4: CRS SELECT Command

Command header					Command Data
CLA	**INS**	**P1**	**P2**	**Lc**	**CRS AID**
'00'	'A4'	'04'	'00'	'09'	'A00000015143525300'
					Response Data
					FCI Template

Once the CRS has been selected, the AAUI can retrieve data from the CRS either based on the state of the applications and the CRS, or across all applications, as described in the following sections.

State-Based

If the AAUI keeps its own record of the contactless applications and parameters, it must also keep a record of the current state of each application and the state of the CRS itself. This will allow the AAUI to first check whether the CRS has changed in any way since the AAUI was last run, and if the state of the CRS has changed, to determine which contactless application parameters have changed or whether new contactless application parameters have been added to the CRS (for example, if a new contactless application has been added to the Secure Element).

The AAUI can use the Global Update Counter returned in the SELECT command response data to determine whether any of the information in the CRS has changed.

If the Global Update Counter matches the Update Counter stored by the AAUI, no changes have occurred since the AAUI last accessed the CRS. The AAUI can therefore present the stored contactless information to the consumer.

If the Global Update Counter does not match the Update Counter stored by the AAUI, the AAUI can either retrieve all the information or identify which contactless applications have changed as described hereafter. As specified by *[GPCARD]*, there are multiple ways of retrieving the needed information and the following is just one example. The AAUI can retrieve the Update Counter of all applications by issuing the GET STATUS command detailed in Table A.5. (For more detail on this command, refer to *[GPCARD]*, section 3.11.3.)

Table A.5: GET STATUS Command (Application Update Counter)

Command header					Command Data		
CLA	**INS**	**P1**	**P2**	**Lc**	**Search on: All AIDs**	**Return: AID/Update Counter**	
'80'	'F2'	'40'	'00'	'0D'	'4F' '00'	'5C' '01' '80'	
					Response Data		
					Application Related Data	**AID**	**Update Counter**
					'61##'	'4F' '##' 'xx…xx'	'80' '02' 'xxxx'
						…	…
						…	…
						'4F' '##' 'xx…xx'	'80' '02' 'xxxx'

If the Update Counter retrieved from the CRS for a particular application does not match the corresponding Update Counter stored by the AAUI, or if a new application is present in the list, the AAUI can then retrieve all, or a subset of, the information for that application by issuing the GET STATUS command. Table A.6 provides an example for retrieving all the contactless information for a particular application.

Table A.6: GET STATUS Command (Contactless Parameters – Single Application)

Command header					Command Data
CLA	**INS**	**P1**	**P2**	**Lc**	**Search on: Specific AID**
'80'	'F2'	'40'	'00'	'0#'	'4F' '##' 'xx…xx'
					Response Data
					See *[GPCARD]*.

Retrieve All

The AAUI can alternatively retrieve all, or a subset of, the information for all contactless application by issuing the GET STATUS command. Table A.7 provides an example in which a subset of the contactless information (Application Lifecycle State and priority indicator) is retrieved for all applications.

Table A.7: GET STATUS Command (Contactless Parameters – All Applications)

Command header					Command Data	
CLA	**INS**	**P1**	**P2**	**Lc**	**Search on: All Applications**	**Return: State/Priority**
'80'	'F2'	'40'	'00'	'02'	'4F' '00'	'5C' '03' '9F7081'
					Response Data	
					See *[GPCARD]*.	

A.1.2.2 Usage of CRS Data Elements

As described in section 7.3, the information retrieved from the CRS is used to present consumer-facing information related to the relevant contactless application to the consumer and to effectively manage the contactless application based on the choices made by the consumer.

The full contactless data returned by the CRS for each contactless application is formatted as detailed in *[GPCARD]*, Table 3-13. An AAUI may use this information in the following manner:

AID (tag '4F')

The AID identifies the contactless application on the Secure Element. The AAUI uses the AID to track the contactless applications and parameters and to identify changes to the contactless parameters. The AID is never presented to the consumer.

Application Discretionary Data (tag 'A6')

In the context of EMV, this data element provides data that is used by the AAUI to assist in managing the PPSE (External Mode) or used by the PPSE itself (Internal Mode). While other application-specific data may be present, the information relevant in this context is as listed in Table A.3 on page 62.

