Mobile MasterCard® PayPass™
User Interface Application Design Guide

User Experience, Use Cases, Screen Layouts and Design
This document is designed to help you create either standalone User Interface Applications that enable cardholders to setup and use MasterCard® PayPass™ on their Mobile Device, or to integrate PayPass card management into existing mobile banking applications.

The overall proposition is referred to as Mobile MasterCard PayPass - the implementation of PayPass technology on Mobile Devices.

At the core of any such implementation is the Payment Application which must reside within a secure memory area on the mobile device (e.g. Secure UICC, embedded Secure Element or other form of secure chip). This Payment Application must conform to a valid MasterCard Technical Specification in order to be able to communicate with PayPass enabled contactless readers at merchant locations (e.g. MasterCard PayPass MagStripe, MasterCard PayPass M/Chip 4 or Mobile MasterCard PayPass M/Chip 4).

User Interface Applications enable additional functionality such as high value contactless transactions, Over-The-Air (OTA) Counter Reset, multiple card (account) management and increased end-user (or cardholder) control of their cards, and as such are an important part of any deployment.

This document describes a core set of functions that such a User Interface Application can provide, with a particular focus on functions that are possible with Payment Applications that conform to the Mobile MasterCard PayPass M/Chip 4 Technical Specifications.

There are many possible use cases that can be implemented in User Interface Applications used in the context of Mobile MasterCard PayPass implementations. This document focuses on the most common use cases. The use cases defined in this document follow a user-centred approach throughout, aiming to identify the best practice methods for guiding users through setup, use and management processes.

Notes:
The flows and screen designs in this document are provided for guidance purposes only and do not constitute a set of rules or standards that must be adhered to. The formal requirements for User Interface Applications are covered in [Mobile MasterCard PayPass User Interface Application Requirements] and [Mobile MasterCard PayPass TSM Functional Requirements] which are both available from www.mastercard-mobilepartner.com. The screen designs in this document are an example of how a User Interface Application can be designed in compliance with these requirements. All branding must comply with [MasterCard PayPass Branding Standards] and where applicable [Maestro PayPass Branding Standards] which are available to all PayPass and Mobile MasterCard PayPass licensees. Implementation of this document requires a separate license from MasterCard, as specified in [Mobile MasterCard PayPass User Interface Application Requirements].
How to use this document

There are four sections in this document that describe the use cases and give guidance on the User Interface Application flow and design - these are:

**Section 3 Core functionality**
This section focuses on the most important functions where the User Interface Application will be required:
- Installation & Activation
- Low Value Payments
- High Value Payments
Each of the use cases in this section is also described by means of an icon-based flow diagram to highlight the key steps in the process.

**Section 4 Extended functionality**
This section focuses on the additional functions that a User Interface Application may need to better support frequent use cases that a cardholder may expect from their mobile payment enabled phone:
- Adding a new card
- Choosing to pay with other cards
- Reviewing card and transaction details

**Section 5 Settings & setup functionality**
This section focuses on functions related to the ongoing management and configuration of any payment application through the User Interface Application:
- Changing mPIN
- Setting a Default Card
- Responding to a Counter Reset request
Each of these three sections includes an icon-based flow diagram and a more detailed wireframe-based flow diagram.

**Section 6 Detailed screen designs**
This section contains examples of screen designs for all of the use cases described in the preceding three sections.
Use case Legend

The icons used in the flow diagrams in section 3 (Core functionality) are defined as follows:

USER ACTIONS

UI APPLICATION COMMUNICATION

PAYMENT TERMINAL FEEDBACK

CONTENTS

GLOBAL ICONS

Annotations are indicated by circled numbers at relevant locations in flow diagrams and screen designs. Explanations relating to each of the numbers is presented in the correspondingly numbered list at the bottom of each page.
Core functionality

This section includes the first-time setup and typical usage scenarios of Mobile MasterCard® PayPass™.

This represents the core functionality of any Mobile MasterCard PayPass implementation.

There are various ways of provisioning, personalizing and managing MasterCard Payment Applications on Mobile Devices. A more extensive list can be found in Appendix A.

For the purposes of this document, only two of these have been chosen to show how the flow and screens can be designed. The screens used in these two flows can easily be transferred to the remaining flows.

