Mobile MasterCard PayPass UI Application Requirements

February 2013 - Version 1.4

MasterCard Worldwide
Chip Centre of Excellence
Chaussée de Tervuren 198A
B-1410 Waterloo
Belgium.
www.mastercard.com

1 Using this Manual

This chapter contains information that helps you understand and use this manual.

1.1 Scope

This document lists the basic requirements that must be met in order for a User Interface solution (used in conjunction with a Payment Application on an NFC enabled mobile device) to achieve MasterCard approval.

It also lists functionality options that are relevant to Mobile MasterCard *PayPass* implementations and that may be included in a User Interface Application, and which will therefore be subject to MasterCard Approval.

1.2 Audience

This document is aimed primarily at:

- User Interface Application developers.

However, other members of the mobile contactless payment ecosystem may also find the information contained in this document useful or may actually wish to develop and therefore submit for approval their own UI. These include:

- Issuers
- Mobile Network Operators (MNOs)
- Mobile Device Manufacturers
- Trusted Service Managers (TSMs)
- Payment Application Providers

1.3 Reader Guidance

This document lists the licensing and basic requirements that User Interface Applications that are used in implementations of Mobile MasterCard *PayPass* must adhere to. It also includes recommendations for best practice and clarifications on what options are also allowed.

In this regard the following wording is used:

"must" – means that the statement is a requirement and failure to comply may mean that the User Interface Application cannot be approved Some requirements are applied conditionally if optional UI functionality is supported.

"should" – means that the statement is a recommendation made by MasterCard to ensure best practice is applied, failure to comply with such a statement does not mean that the User Interface Application cannot be approved

"may" – means that the statement is not a MasterCard requirement or recommendation, but is designed to clarify that such an approach is not in contradiction of any MasterCard requirement or recommendation

1.4 Abbreviations and Acronyms

The following abbreviations and acronyms are used in this manual:

Acronym	Meaning
CVC	Card Verification Code
CVM	Cardholder Verification Method
HVT	High Value Transaction
J2ME	Java 2 Micro Edition
LVT	Low Value Transaction
MNO	Mobile Network Operator
mPIN	mobile Personal Identification Number
OTA	Over The Air
PAN	Primary Account Number
POS	Point of Sale
PPSE	Proximity Payment System Environment
SE	Secure Element
SIM	Subscriber Identity Module
STK	SIM Application Toolkit
TSM	Trusted Service Manager
UI	User Interface
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module

1.5 Related Information

The following documents and resources provide information related to the subjects discussed in this manual.

Note

MasterCard reserves the right to release new versions of documents referenced by this process. Partners should therefore check for the latest documentation versions and the impact of any amendments they contain before starting the partner testing process.

Mobile MasterCard PayPass Requirements	Mobile MasterCard *PayPass* – Requirements
Mobile MasterCard PayPass User Interface Application Approval Guide	Approval process guide document for User Interface Applications designed for use with MasterCard Payment Applications
MasterCard PayPass Branding Standards	Branding standards document covering implementations and supporting material relating to MasterCard *PayPass* deployments
Maestro PayPass Branding Standards	Branding standards document covering implementations and supporting material relating to Maestro *PayPass* deployments

1.6 Terminology

This section explains a number of key terms and concepts used in this manual.

Term	Meaning
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.
Approval	The umbrella term for all testing and/or evaluation and/or review processes and outputs thereof relating to products or services or components thereof that are used in implementations of Mobile MasterCard *PayPass*.

Term	Meaning
Assembly	A combination of components that, when brought together, can perform the basic function of making a contactless payment and can therefore be tested for functional compliance with Mobile MasterCard *PayPass* requirements. Typically this includes the mobile device, the Secure Element, the contactless processor, the contactless antenna and the necessary software to perform payment transactions. This does not include any OTA component..
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).
CVM	Cardholder Verification Method - 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).
CVC2	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).
CVC3	Dynamic Card Verification Code as calculated dynamically by the Payment Application during a PayPass MagStripe transaction.
Formal Tests or Formal Evaluation	The set of testing or evaluation sub-processes that have a defined start (sample requirements etc.) and end point (test assessment, test report etc.) and are required as input to a product or service Approval.
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..

Term	Meaning
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).
mPIN	Mobile Personal Identification Number – Code required to verify end-user in order to enable transactions to take place (e.g. offline PIN entered on Mobile Device for mobile contactless payments or verification code to verify cardholder for remote payments).
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.
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 "usable" or "selectable" to be "not usable" or "not selectable" such that it cannot perform contactless transactions.
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.
User Interface or Wallet 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.