Notes:

- An application that indicates the PPSE as its CREL has at least one Directory Entry in the data object and may indicate subsequent Directory Entries if the application is a group head.
- Length of base AID may be present in the data object, but is not intended to be present within an FCI Proprietary Template populated to the PPSE.

  It is the responsibility of the AAUI (External Mode) or the PPSE (Internal Mode) first to strip from the template any directory entry that has the same base AID as a directory entry with a higher priority, and then to strip out the base AID (tag, length, and value) from each remaining directory entry, prior to populating the template to the PPSE.

  The rational 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, the lower priority applications can be removed from the list.

- While the priority indicator field is not present in each directory entry, it is the responsibility of the AAUI (External Mode) or the PPSE (Internal Mode) to insert the priority indicator (tag, length, and value) for each directory entry. The value for each priority is dependent on the priority order of the application.
- Apart from the behaviour described in the two preceding notes, all Directory Entry data objects are to be present in Directory Entries populated to the FCI Proprietary Template.

Application Family Identifier (tag '87')

The Application Family Identifier can be used to group certain applications together, indicate the application type, or exclude an application from those presented to the consumer. As examples, the AAUI may:

- Group payment, transit, loyalty, etc., applications together,
- Visibly differentiate how applications from different families are presented, or
- Choose not to present applications from certain families at all. That is, the AAUI could present payment and loyalty applications but not transit applications.

Application Lifecycle State (tag '9F70')

The Application Lifecycle State identifies the current state of the application according to the CRS.

This state is used to indicate the current state of the contactless application to the consumer and whether it is an application ready for use when presented to a contactless terminal. (Only applications that are ACTIVATED are accessible over the antenna interface.) The consumer will be able to manage the ACTIVATED/DEACTIVATED state of contactless applications.

Application Update Counter (tag '80')

The AAUI can use the Application Update Counter to determine whether any contactless information related to the application has changed.

CREL Application AID List (tag 'A4')

This data element indicates whether one or more Event Listeners are associated with the contactless application. In the context of EMV and for all EMV-based Contactless Mobile Payment applications, the PPSE is a CREL.

Display Control Template (tag '7F20')

The Display Control Template is relevant to group head applications or standalone applications only. If this data element is not present (and immaterial of whether or not it contains data), the AAUI does not present this contactless application to the consumer. It is an AAUI implementation-specific choice as to whether the AAUI uses the data returned in this template. That is, the AAUI could rely on data stored within the AAUI to present the contactless application to the consumer. Contactless applications that would not have a Display Control Template include the PPSE and any contactless application that is a group member under a group head application.

The Display Control Template may contain one or more of the following data elements:

- URI (tag '5F50') – A link to additional information regarding the contactless application.
- Application Image Template (tag '6D') –Contains details of a graphical image that can be associated with the application to assist the consumer in easily identifying the contactless application.
- Display Message (tag '5F45') – Descriptive text that can be associated with the application to assist the consumer in easily identifying the contactless application.

Display Required Indicator (tag '88')

This optional tag indicates whether this contactless application is capable of operating when the Mobile Device is not Switched On. The AAUI can present this information to the consumer so that the consumer is aware of what the behaviour of their contactless applications would be when their Mobile Device is not Switched On. If this tag is not present, the AAUI assumes that the application is capable of operation only when the Mobile Device is Switched On.

Group of Applications (tags 'A2' and 'A3')

These tags and values are conditional, relevant only if the application is a member of a group, and dependent on whether the application is a group head or a group member.

An application that is a group head is the only application in that group that has tag 'A3' – indicating the members within the group – and that the AAUI presents to the consumer. All the applications that are members of the group have tag 'A2', indicating the Application Group Head.

Management of the group head application is intended to affect all the contactless applications in the group. For example, if the consumer changes the state or priority of the group head application, the state or priority of all applications in the group are affected as well. The Application Group (tag 'A3') indicate the applications that are authorized to be part of this group but do not imply that they are necessarily present on the Secure Element (that is, they could be installed on the Secure Element at a later stage).