1. Full OTA without Activation (Over The Air download of Personalization Proxy or Agent and Payment Application, followed by Personalization based on a Verification Code, no further Activation sequence required)

2. UI OTA with Activation (Over The Air download of User Interface Application - acting as Activation Proxy or Agent - followed by Activation sequence)

Annotations

1. A differentiation is made between the Verification Process (usually an integral part of the Provisioning and or Personalization process) and the Activation process (which is typically applied to a Payment Application or account that is already personalized).

2. The User Interface Applications that are described as acting as Personalization Proxies or Agents, are the type of UI Application that facilitate the setup of a secure connection between the Secure Element and the issuer host, either directly or via a Trusted Service Manager, in order to enable the Personalization of cardholder data into the Payment Application. Their functional scope may also extend to the actual Provisioning of the Payment Application and in life management of the Payment Application once personalized and deployed.
Full OTA Installation and first time use - flow diagram

Full OTA no Activation

The user downloads the User Interface and Payment Applications over the air and confirms they are the valid cardholder by entering a verification code. The application is installed with the card (account) already in an active state. As the verification mechanism has been implemented no further activation is required.

Annotations

1. The standard approach for the verification process is to use some form of code entry prior to the personalization sequence (as shown here). Please refer to the Mobile MasterCard PayPass TSM Functional Requirements for further guidance.

2. When the verification process has failed (for example, due to multiple consecutive incorrect code entries) an appropriate message should be displayed informing the cardholder that the process cannot be completed and advising how to resolve the problem.

3. The user may not wish to set the new card as Default, in which case the card will be made available in the list of alternative cards within the UI once the setup is complete.
Full OTA Installation and first time use - screen flow

1 How to use this document
1.1 Use case legend
2 Propositions to the user and to the card issuer
3 Core functionality
3.1 Installation and activation process
3.2 Low Value Transaction
3.3 High Value Transaction
4 Extended functionality
4.1 Adding a new card
4.2 Choosing to pay with an alternative card, one time only
4.3 Viewing card details and transaction history
5 Settings & setup functionality
5.1 Changing mPIN
5.2 Setting a Default Card and preferred card
5.3 Responding to a Counter Reset request
6 Example graphic design for interface elements
7 Appendix A
8 Appendix B

Full OTA no Activation

This scenario covers the download and installation of a User Interface Application and Payment Application followed by Personalization with Verification Code.

Annotations

1. It is possible to download the User Interface Application first and the Payment Application after the Verification step. Alternatively both the User Interface Application and Payment Application could be downloaded initially, with the Personalization being dependent on the Verification step.
2. Depending on the TSM or Issuer preference, verification codes may be generated by the TSM, the Issuer or the cardholder. Various channels can be used to provide the Verification Code to the cardholder in order for them to verify they are the intended cardholder for OTA personalization including online, telephone banking or PIN-mailer type process.
UI OTA with Activation

The Payment Application is pre-installed and already personalized on the Secure Element. The user downloads the User Interface Application for a specific issuer Over The Air and confirms they are the valid cardholder by completing an activation process that uses a unique code (similar to the Verification Code entry process for personalization). This process is well suited for the issuance of new pre-paid accounts or for streamlining the deployment process of mobile instances of existing cards by making use of MasterCard’s mapping service (whereby issuers can have new accounts mapped to existing card accounts, thus removing the need to deploy new accounts Over The Air).

Annotations
1. There are various options for an Activation Process. This example is based on a process where the PIN change process is used as the verification step to activate the Payment Application so that it can be used for payments.
2. The user may not wish to set the new card as Default, in which case the card will be made available in the list of alternative cards within the UI once the setup is complete.
OTA Installation of UI with Activation and first time use - screen flow

UI OTA with Activation

This scenario covers the download and installation of a User Interface Application and the subsequent activation of the Payment Application.

User clicks on a link in sms, e-mail or on the web
User downloads the User Interface Application

User launches User Interface Application
Introductory text to the application

User touches to initiate Activation process

Welcome to PayPass
To use PayPass, you need to activate your cards.
Touch Next to set up.

My Wallet
AnyBank
**** **** **** 5467
Mr John Smith

This card needs activating
Touch here to activate

My Wallet

Congratulations on activating your card
OK

The card is activated.

Annotations

1. The Activation sequence will vary depending on the mechanism chosen by the issuer. Other common options include the entry of an Activation Code within the User Interface Application in order to make the Payment Application selectable.