Term	Meaning
User Interface or Wallet 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".

1.7 Revision History

MasterCard periodically will issue revisions to this document as and when any enhancements, new developments, corrections or any other changes are required.

Each revision includes a summary of changes which is added to the revision history below, describing what has changed and how. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appear at the right of each revision marker.

MasterCard may publish revisions to this document in a MasterCard bulletin, another MasterCard publication, or on MasterCard OnLine, with the Mobile Partner Program section: www.mastercard-mobilepartner.com.

A subsequent revision is effective as of the date indicated in that publication or on MasterCard OnLine and replaces any previous edition.

Version	Date	History	Impact
1.0	December 2009	First published version.	Set of defined requirements for User Interface Applications, augmenting *PayPass* on Mobile Requirements
1.2	February 2011	Updated version following publication of Mobile MasterCard *PayPass* M/Chip 4 Technical Specifications and User Interface Design Guide	Additional recommendations and revised requirements.
1.3	May 2012	Fixed typographical error in “Payment Application De-Activation” entry in Terminology table.	None

Version	Date	History	Impact
1.4	February 2013	Clarification of the classification of Requirements and Recommendations. Also new requirements related to the display of sensitive account holder information	Additional requirements and revised requirements and recommendations.

2 Introduction

This document lists the functional requirements for User Interface or Wallet Applications that are to be used as part of Mobile MasterCard *PayPass* implementations.

It will provide information with regards to:

- The licensing requirements
- The requirements that must be met
- Optional functionality

2.1 Background

MasterCard has developed a comprehensive test and validation process for Mobile MasterCard *PayPass* implementations which is based on the existing *PayPass* test and validation process, Personalization Bureau Accreditation Process and Branding Approval Process for cards and devices. This ensures world-wide interoperability as well as high quality, reliability and security assurance at acceptable levels of time and cost.

All components and sub-components used in an implementation of Mobile MasterCard *PayPass* must go through a test and validation process. All approved products, services, components and subcomponents are documented and held in a database maintained by MasterCard.

This information is made available to issuers and all other partners via the Mobile Partner Program to enable issuers to ensure that only approved components are used in deployments of Mobile MasterCard *PayPass*.

The User Interface Applications (UIs), also often referred to as Wallets, are designed to provide the end-user, or account holder, access to the Payment Application and in turn, control over certain features relating to making payments using the Payment Applications that are installed on the Secure Element within a Mobile Device (regardless of architecture – e.g., SWP UICC or embedded Secure Element). Therefore all aspects of a User Interface Application that relate to MasterCard specified functionality and all usage of MasterCard brand identifiers or any other MasterCard properties must be evaluated to validate conformance to the prescribed MasterCard requirements and standards.

2.2 Who Needs to Implement these Requirements?

The requirements need to be met by any organization wishing to gain approval from MasterCard to provide a UI or Wallet to MasterCard issuing institutions in the context of Mobile MasterCard *PayPass* issuance.

2.3 When must these Requirements be Implemented?

The basic requirements apply to all UI solutions and must be implemented in all deployments.

Requirements relating to the optional features only, apply to UI solutions where it is possible to enable such options within the implementation. If these features are not built in to the UI, the requirements are not applicable.

Note

Any UI Application that interfaces with a MasterCard compliant Payment Application and/or makes use of any MasterCard brand identifiers or other properties will need to comply with these requirements.

3 Prerequisites and High Level Requirements

3.1 UI Approval Requirement Applicability Check

User Interface (UI) Applications vary greatly in terms of scope and purpose and for the avoidance of doubt, all providers of UI Applications that are designed for use in the context of Mobile Payments should check if their application requires approval from MasterCard based on the requirements defined in this document.

3.1.1 Interface with MasterCard Payment Application

Any UI that interfaces in any way with a MasterCard Payment Application (such as a Mobile MasterCard *PayPass* M/Chip 4 application) will need to be approved by MasterCard and therefore all of the requirements described in this document will apply.

3.1.2 Requirement to use MasterCard Branding when Interfacing with MasterCard Payment Applications

Any UI that interfaces in any way with a MasterCard Payment Application (such as a Mobile MasterCard *PayPass* M/Chip 4 application) must display the necessary MasterCard brand identifiers as defined in the Branding Requirements below.

3.1.3 Use of MasterCard Properties

Any UI that makes use of any MasterCard properties (such as MasterCard *PayPass* brand identifiers) will need to be approved by MasterCard and therefore all of the requirements described in this document will apply.