Policy Restricted Application(s) (tag 'A5')

This template indicates that when this contactless application is in an active state, the identified application(s) are to be deactivated. If an application is a CREL or a group head application, this also applies to all applications that rely on the CREL or are members of the group. The AAUI does not present this information to the consumer but may use it to manage and inform the consumer of conflicts (see section 7.4.1).

A.1.2.3 GlobalPlatform Specific – CRS Setting States

As per section 7.4, the AAUI is responsible for updating the relevant SECM entities depending on the choices made by the consumer.

The AAUI can modify the contactless characteristics for a single application or multiple applications by issuing the SET STATUS Command detailed in Table A.8. (For more detail on this command refer to *[GPCARD]*, section 3.11.4.)

Table A.8: SET STATUS Command (Contactless Parameters – Single Application)

Command header					Command Data
CLA	**INS**	**P1**	**P2**	**Lc**	**Application AID**
'80'	'F0'	'01'	'xx'	'0x'	'4F' '##' 'xx…xx'
					Response Data
					See *[GPCARD]*.

If the AAUI is setting the state of an application to ACTIVATED, the CRS will indicate whether or not the operation was successful; if it was unsuccessful, the CRS will provide a list of conflicting applications. As per section 7.4.1, the AAUI is responsible for managing the reported conflicts.

A.1.3 Usage of the CRS in Internal Mode

This section details the manner in which a PPSE configured for Internal Mode makes use of the CRS API.

The PPSE must implement and expose the **`CRELApplication`** interface.

The **`notifyCLEvent()`** method provides a means for the OPEN to inform 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 the Internal Mode.

Functional Behaviour

Behaviour

- On receipt of a notification that the contactless state of an application has been set to ACTIVATED, the PPSE must populate the FCI with the Directory Entry information of all its active contactless application(s).

  This notification would be the **`notifyCLEvent()`** indicating the target application with an `event` parameter of `EVENT_ACTIVATED`.

  The PPSE retrieves the Directory Entry information of each standalone or group head application from the `INFO_DISCRETIONARY_DATA` of the target **`GPCLRegistryEntry`**. For each retrieved Directory Entry, the PPSE removes the Length of Base AID TLV and includes a Priority TLV. If there are multiple Directory Entries, the first entry is given the highest priority '01' and each successive entry is given a continually lesser priority.

- If the PPSE is capable of determining whether the Mobile Device is Switched On, and if any of its active applications require that the Mobile Device be Switched On in order to process a contactless payment transaction, then the PPSE must build a separate FCI excluding such applications; the tailored FCI will be returned when the Mobile Device is not Switched On.

  This information is retrieved from the `INFO_DISPLAY_REQUIREMENT` of the target **`GPCLRegistryEntry`**.

  - A value of zero indicates that the Directory Entry 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 is populated to both the FCI to be returned when the Mobile Device is Switched On and the tailored FCI to be returned when the Mobile Device is not Switched On.

Behaviour

- On receipt of a notification that a previously activated application is no longer activated, the PPSE must remove the directory information from the FCI.

  This notification would be 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 should behave as if it were not present.

A.1.4 Contactless Mobile Payment Application

This section describes an application's behaviour primarily for the case where the CRS APDU interface is not supported by the GlobalPlatform implementation – although it is possible to use this same functionality on an implementation when the CRS APDU is supported. In either case, the PPSE must be configured to support Internal Mode.

In order for an application to set its own contactless state, it must be installed with the Contactless Self-Activation privilege as defined in *[GPCARD]*, Table 7-1: Privileges.

The contactless application will inform the CRS whenever its own contactless states change using the **`setCLState()`** method. The implementer of the AAUI determines how a Contactless Mobile Payment Application is made aware of a contactless state change. However, EMVCo has defined the SET STATUS command (see Annex C), which provides an interoperable mechanism for an AAUI to indicate a contactless state change to a Contactless Mobile Payment application.