©2011 MasterCard. All rights reserved.
This diagram shows an overview of the typical Low Value Transaction process for both online and offline configurations.

Low Value Transactions in offline environments can also be configured to work in two further ways in addition to the typical flow shown below (depending on issuer configuration of the Payment Application).

The three configuration options for offline therefore are:

1. Simple Tap & Go - in this scenario the cardholder simply taps the device on the Payment Terminal and as long as there is an active default Payment Application in the Secure Element, that card will be used to perform the transaction and complete the payment. This configuration is closest to the standard configuration of other PayPass devices (such as PayPass enabled cards or mobile Tags).

2. Pre-mPIN - in this scenario the cardholder is required to enter their mPIN (Offline PIN) via the User Interface Application before presenting their device for payment, in order for the Payment Application to be able to respond to the Payment Terminal.

3. Pre-Acknowledgement - in this scenario the cardholder is required to "Acknowledge" a transaction, or more specifically "enable" the Payment Application to respond to the Payment Terminal through a simple interaction via the User Interface Application, before placing the device on the Payment Terminal to make a payment.

All three of these scenarios are covered in the wireframes for Low Value Transactions.

Activity above the central black line indicates User Interface Application interaction and below the central black line indicates Payment Terminal interaction.

Annotations

1. It is possible to configure the Payment Application such that the cardholder is required to pre-acknowledge a transaction or alternatively enter their mPIN prior to any transaction. This step would need to be completed before the cardholder taps the phone on the Payment Terminal. This flow does not show these variations on the Low Value Transaction process, but the subsequent wireframes do show these options.

2. Depending on the cause of the failure a relevant error message should be displayed by the User Interface Application.

3. Payment Applications that are configured to require online authorization always, will only work on online capable terminals and will require the terminal to go online for every payment.
This diagram shows an overview of the Low Value Transaction process.

Optional “Pre-mPIN” and “Pre-Acknowledgement” configurations

1. The main part of this use case is based on the scenario where a Default Card is set, which is then automatically used when the cardholder presents the Mobile Device to make the payment.
2. The payment may fail if no Default Card is set, although other reasons could also cause a failure (e.g., if the card is blocked). In such cases the customer may be able to use another card that is set up on their mobile device.
3. It is also possible to configure the Payment Application such that it requires the mPIN to be entered by the user before every transaction (including Low Value Transactions), in which case the user will need to open the User Interface Application and enter the mPIN for the relevant card before tapping the handset on the Payment Terminal.
4. Alternatively in some cases the Issuer may chose to configure the Payment Application such that every single transaction requires a simple “Pre-Acknowledgement” for Low Value Transactions (utilizing a function within the Payment Application which requires to user to “enable” the Payment Application to perform a transaction prior to every payment. This option does not require the user to enter an mPIN. An example of the “Pre-Acknowledge” scenario is included in the wireframes for “Choosing to pay with an alternative card” on page 18.

Annotations

Note that the mPIN is not stored on the Mobile Device or any other device, and is only available to the Payment Application during the payment flow if an EMV transaction is taking place.
This diagram shows an overview of the High Value Transaction process (using mPIN).

This is a transaction that exceeds the Cardholder Verification Method limit (CVM limit), and therefore requires cardholder verification to enable the transaction to complete. This flow shows the use of an mPIN (the offline mobile PIN) which is entered on the keypad of the Mobile Device.

Above the central black line shows User Interface Application interaction. Below the central black line shows Payment Terminal interaction.

Annotations

1. Depending on the cause of the failure a relevant error message should be displayed by the User Interface Application.
2. As shown in the Low Value Transaction flow, it is also possible to configure the Payment Application such that the cardholder can enter their mPIN prior to any transaction, in which case only one tap would be required. This step would therefore take place prior to the first tap shown in this diagram.
This diagram shows an overview of the High Value Transaction process (using Online PIN).

This is a transaction that exceeds the Cardholder Verification Method limit (CVM limit), and therefore requires cardholder verification to enable the transaction to complete. This flow shows the use of an Online PIN, which is entered on the PIN Entry Device at the Point of Sale.

Above the central black line shows User Interface Application interaction. Below the central black line shows Payment Terminal interaction.

Annotations
1. Depending on the cause of the failure a relevant error message should be displayed by the User Interface Application.
This diagram shows an overview of the high value transaction process.