3.2 Branding Requirements

3.2.1 Use Cases

Certain Use Cases will require the display of brand identifiers (brand images or brand names) within the UI in order to indicate to the end-user what account is currently being used or accessed through the UI.

The requirements for the Functions described in section 4 of this document, will include, where applicable, references to the branding requirements detailed herein.

The User Interface Application Evaluation process as defined in [*Mobile MasterCard PayPass User Interface Application Approval Guide*] will determine whether or not brand identifiers have been used in the relevant functions which will in turn determine if the UI being evaluated is compliant with the requirements defined in this document.

The Branding Review which is defined in [*Mobile MasterCard PayPass User Interface Application Approval Guide*] will determine whether the brand identifiers conform to MasterCard's branding standards as defined in [*MasterCard PayPass Branding Standards*] and [*Maestro PayPass Branding Standards*].

3.2.2 Text Only User Interface Applications

Certain programming options for User Interface Applications are limited to a text-only interface (such as SIM Application Toolkit – STK – Applications). In such cases the requirements for the use of brand identifiers in the context of the Functions detailed in section 4 of this document will be limited to the use of brand names which are displayed in text format (e.g., MasterCard *PayPass*).

3.2.3 Graphical User Interface Applications

All User Interface Applications which are programmed in a format that allows the use of graphical images (such as J2ME, Symbian or a programming language that is native to a Mobile Device) must use the correct graphics as defined in [*MasterCard PayPass Branding Standards*] and [*Maestro PayPass Branding Standards*]. These can be obtained from MasterCard by contacting license@*PayPass*.com and are only available to *PayPass* licensees as defined below in Licensing Requirement.

3.2.4 Brand Parity

In most cases, brand identifiers associated with the issuing institution, and in some cases other entities such as MNOs and Handset Manufacturers, may also be used on the same screen as MasterCard brand identifiers. In all such cases the minimum requirement of "Brand Parity" between the brand identifiers used must be maintained as defined in [*MasterCard PayPass Branding Standards*] and [*Maestro PayPass Branding Standards*].

This will be determined during the Branding Review process as defined in [*Mobile MasterCard PayPass User Interface Application Approval Guide*].

3.3 Licensing Requirement

Vendors wishing to receive MasterCard *PayPass* specifications and ultimately support a UI product for approval must sign the appropriate MasterCard *PayPass* License Agreement. Vendors who do not yet have a relevant license agreement in place should contact the Mobile Partner Program by email:

mobilepartner@mastercard.com

There are several licensing options, depending on the type of implementation or the role of the UI Application provider.

Note **Any entity that wishes to submit a UI for approval based on the requirements defined in section 2.1 will need to hold a relevant license agreement.**

3.3.1 Issuer *PayPass* Program enrolment requirement

Issuers that are developing their own UI Application and wish to deploy such an application will need to be enrolled in the *PayPass* program. All such User Interface Applications (and versions thereof) must be submitted to MasterCard for approval.

3.3.2 Mobile MasterCard *PayPass* M/Chip 4 License Option

This license is the most appropriate license agreement for mobile application developers as it includes access to the Mobile MasterCard *PayPass* M/Chip 4 Technical Specifications, which is MasterCard's payment application specification designed for implementing *PayPass* on mobile devices.

3.3.3 Standard *PayPass* License Option

This license provides access to all existing *PayPass* specifications, branding and other relevant material (except the Mobile MasterCard *PayPass* M/Chip 4 Technical Specifications) and is therefore designed for vendors who may cover several areas of *PayPass* related products, but are not commercializing Mobile MasterCard *PayPass* M/Chip 4 payment applications..

3.3.4 Mobile Network Operator *PayPass* License Option

This *PayPass* license option has been developed primarily for Mobile Network Operators, who may not require access to all specifications and materials that would normally be required for MasterCard vendors. It will provide sufficient access to specifications and MasterCard *PayPass* properties to enable Mobile Network Operators to develop User Interface Applications (or functionality) to be embedded on (or distributed to) mobile handsets. This license may also be suitable for entities other than Mobile Network Operators (such as Handset Manufacturers or other members of the distribution chain).

3.4 Functionality Options

A large number of functions can be implemented in a UI.

The classification of a "Function" is the group of associated actions that allow the user to interact with a MasterCard Payment Application, either directly associated with a payment or in the context of managing one or more MasterCard Payment Applications that are installed on the Secure Element.

The requirements and recommendations associated with each function will be applied if the function is supported by the UI Application.

3.4.1 Requirement for Evaluation of Enabled Functions

Although the support of the functions listed is not mandatory, every function that is supported must be checked for functional reliability and usability.