Contactless Mobile Payment Application Usage of GlobalPlatform APIs

Anticipated Behaviour
• If the application has been instructed to change its state to activated, the application will invoke the **`setCLState()`** method with a parameter of `STATE_CL_ACTIVATED`. • If the **`setCLState()`** method returns a value of `STATE_CL_DEACTIVATED`, the application can retrieve the AID of each conflicting application by invoking the **`getNextConflictingApplication()`** method with an **`oEntry`** parameter of `NULL`. • If the application has been instructed to change its state to deactivated, the application will invoke the **`setCLState()`** method with a parameter of `STATE_CL_DEACTIVATED`. • If the application has been instructed to assign itself the Override Priority, the application will invoke the **`setVolatilePriority()`** method with an **`oEntry`** parameter of this application. • If the application has been instructed to reset its Override Priority, the application will invoke the **`setVolatilePriority()`** method with an **`oEntry`** parameter of `NULL`.

Annex B PPSE Functionality and Requirements

This annex details the functionality of a PPSE on a Mobile Device as well as some specific implementations of that PPSE. As there is more than one option for how to ensure that a Mobile Device responds with the consumer's choice of accessible application over the antenna interface, this annex will detail the various implementation choices. At the time of publication of this document, both choices specified (Internal and External Mode) assume the presence of the PPSE on a Secure Element of the Mobile Device.

B.1 PPSE Functionality

The main purpose of any PPSE is to return an 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 list of directory entries, identifying the following information applicable to the entity selecting the PPSE (typically a contactless payment terminal):

- A product or products supported by the Mobile Device; that is, contactless applications available for selection (by AID) and use by the contactless payment terminal
- The priority of each application; that is, the lower the value, the higher the priority[9]
- The specific application underpinning the product; that is, the terminal application used to interact with this application on the Mobile Device
- Other application-specific data

This specification focuses on the mechanisms used to populate the PPSE with directory entries and how to indicate which directory entry/entries within the PPSE are, at a given point in time, returned to the contactless terminal. Two mechanisms are defined for achieving this: External Mode and Internal Mode. An implementation may support either mode or both. If both are supported, the implementation must allow an AAUI to indicate which mode it will be using.

All EMVCo contactless products 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 contactless interface, personalized with an Issuer-defined prioritization of each payment application.

[9] Except that priority '0' means no priority assigned.

For Mobile Devices, the PPSE shall contain additional functionality that allows the application(s) that could be returned to the contactless terminal to be dynamically managed by the consumer through an AAUI. This mobile-specific functionality allows an AAUI to control the SELECT command response depending on the choices of the consumer.

This functionality allows for a single application or multiple applications to be visible in the SELECT command response depending on choices made by the consumer. Additionally, and again depending on choices made by the consumer, the SELECT command response could depend on the PPSE's assumption related to whether the Mobile Device is Switched On or not at the time it is presented to a contactless payment terminal.

Internal Mode is intended primarily for use in single Secure Element environments and relies on an SECM that provides a means for the PPSE to determine which contactless applications are active. The PPSE uses information related to these active applications to build the SELECT command response to be returned to the contactless terminal. This same SECM must allow an AAUI to retrieve contactless application information and to set which contactless applications are active. As an alternative, if the SECM does not provide an interface to the AAUI, the contactless applications themselves may set their own contactless states. (See Annex C for an example of an interoperable command of managing application activation.)

External Mode is used in single and multiple Secure Element environments and relies on an SECM that allows an AAUI to retrieve contactless application information and to set which contactless applications are active. The AAUI provides the PPSE with the SELECT command responses to be returned to the contactless terminal.

B.2 General Functional Requirements

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

Requirements – General (Internal and External Modes)	
B.2.1.1	The SELECT command SHALL be accessible over the device interface and over the antenna interface.
B.2.1.2	The GET TEMPLATE command SHALL be accessible over the device interface and SHALL NOT be accessible over the antenna interface.
B.2.1.3	The SET MODE command MAY be supported. **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.

Requirements – General (External Mode)	
B.2.1.4	The PUT TEMPLATE command SHALL be accessible over the device interface and SHALL NOT be accessible over the antenna interface.

Requirements – General (Internal Mode)	
B.2.1.5	The PPSE SHALL be capable of retrieving the directory entry information of the Secure Element's active applications from an SECM.

B.3 Secure Element Implementation

The following sections describe the functionality and requirements of a PPSE implementation for a Secure Element.

B.3.1 SELECT Command

Command Data

Table B.9: SELECT Command Message

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

Functional Requirements

B.3.1.1 Internal and External Mode

Requirements B.3.1.1 to B.3.1.3 apply to the SELECT command when received over the device interface only and apply to both Internal and External Modes.