There are two branches to the high value transaction use case: high value transactions enabled through PIN entry on the PIN Entry Device at the Point of Sale (predominantly used in Online PIN markets); and high value transactions enabled through mPIN entry on the keypad on the Mobile Device. Both options are covered in the flow described below.

Annotations

1. Default card may not be able to successfully complete if the Payment Application is blocked for example.
2. Handset PIN will be required if the Payment Application has been configured by the Issuer for offline mPIN entry on the handset for high value transactions and if the terminal supports mobile initiated offline mPIN high value transactions.
3. Terminal PIN will be required if the Payment Application has been a configured by the Issuer for "Online PIN always" for high value transactions.
4. The PIN retry process for mobile PIN entry on the mobile device (as defined in Mobile MasterCard PayPass M/Chip4 Technical Specifications) is the same as standard PIN retry processes for contact cards in contact terminals. Issuers can configure the retry limit and once the limit is reached can block the Payment Application and display a suitable error message to the cardholder within the User Interface Application.
This section outlines the next layer of functionality that Mobile MasterCard® PayPass™ offers issuers and their cardholders.

These additional features may not be used as frequently as the core functions, but they are crucial in offering cardholders a means of managing the use of their Mobile MasterCard PayPass enabled cards on a mobile device.

As the mobile device provides a means of displaying information on the screen, as well as a means of updating information on the device via the mobile network, a number of additional features have been incorporated into the Mobile MasterCard PayPass M/Chip Technical Specifications. The use cases described in this section give examples of how some of these features can be implemented.
Multiple cards with the User Interface Applications.

This flow shows how a cardholder can use a User Interface Application to add a new card to their Mobile Device.

Annotations

1. Multiple forms of activation are possible. The above flow shows two common options:
   A. The first branch of the flow (horizontal) shows the scenario in which the activation sequence is linked to the first configuration of the mPIN by the end-user.
   B. The second branch of the flow (vertical) shows the scenario in which the activation sequence involves an Over The Air activation of the card or account at the issuer host.
2. Secure Word is an optional feature that is configurable in Mobile MasterCard PayPass M/Chip4 compliant applications.
Choosing to pay using a non-default card from within the User Interface Application.

In this scenario, the user has decided to make a purchase using a card other than their nominated Default Card.

Annotations

1. User can choose to override default card for the payment, by simply choosing another card from the User Interface Application. The example shown is based on a horizontal scrolling between cards, such that the user can swipe left and right to view and select an alternative card.

2. The example shown here uses the "Pre-Acknowledgement" option defined in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications. Where pre-acknowledgements are enabled, the cardholder will be required to enable the use of a card before every single payment as shown in this example.

3. The use of the "Pre-Acknowledge" feature should also include the use of a countdown timer as shown here, indicating to the cardholder how long their card is enabled (or "Pre-Acknowledged") for before it times out and they have to re-enable it for payment.
Card details and transaction history.

Users can review basic details relating to a card. This includes recent transaction history.

Annotations

1. Transaction history display based on locally stored transaction logs alone [EMV log] will typically not include individual merchant names. This example is based on a consolidated transaction history that may use data from the locally stored transaction log (within the Payment Application) but will rely on the transaction data from the issuer host system for merchant names.
This section contains the screen flows for functionality that helps issuers implement risk management in a user friendly manner and allows users to manage their cards and usage.

MasterCard has incorporated a number of flexible risk management and cardholder configuration management features which issuers can make use of in their deployments of Mobile MasterCard PayPass M/Chip 4 compliant applications.

These can be implemented in a variety of ways, depending on the risk management objectives of the individual issuer.

The use cases in this section are an example of common implementation approaches when deploying Mobile MasterCard PayPass M/Chip 4 compliant applications. User Interface Applications that are deployed in conjunction with non-Mobile MasterCard PayPass M/Chip 4 payment applications, may not offer this level of functionality.
Changing mPIN - screen flow

1 How to use this document
1.1 Use case legend

2 Propositions to the user and to the card issuer

3 Core functionality
3.1 Installation and activation process
3.2 Low Value Transaction
3.3 High Value Transaction

4 Extended functionality
4.1 Adding a new card
4.2 Choosing to pay with an alternative card, one time only
4.3 Viewing card details and transaction history

5 Settings & setup functionality
5.1 Changing mPIN
5.2 Setting a Default Card and preferred card
5.3 Responding to a Counter Reset request

6 Example graphic design for interface elements

7 Appendix A
8 Appendix B
Setting a Default Card and preferred card - screen flow

Setting a Default Card.