When a UI is being submitted for approval, the Vendor will be requested to provide information regarding the functions and optional features that it supports in the [*Mobile MasterCard PayPass User Interface Application Registration Form*].

All functions that are identified by the vendor as having been implemented will then be evaluated.

3.5 Approval Process

Based on basic requirements defined above, the UI provider must submit the UI for formal evaluation and approval.

The process that the UI provider should follow to gain approval for their UI is defined in detail in [*Mobile MasterCard PayPass User Interface Application Approval Guide*].

This document is available from the Mobile Partner Program

www.mastercard-mobilepartner.com

4 Functional Requirements

4.1 General UI Application Requirements

4.1.1 Stable Operation

Requirement 4.1.1

All UI applications must show stable operation during the Functional Evaluation. Unexpected errors, timeouts or instability will be marked up as non-compliant and the vendor will be required to take corrective action and may need to resubmit the User Interface Application for evaluation.

4.1.2 Requirement for Inoperable Functions to be Invisible

Requirement 4.1.2

Any features that are visible but are inactive or inoperable will be marked up as non-compliant and the vendor will be required to take corrective action and may need to resubmit the User Interface Application for evaluation.

4.1.3 Clear Cache Requirement

Requirement 4.1.3

In all UI Applications, any data that is accessed and/or displayed (as defined below) must not be stored within the UI once the function for which it was used has been completed.

Data stored in a Payment Application within the Secure Element must only be accessed or retrieved for display on request from the UI as defined below and must then be removed from any cache or temporary memory within the non-secure memory, or run-time environment associated with the UI, as soon as the action has been completed.

4.1.4 Version Control and Numbering

In order to cross reference a released UI application with the Letter of Approval, the UI must have a unique software version number.

The UI application must be assigned a software version number that must be incremented each time the UI Application is changed and released. The format of this version number is unrestricted, and the UI vendor may choose their own format, or use the versioning controls available within the mobile device Operating System. The software version number must be accessible without special knowledge, equipment or privileges. For example, it can be shown on an 'About' or 'Help' screen or menu, or be accessible through the devices operating system.

MasterCard must be informed of all changes to the UI application (using the UI registration process) after the LoA has been granted, and will determine if changes are minor or major. Changes that fall outside of the requirements in this document are deemed to be minor. Changes that impact the requirements in this document are deemed to be major. In the case of major changes, the software version number must increment and the UI may need to be reevaluated.

Requirement 4.1.4

The UI application shall be assigned a unique software version number for each release of the UI application. This version number can be displayed from within the UI application or from within the mobile device operating system, but in either case it shall be user accessible.

4.2 Provisioning support

Some UI Application or Wallets may include functionality to allow the account holder to download 'cards' to their handset. This process may include transferring account holder details, such as the personalization of the Payment Application, over the air. It must be established that the initiator of the OTA personalization process is the legitimate owner of the account and in control of the handset at the time of the personalization.

Requirement 4.2

User authentication shall take place before any account holder credentials are transferred to the user handset. The authentication method may take the form of,

- Entry of a predetermined verification code, or
- Other methods where the Issuer can ensure that the handset is in possession of the legitimate owner at the time of personalization.

4.2.1 Use of Verification Code

If a verification code is used it shall meet the following requirements.

4.2.1.1 Verification Code Length

Conditional Requirement 4.2.1.1 a – applies if a verification code is used

The minimum length of Verification Code shall be four (4) characters. The maximum length is at the discretion of the service provider. However, this needs to be synchronized with the registration screens (in the event of user creation of the Verification Code) and the TSM or Issuer's Verification Code generation facility.

Recommendation 4.2.1.1 b

It is recommended that this code is numeric only (for usability reasons). It should also be of a manageable size to ensure that:

- The user can easily remember this code.
- It provides sufficient security.
- It is acknowledged that there is always a tradeoff between convenience and security.

4.2.1.2 Verification Code UI Appearance

Conditional Requirement 4.2.1.2 – applies if a verification code is used

The Verification Code should not appear "in the clear" on the user's handset screen when it is entered. A masking technique should be used to preserve the security of this code.

For example, the entry of a four-character Verification Code may appear as four asterisks

4.3 Access control for User Interface Applications

Recommendation 4.3 a

MasterCard recommends that User Interface Applications should not include a password to enable access to the User Interface Application as the majority Mobile MasterCard PayPass M/Chip 4 Payment Applications will make use of the mPIN functionality. The use of both an access code for the User Interface Application and an mPIN for Payment Application related functionality may lead to confusion and an undesirable user experience.