Requirements – SELECT Command – Device Interface	
B.3.1.1	**If** a SELECT command is received over the device interface, **then** the PPSE response, constructed as specified in Table B.10 on page 86, SHALL be returned.
B.3.1.2	**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'.
B.3.1.3	**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'.

B.3.1.2 External Mode

When the PPSE is configured to operate in External Mode:

- Requirements B.3.2.4 to B.3.2.9 apply to the SELECT command when received over the antenna interface only.
- Requirements B.3.2.4 to B.3.2.7 (in the order listed) apply when the Mobile Device is Switched On or when the PPSE is incapable of determining whether the Mobile Device is Switched On.

Requirements – SELECT Command – Antenna Interface / Mobile Device Switched On	
B.3.2.4	**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 B.11 on page 87, SHALL be returned.
B.3.2.5	**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.
B.3.2.6	**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.

Requirements – SELECT Command – Antenna Interface / Mobile Device Switched On

B.3.2.7 **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].
- No subsequent PUT TEMPLATE command with a Usage parameter of '04' [Cancel override] or '05' [Mandatory data only] or '06' [Hide] has been received.
- The override has not been cancelled due to the Mobile Device being switched off (see B.3.2.9).

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.

- Requirements B.3.2.8 to B.3.2.9 (in the order listed) apply when the PPSE is capable of determining whether the Mobile Device is not Switched On and it is not.

Requirements – SELECT Command – Antenna Interface / Mobile Device not Switched On

B.3.2.8 **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 B.11 on page 87, SHALL be returned.

Else:

- **If** no [Device not Switched On] FCI is currently configured,
  then a response of '6A82' [Application not found] SHALL 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] SHALL be returned.

B.3.2.9 **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 FCI SHALL be cancelled.

B.3.1.3 Internal Mode

When the PPSE is configured to operate in Internal Mode:

- Requirements B.3.3.10 to B.3.3.13 apply to the SELECT command when received over the antenna interface only.
- Requirements B.3.3.10 and B.3.3.11 apply when the Mobile Device is Switched On, or when the PPSE is incapable of determining whether or not the Mobile Device is Switched On.

Requirements – SELECT Command – Antenna Interface / Mobile Device Switched On	
B.3.3.10	**If** no contactless mobile payment application has indicated to the PPSE that it is in the active state, **then** a response of '6A82' [Application not found] SHALL be returned.
B.3.3.11	**If** one or more contactless payment applications have indicated to the PPSE that they are in the active state, **then** the PPSE response shall contain the directory entries of the active applications.

- Requirements B.3.3.12 and B.3.3.13 apply when the PPSE is capable of determining whether the Mobile Device is Switched On and it is not.

Requirements – SELECT Command – Antenna Interface / Mobile Device not Switched On

B.3.3.12 **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,

Then a response of '6A82' [application not found] SHALL be returned.

B.3.3.13 **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,
then the PPSE response returned shall contain the directory entries of these active applications.

Response Data

The PPSE response depends on whether the PPSE is being selected by the AAUI or over the antenna interface.

- The response to a SELECT command received from the AAUI over the device interface is coded as per Table B.10.

Table B.10: PPSE Response over the Device Interface

Tag	Value			Presence
'6F'	FCI Template			M
	'84'	‘2PAY.SYS.DDF01’		M
	'A5'	FCI Proprietary Template		M
		'9F08'	'10' – Version	M
		'89'	Current Mode: • '01' – External • '02' – Internal	M

- The response to a SELECT command received over the antenna interface is coded:
  - as per Table B.11 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
  - as per Table B.12 if at least one EMV-based contactless application is to be accessible over the antenna interface.

Table B.11: PPSE Response Without an FCI Proprietary Template

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

Table B.12: 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
				'9F28' Kernel Identifier	C
				...	O
			...		
			'61'	Directory Entry	O
				'4F' DF Name (AID)	O
				'50' Application label	O
				'87' Priority indicator	O
				'9F28' Kernel Identifier	O
				...	O

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

Table B.13: 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

B.3.2 PUT TEMPLATE Command

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

Command Data

Table B.14: PUT TEMPLATE Command Message

Code	Value
CLA	'80'
INS	'D2'
P1	Usage – see Table B.15
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 B.15: PUT TEMPLATE Command P1 Usage

Code	Meaning
'01'	Device Switched On no override
'02'	Device not Switched On
'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 B.16.