This flow shows how a cardholder can set a Default Card and how cards can be re-arranged in the list view. The Default Card is defined as the card (or Payment Application) which will be used when the cardholder presents their device to a payment terminal to make a payment.

The same flow as described below also applies to the concept of changing or setting a Preferred Card within any User Interface Application. The Preferred card is defined as the card (or Payment Application) which is at the top of the preference list within a User Interface Application and which that User Interface Application would set as the Default Card in cases where multiple User Interface Applications (each with multiple cards) may be installed on a mobile device.

Annotations

1. At a technical level the Default Card is the Payment Application (represented by a unique AID) that is set in the PPSE as the application that responds to the transaction request from the payment terminal when the mobile device is presented to the terminal. Changing the default card from the User Interface Application as shown in this flow will overwrite what is set in the PPSE with a new AID that is associated with the Payment Application that is represents the new card.

2. As multiple User Interface Applications may be installed on a mobile device, each of which may be linked to multiple Payment Applications, a differentiation is made between the concept of Default Card and Preferred Card. The Preferred Card is the card that is at the top of the ordered list of preferred payment cards within a specific User Interface Application. The Preferred Card setting is therefore stored within the User Interface Application and not within the PPSE (as in the case of the Default Card). When a User Interface Application is launched, it may therefore try to overwrite the Default Card (or AID) that is set in the PPSE.

3. Full card details such as PAN, expiry date and CVC2 should only be shown following cardholder verification such as PIN entry.
Responding to a Prompted Counter Reset Request.

There are two mechanisms that can be used to initiate the reset of the Offline Risk Management Counters on a mobile device. The first of these is described in the flow below: Responding to a Prompted Reset Request.

In this flow the Payment Application will be configured to send an instruction to the User Interface Application when the counter limit has been reached, to display a request for the cardholder to initiate the Counter Reset. This can be configured to occur immediately after a transaction that causes the offline counters to reach their limit.

For the purposes of this illustration, the term “Authorizing Card” has been chosen to refer to the Counter Reset process in the User Interface Application.

Annotations

1. Once the cardholder has entered their mPIN on the keypad of the mobile device the User Interface Application will emulate a Point of Sale terminal by generating an ARQC. The User Interface Application will then send the ARQC to the issuer host or appropriate gateway that can forward the request on to the host in order for the request to be processed. When the host responds by sending back an appropriate ARPC the User Interface Application will receive the response and forward it to the Payment Application in order to reset the counters. Once this process is completed the Payment Application can be used for payments once again and an appropriate screen can be shown to the cardholder to confirm this.

2. The PIN retry process for mobile PIN entry on the mobile device (as defined in Mobile MasterCard PayPass MChip4 Technical Specifications) is the same as standard PIN retry processes for contact cards in contact terminals. Issuers can configure the retry limit and once the limit is reached can block the Payment Application and display a suitable error message to the cardholder within the User Interface Application.

Cardholder makes payment causing offline counters to reach limit, or issuer sends script to Payment Application on mobile device to cause counters to reach limit, thus triggering Counter Reset sequence.
Resetting Offline Risk Management Counters - screen flow

Manual Initiation of a Counter Reset Request.

The second scenario for a Counter Reset is described in the flow below: Manual Reset.

In this flow the cardholder may have previously ignored the prompt to Reset the Counters, in which case the cardholder may chose to initiate the process at any time, by launching the User Interface Application and following the instructions as shown in the example below.

Annotations

1. If the user chooses to ignore the initial prompt to authorise the card (reset counters), the User Interface Application will remain in a state where it requires the user to enter the mPIN to reset the counters, so every time the user view that particular card in the User Interface Application, the prompt will be displayed. Once the cardholder has entered their mPIN on the keypad of the mobile device the same process as described in the previous use case will take place. Once this process is completed the Payment Application can be used for payments once again and an appropriate screen can be shown to the cardholder to confirm this.
The following pages show example screen designs for a selection of common Mobile MasterCard PayPass use cases on a typical smartphone.

They are intended to provide stimulus and to highlight the opportunities available; they are not a complete set of screens and neither are they prescriptive. Partners may choose to skin their Mobile MasterCard PayPass User Interface Applications using their own branding and style. It must be noted however that any such User Interface Application must still comply with the MasterCard Branding Standards and Mobile MasterCard PayPass User Interface Application Requirements.

The screens show a variation in approach to design, including both simple and straightforward styles plus more graphically rich treatments that take up the wallet metaphor.

These designs are included to show a range of options for creating innovative and appealing User Interface Applications for smartphones that support an interface with MasterCard Payment Applications.
1 How to use this document
2 Propositions to the user and to the card issuer
3 Core functionality
4 Extended functionality
5 Settings & setup functionality
6 Example graphic design for interface elements
7 Appendix A
8 Appendix B

Home screen & card list (touch-screen device).

Annotations
1. Where card images are used in User Interface Applications, they should always be the previously approved card image of the “parent” or existing physical card that the issuer has had approved by MasterCard.
2. The EMVCo Contactless Indicator is an optional element in card layout designs and User Interface Application screens. Please refer to the MasterCard PayPass and/or Maestro PayPass Branding Standards for further guidance or contact mobilepartner@mastercard.com.
3. Any User Interface Applications which use card images or account detail views that do not utilize any issuer branding, must comply with the rule specified in the MasterCard Card Design Standards Manual which stipulates that as an alternative to an issuer brand identifier the following statement must be displayed: “This account is issued by [FULL ISSUER NAME] pursuant to license by MasterCard International.”

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Example graphic design for interface elements - screen layouts

1 How to use this document
1.1 Use case legend
2 Propositions to the user and to the card issuer
3 Core functionality
3.1 Installation and activation process
3.2 Low Value Transaction
3.3 High Value Transaction
4 Extended functionality
4.1 Adding a new card
4.2 Choosing to pay with an alternative card, one time only
4.3 Viewing card details and transaction history
5 Settings & setup functionality
5.1 Changing mPIN
5.2 Setting a Default Card and preferred card
5.3 Responding to a Counter Reset request
6 Example graphic design for interface elements
7 Appendix A
8 Appendix B

Annotations
1. Where actual card images are not used an alternative design option is to display all relevant identifiers (Issuer logo, relevant MasterCard brand identifier and any additional identifiers set by the issuer or cardholder) as shown in this example. Logos and brand identifiers should be sized in order to make them legible.

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Example graphic design for interface elements - screen layouts

Card details & transaction history screen (touch-screen device).

1 How to use this document
1.1 Use case legend
2 Propositions to the user and to the card issuer
3 Core functionality
3.1 Installation and activation process
3.2 Low Value Transaction
3.3 High Value Transaction
4 Extended functionality
4.1 Adding a new card
4.2 Choosing to pay with an alternative card, one time only
4.3 Viewing card details and transaction history
5 Settings & setup functionality
5.1 Changing mPIN
5.2 Setting a Default Card and preferred card
5.3 Responding to a Counter Reset request
6 Example graphic design for interface elements
7 Appendix A
8 Appendix B

Annotations

1. The display of full card details should require the entry of an mPIN or other verification code as defined in [Mobile MasterCard PayPass User Interface Application Requirements].

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Card details & transaction history screen (non-touch-screen device).

Annotations

1. Transaction history display based on locally stored transaction logs alone (EMV log) will typically not include individual merchant names. This example is based on a consolidated transaction history that may use data from the locally stored transaction log (within the Payment Application) but will rely on the transaction data from the issuer host system.

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Example graphic design for interface elements - screen layouts

Annotations

1. When configuring a card for offline High Value Transactions or for pre-acknowledgement (pre-signing) for all offline transactions, issuers need to configure a time limit on how long the payment can be made after successful PIN entry/verification.

The example shown here shows an arbitrary 60 second time-out limit. The User Interface Application would typically display a count down until the time-out limit is reached.

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Annotations

1. The user can change the order of preference of cards by dragging cards up and down the list and dropping them in the preferred location in the list. The card at the top of the list automatically becomes the default card, and an appropriate notification should be displayed to the user if the default card is updated in order to be compliant with the Mobile MasterCard PayPass User Interface Application Requirements.

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Payment process with PIN request (touch-screen device).

**Annotations**

1. Where the PayPass logo is not shown on the adverse side of existing card designs, it is possible to use the “flip” view within the User Interface Application to ensure that the relevant PayPass logo can be shown and thus comply with MasterCard (or Maestro) PayPass Branding Standards.