Table B.16: 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
			'9F28'	Kernel Identifier	C
			...		O
		...			O
		'61'	Directory Entry		O
			'4F'	DF Name (AID)	M[10]
			'50'	Application label	O
			'87'	Priority indicator	C
			'9F28'	Kernel Identifier	C
			...		O

Functional Requirements

Requirements – PUT TEMPLATE Command	
B.3.1.14	**If** P1 of the PUT TEMPLATE command 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.
B.3.1.15	**If** a PUT TEMPLATE command is received over the antenna interface, **then** a response of '6985' SHALL be returned.

[10] Only relevant if Directory Entry is present.

Requirements – PUT TEMPLATE Command	
B.3.1.16	**If** the PPSE is not currently configured to operate in External Mode, **then** a response of '6985' SHALL be returned.
B.3.1.17	**If** the template received in the command data is not formatted as per Table B.16, **then** a response of '6984' SHALL be returned.
B.3.1.18	**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 the device is in full power mode (that is, Switched On) and no override is currently set.
B.3.1.19	**If** P1 contains a value of '02' [Device not Switched On], **and** the PPSE is not capable of determining whether the device is Switched On or not, **then** a response of '6985' SHALL be returned.
B.3.1.20	**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 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 the device is not Switched On.
B.3.1.21	**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) when the device is Switched On. (This FCI is returned over the antenna interface until the override is cancelled.)
B.3.1.22	**If** P1 contains a value of '04' [Cancel override], **then** the current override, if any, SHALL be disabled.

Requirements – PUT TEMPLATE Command	
B.3.1.23	**If** P1 contains a value of '05' [Mandatory data only], **then** only the DF Name within the FCI Template (see Table B.11 on page 87) SHALL be returned (as a response to the SELECT command over the antenna interface), whether the device is Switched On or not.
B.3.1.24	**If** P1 contains a value of '06' [Hide], **then** the PPSE SHALL behave as if it were not present.
B.3.1.25	**If** command data contains an FCI Proprietary Template, **then** the length field of the 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.

Response Data

The response Status Word may contain one of the values shown in Table B.17.

Table B.17: 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

B.3.3 GET TEMPLATE Command

The GET TEMPLATE command enables the AAUI 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.

Command Data

Table B.18: GET TEMPLATE Command Message

Code	Value
CLA	'80'
INS	'D4'
P1	Usage; see Table B.19
P2	'00'
Lc	'00'
Le	'00'

Usage (P1)

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

Table B.19: GET TEMPLATE Command P1 Usage

Code	Meaning
'01'	Device Switched On no override
'02'	Device not Switched On
'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.

Functional Requirements

Requirements – GET TEMPLATE Command	
B.3.1.26	**If** P1 of the GET TEMPLATE command 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.
B.3.1.27	**If** the GET TEMPLATE command is received over the antenna interface, **then** a response of '6985' SHALL be returned.
B.3.1.28	**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.
B.3.1.29	**If** P1 contains a value of '02' [Device not Switched On], **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 not Switched On.
B.3.1.30	**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 B.11 on page 87).
B.3.1.31	**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.
B.3.1.32	**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.[11]

[11] 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.

Response Data

The response command data is formatted as defined in Table B.11 on page 87 or Table B.12 on page 87.

The response Status Word may contain one of the values shown in Table B.20.

Table B.20: GET TEMPLATE 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

B.3.4 SET MODE Command

The SET MODE command provides a means for an application on the Mobile Device (an AAUI) to set the mode (Internal or External) of the PPSE.

Command Data

Table B.21: SET MODE Command Message

Code	Value
CLA	'80'
INS	'D6'
P1	Mode – see Table B.22
P2	'00'
Lc	'00'
Le	'00'

Mode (P1)

This parameter indicates the mode of operation of the PPSE.

Table B.22: SET MODE Command P1 Mode

Code	Meaning
'01'	EXTERNAL
'02'	INTERNAL

Functional Requirements

Requirements – SET MODE Command	
B.3.1.33	**If** P1 of the SET MODE command contains a value other than '01' or '02', **then** a response of '6A86' SHALL be returned.
B.3.1.34	**If** the SET MODE command is received over the antenna interface, **then** a response of '6985' SHALL be returned.
B.3.1.35	**If** P1 contains a value of '01' [EXTERNAL], and External Mode is not supported by the implementation, **then** a response of '6985' SHALL be returned.
B.3.1.36	**If** P1 contains a value of '02' [INTERNAL], and Internal Mode is not supported by the implementation, **then** a response of '6985' SHALL be returned.
B.3.1.37	Following the setting of the mode, any current FCI Templates SHALL be reset.

Response Data

The response Status Word may contain one of the values shown in Table B.23.

Table B.23: 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

Annex C Alternate Activation Mechanism in Absence of SECM Interface

This annex details an interoperable alternative command for managing application activation. This command is intended for single Secure Element environments where the SECM does not provide an interface that the AAUI can use and it is therefore necessary to manage the state of contactless applications through the applications themselves. The ability of an application to support this command depends on the platform on which the application is being hosted, any necessary privileges, and the SECM employed by the platform. Note that *[GPCARD]* does not currently support the full functionality of this command.

C.1 SET STATUS Command

The following SET STATUS command enables an AAUI to indicate a contactless state change to the contactless application itself.

Command Data

Table C.24: SET STATUS Command Message

Code	Value
CLA	'8x'
INS	'F0'
P1	'01' – Availability State [over the antenna interface]
	'02' – Activate and Set Priority Order [for Application Selection]
P2	State
Lc	'xx'
Data	Command Template
Le	'00'

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 as per Table C.25.

Table C.25: 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 Order], this parameter is used to set the priority order of this application for a single imminent transaction or for future transactions. The priority order is set/reset for this contactless application as per Table C.26.

Table C.26: SET STATUS Command P2 if P1 is '02'

Code	Meaning
'01'	Assign Highest Priority
'81'	Assign Lowest Priority
'02'	Assign Override Priority
'82'	Reset Override Priority

Command Data

The command data contains a Template that is either empty or contains application-specific TLV-coded data objects. For example, an authentication TLV coded data object.

Response Data

If any currently active application conflicts with this application, then the Response Data contains a Template containing a data object list containing the AIDs of the conflicting applications, as shown in Table C.27.

If no currently active application conflicts with this application, then the Response Data contains an empty Template.

Table C.27: SET STATUS Response Data

Value				Presence
'61'	Application Template			M
	'A0'	List of Conflicting Applications		O
		'4F'	AID of first or only conflicting application	O
		…		
		'4F'	AID of final conflicting application	O

Functional Behaviour of the Environment

Anticipated Behaviour

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

- If P2 contains a value of '01' [ACTIVATED], this application should become active over the antenna interface and any currently active application should become inactive.
- 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 Order], then the following behaviour is anticipated:

- If P2 contains a value of '01' [Assign Highest Priority], this application should become active over the antenna interface and have the highest priority of the currently active applications. That is, the current highest priority application will now be the second highest priority application, and so on.
- If P2 contains a value of '81' [Assign Lowest Priority], this application should become active over the antenna interface and have the lowest priority of the currently active applications; that is, lower than the current lowest priority application.
- 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.

The response Status Word may contain one of the values shown in Table C.28.

Table C.28: 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'	Warning	Application not activated
		'9000'	Normal	Successful processing

Annex D Glossary

This is a glossary of terms and abbreviations used in this specification. Additional concepts are defined in section 3.1.

AAUI	Application Activation User Interface
Accessibility State	Whether the application is immediately accessible over the antenna interface.
AID	Application Identifier
ADF	Application Definition File
Always On	A state in which a contactless application on a Mobile Device is accessible to a contactless terminal as long as the Mobile Device is capable of communicating over the antenna interface. For more information, see section 3.1.3.
APDU	Application Protocol Data Unit
Application Activation User Interface	A user interface application on a mobile device that enables the consumer to manage the use of their contactless applications.
C	Conditional
CCPS	Contactless Communication Protocol Specification
Consumer Facing	Describes a contactless application about which information may be presented to the consumer; excludes, e.g. the PPSE and any contactless application that is a group member but not the group head or group owner.
Contactless Mobile Payment	Integration of EMV-based contactless payment technology in mobile devices.
Contactless Mobile Payment Application	An application that is hosted in a Secure Element and that performs information exchange and processing needed to perform a contactless mobile payment transaction.