2. Any card image or card detail view that includes sensitive data such as the full card number (PAN) and/or CVV2 code and/or expiry date should not be shown without a suitable verification step.

The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
The use of card images in User Interface Applications is one way of clearly displaying to the cardholder which account they are interacting with. MasterCard does not mandate the use of card images in User Interface Applications, but this option is supported in the Mobile MasterCard PayPass M/Chip 4 Technical Specifications through the Card Layout Display feature. Issuers, or providers of User Interface Applications, take full responsibility for the use of any features or design conventions, including those shown in this set of examples. MasterCard is not liable for any intellectual property rights infringement that may arise out of the use of any such features or example designs used in this design guide.
Appendix A - Common first-time setup process examples

1. Full OTA without Activation
(Over The Air download of User Interface Application - acting as Personalization Proxy or Agent - and Payment Application, followed by Personalization based on a Verification Code, no further Activation sequence required)

2. Full OTA with Activation
(Over The Air download of User Interface Application - acting as Personalization Proxy or Agent - and Payment Application, followed by Personalization based on a Verification Code, followed by a further Activation sequence)

3. UI OTA with Personalization
(Over The Air download of User Interface Application - acting as Personalization Proxy or Agent - followed by Personalization based on a Verification Code, no further Activation sequence required)

4. UI OTA with Activation
(Over The Air download of User Interface Application - acting as Personalization Proxy or Agent - followed by Activation sequence)

5. UI OTA with Personalization and Activation
(Over The Air download of User Interface Application - acting as Personalization Proxy or Agent - followed by Personalization based on a Verification Code, followed by further Activation sequence)

6. Applet OTA with Personalization
(Over The Air download of Payment Application, followed by Personalization based on a Verification Code, no further Activation sequence required)

7. Applet OTA with Activation
(Over The Air download of Payment Application, followed by Activation sequence)

8. Applet OTA with Personalization and Activation
(Over The Air download of Payment Application, followed by Personalization based on a Verification Code, followed by further Activation sequence)

9. Personalization only
(Personalization based on a Verification Code only, no further Activation sequence required)
Appendix A - Common first-time setup process examples

10. Activation only
(Activation sequence for already installed and personalized Payment Application only)

11. Personalization and Activation only
(Personalization based on a Verification Code, followed by further Activation sequence)
Appendix B - Glossary

**Account Activation**
Change of status of an account on the Issuer host system from inactive or "not usable" to active or "usable".

**Account Deletion**
The permanent removal of PayPass account details from a secure element.

**Account Details**
An issuer-specific set of cardholder personalization details allowing a PayPass transaction to take place.

**Application Identifier**
The Application Identifier (AID) is a unique identification code denoting the type of application (e.g. MasterCard, Maestro or other scheme ID). Depending on supported formats (e.g. with extensions) the AID may also be configured such that it denotes a specific Payment Application with a type (i.e. specific Payment Applications representing different accounts within a group of MasterCard Payment Applications).

**ARPC**
Authorization Response Cryptogram

**ARQC**
Authorization Request Cryptogram

**Blocked**
A status of a Payment Application meaning it is unable to perform a transaction (i.e. the Payment Application may be put into this state by means of a “Block” command sent in a script by the Issuer host system).

**Card Verification Code 2**
Static Card Verification Code as normally printed on the reverse of payment cards for use in the validation of card holders for Cardholder Not Present transactions (such as online or telephone-based transactions).
Appendix B - Glossary

Card Verification Code 3
Dynamic Card Verification Code as calculated dynamically by the Payment Application during a PayPass MagStripe transaction.

Cardholder Verification Method (CVM)
Verification method used to validate the presence of the cardholder at the time of the transaction (options include use of PIN or signature).

CVM Limit
The transaction amount, typically defined at a market level by the banks, above which contactless transaction require cardholder verification (such as a signature or PIN).

Default Payment Application
The card or Payment Application which is set to be used when the device is presented to a contactless reader for payment.

Handset
A type of mobile device, specifically a mobile phone handset.

High Value Transaction
Transactions where the amount exceeds the applicable CVM Limit, i.e. where an appropriate form of CVM is required such as offline or online PIN.