Contactless Module	A module within a mobile device providing a contactless interface compatible with EMV Contactless Communication Protocol Specification *[CCPS]*.
Contactless Payment Terminal	A contactless reader conforming to EMV Contactless Communication Protocol Specification *[CCPS]* and compliant with EMV specifications related to the use of the PPSE that is capable of conducting a payment transaction with a Contactless Mobile Payment Application.
Contactless Registry Service	A GlobalPlatform SECM service for managing the contactless applications on a Secure Element.
CREL	Contactless Registry Event Listener
CRS	Contactless Registry Service
EMV	A global standard for credit and debit payment cards based on chip card technology. The EMV Integrated Circuit Card Specifications for Payment Systems are developed and maintained by EMVCo.
EMVCo	EMVCo LLC is the organization of payment systems that manages, maintains, and enhances the EMV Integrated Circuit Card Specifications for chip-based payment cards and acceptance devices, including point of sale (POS) terminals and ATMs. EMVCo also establishes and administers testing and approval processes to evaluate compliance with the EMV Specifications. EMVCo is currently owned by American Express, JCB, MasterCard, and Visa.
External Mode	The mode in which the AAUI provides the PPSE with the details of the active applications that will be presented to a contactless payment terminal. For more information, see section 3.1.4.
FCI	File Control Information
Group	A set of contactless applications consisting of a group head/owner application and one or more member applications. For more information, see section 3.1.2.

Handset	A type of mobile device, specifically a mobile phone handset.
Internal Mode	The mode in which the PPSE itself collects details of the active applications and builds the data to be presented to the contactless payment terminal. For more information, see section 3.1.4.
M	Mandatory
Mobile Device	A portable electronic device with contactless and wide area communication capabilities. Mobile devices include mobile phones and other consumer electronic devices such as suitably equipped PDA.
Mode	The manner in which the PPSE receives and builds the information that will be provided to a contactless payment terminal. See *External Mode* and *Internal Mode*. For more information, see section 3.1.4.
Near Field Communication	A short range contactless proximity technology based on ISO/IEC 18092, which provides for ISO/IEC 14443 compatible communications and enables wireless devices to communicate with each other when brought into close range.
O	Optional
PPSE	Proximity Payment System Environment
Proximity Payment System Environment	A mechanism for presenting the contactless applications available for conducting a transaction to a Contactless Payment Terminal. The PPSE is the first application selected by a Contactless Payment Terminal, and based on the information provided by the PPSE, the terminal uses the highest priority application it supports to process a contactless payment.
Power State	Whether or not the Mobile Device is Switched On.
SECM	Secure Element Contactless Management

Secure Element	A tamper resistant module in a mobile device capable of hosting applications in a secure manner. A Secure Element may be an integral part of the mobile device, or may be a removable element which is inserted into the mobile device for use.
Secure Element Contactless Management	A scheme employed by a Secure Element to manage the contactless applications thereon. The scheme could vary depending on the Secure Element implementation.
SIM	Subscriber Identity Module
Single Wire Protocol	The electrical and protocol interface for connecting a UICC to a contactless module. Defined by ETSI TS 102 613 *[SWP]*.
Subscriber Identity Module	A smart card that securely stores the key identifying a mobile phone service subscriber, as well as subscription information, phone numbers, preferences, etc. It can also be used to securely store a contactless mobile payment application.
Switched On	A state in which the Mobile Device is powered up and the user interface is available for use. For more information, see section 3.1.1.
SWP	Single Wire Protocol
TLV	Tag, Length, Value
UICC	Universal Integrated Circuit Card
Universal Integrated Circuit Card	The physical integrated circuit card which hosts the USIM and other applications.
User Interface	Input and output components on a mobile device, for example, display, keyboard and touch screen.

<< END OF DOCUMENT >>