Issuer
A financial institution that is licensed to issue MasterCard payment solutions (such as cards or PayPass devices)

Low Value Transaction
Transactions where the amount is below the applicable CVM limit, i.e. where no form of CVM is mandatory for the transaction to be approved.

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 Personal Digital Assistant (PDA).
Appendix B - Glossary

Mobile MasterCard PayPass Application
A Payment Application that conforms to the Mobile MasterCard PayPass Requirements and Mobile MasterCard PayPass Technical Specifications.

Mobile Partner Programme
The Mobile department within MasterCard Worldwide runs a program for all companies that are involved in, or wish to be involved in, any mobile payment related initiative (including, but not limited to, Mobile MasterCard PayPass), either at an issuer level or at a supplier level. The program is supported by a website (within MasterCard Online: www.mastercard-mobilepartner.com) which acts as a communication tool and resource centre for all partners.

Mobile Payment Device
A portable device that offers wireless communication capability such as a mobile phone, cell phone, Personal Digital Assistant (PDA), etc., and which (once personalized) is capable of executing a payment transaction.

OTA Personalization
Personalization (see definition below) of a Payment Application on a Secure Element within a Mobile Payment Device using a wireless data transfer such as the mobile network.

OTA Provisioning
The transfer of Payment Applications Over The Air onto a Secure Element on a Mobile Payment Device.

OTA Verification
A cardholder password used to authenticate the cardholder as part of the OTA provisioning and/or personalization process.

Over The Air (OTA)
Over-The-Air (OTA) refers to any process that involves the transfer of data (including applications) to the mobile handset or any component within the mobile handset via the mobile network.

Password
A protected word, code, or set of characters used to identify a user and permit access to an application or system and its resources.
Appendix B - Glossary

Payment Application
Generic term for any application which runs in a secure environment on a payment device (such as an ID-1 card or a Secure UICC) and which facilitates the payment transaction taking place with a payment terminal.

Payment Application Activation
Change of status of a Payment Application from "not usable" or "not selectable" to be "usable" or "selectable" such that it can perform contactless transactions.

Payment Application De-Activation
Change of status of a Payment Application from "not usable" or "not selectable" to be "usable" or "selectable" such that it can perform contactless transactions.

Payment Terminal
A device or system at a physical merchant location that initiates a payment transaction with a Payment Device (such as a card or contactless enabled Mobile Device)

Personalization
Installation of cardholder-specific data into the Secure Element of a Payment Device. May take place Over The Air, via the contactless interface or via a contact interface during or after production.

Personalization Proxy
Also known as Personalization Agent or TSM Agent. Software that provides interaction between the Payment Application within the Secure Element and the mobile network for over-the-air personalization. It may also be used to enable provisioning of the Payment Application over-the-air to the Secure Element. May be implemented in a number of ways, for example a Java MIDlet.

Preferred Card
The Preferred card is defined as the card (or Payment Application) which is at the top of the preference list within a User Interface Application and which that User Interface Application would set as the Default Card in cases where multiple User Interface Applications (each with multiple cards) may be installed on a mobile device.
Appendix B - Glossary

Provisioning
Installation of a Payment Application into the Secure Element on or in a Mobile Device.

Proximity Payment System Environment
The Proximity Payment System Environment (PPSE) is an application which points to a default or otherwise selectable Payment Application within the Secure Element. In order to achieve this, the PPSE provides a directory of the Payment Application identifiers (AID), and where applicable the associated priority order. A PayPass terminal is required to select the highest priority application which it supports.

Secure Element
A secure, tamper-resistant storage and execution environment holding payment applications and payment assets such as keys.

Trusted Service Manager
An entity that provisions, personalizes or manages Payment Applications on Mobile Devices on behalf of MasterCard issuers. A TSM may perform any or all of these roles including the data preparation, data management, and key management functions.

UICC
Universal Integrated Circuit Card (commonly referred to as “SIM card”)

User Interface Application
An application that typically runs in the non-secure memory of a mobile device and facilitates user interaction with the Payment Application or Applications running within the Secure Element (supported features may include PIN entry, transaction history review and OTA functionality). May also be referred to as “Wallet”.

User Interface Application Provider
A legal entity that has signed a relevant MasterCard License Agreement, is entitled to use MasterCard brands and supply MasterCard UI/Wallet applications and whose name will be stated on the Mobile MasterCard PayPass User Interface Application - Letter of Approval.