Recommendation 4.3 b

Where passwords (that are not the mPIN of any Payment Application) are used, these should not be referred to as "PIN" or any term that includes the term "PIN" (e.g. "Wallet PIN" or "mobile PIN"). Recommended terms such as "Passcode", "Password" or "Access Code" should be used.

Recommendation 4.3 c

Furthermore such Passwords (that are not the mPIN) should not be configured to be the same format as typical PIN codes in that market (for example as a four digit numeric code in markets where most Issuers set their PINs to be four digits in length).

Requirement 4.3 d

The use of a Password (i.e. a code that is not the mPIN) as a CVM for High Value Transactions is strictly prohibited.

Conditional Requirement 4.3 e – applicable if the UI application can use non mPIN based passwords for UI or wallet access control purposes

Enabling, changing or activating a non mPIN based UI password shall only be done after the user's identity has been successfully verified. This can be achieved by, for example, utilizing the provisioning authentication details, online banking details, or a previously entered password or mPIN. It is acceptable to have the initial password set during initialization of the wallet, but subsequent password changes, activations or deactivations must require the entry of the previously set password. This is to prevent disabled passwords from being enabled and set by someone other than the account holder, and being used to illegitimately access sensitive or personal data.

4.4 Payment Application Activity Display

4.4.1 Transaction Notification

Requirement 4.4.1

All UI Applications that interface with MasterCard Payment Applications must support the display of a Transaction Notification on the Mobile Device when a contactless payment transaction has been completed by the device (i.e. after the Application Cryptogram, in the case of all EMV applications, or Dynamic CVC3 authentication, in the case of all MagStripe applications, has been successfully sent to the payment reader). The Transaction Notification is not an indication that the transaction has been approved by the terminal, but that the transaction details have been passed from the handset to the terminal, and the handsets part in the transaction is completed.

4.4.1.1 Brand Identifier Requirement in Transaction Notification

Whenever a Transaction Notification is displayed it is important that the customer is informed about which payment account or card was used to make the payment. Therefore every Transaction Notification must include the relevant MasterCard Product Identifier, Issuer Identifier and Issuer Product Identifier, as detailed in sections 4.4.1.1.1 and 4.4.1.1.2 .

Recommendation 4.4.1.1

In User Interface Applications where the user has the option to name the account or card, this name should also be displayed in the Transaction Notification.

4.4.1.1.1 Text Only Format

Conditional Requirement 4.4.1.1.1 – applicable for text based UIs

In UI Applications that are programmable in a text-only format (such as STK) the minimum requirement is for the correct full MasterCard Product, Issuer and Issuer Product Identifiers (in words) to be used when displaying the account details to which they correspond. If the UI has technical limitations to the

number of characters that can be displayed, suitable abbreviations can be used if agreed by MasterCard,

4.4.1.1.2 Graphical Format

Conditional Requirement 4.4.1.1.2 a – applicable for graphics based UIs

In UI Applications that are programmable in a visual format and that include the use of graphical images the minimum requirement is for the correct full MasterCard Product, Issuer and Issuer Product Identifiers to be used when displaying the account details to which they correspond.

This will also be subject to Branding Review to ensure the use of the Issuer image in conjunction with the relevant MasterCard Product identifier (as detailed above) is in accordance with [*MasterCard PayPass Branding Standards*] or [*Maestro PayPass Branding Standards*] as applicable.

Recommendation 4.4.1.1.2 b

These identifiers should be displayed in a graphical format, but text format is permissible where a technical limitation may prevent this from being implemented.

4.4.1.2 Prompt Display Speed

Requirement 4.4.1.2

The Transaction Notification shall be visible to the user on the screen of the Mobile Device within 2 seconds after the contactless transaction has completed.

4.4.1.3 Display Duration

Requirement 4.4.1.3

The Transaction Notification shall be visible to the user on the screen of the Mobile Device until the user accepts/cancels the notification. MasterCard will consider compliance with this requirement, on a case by case basis, for mobile devices whose operating systems have either technical limitations, or uses notification mechanisms that do not allow the use of user confirmation.

4.4.2 Single Card/Account Transaction Log Display

Recommendation 4.4.2

All UI Applications that interface with MasterCard Payment Applications should support the display of Transaction Logs where possible. MasterCard Payment Applications (in particular Mobile MasterCard *PayPass* M/Chip 4) will store, (at a minimum), the details of the last 10 transactions that have been made using that Payment Application.

The following data elements are stored as standard and should therefore be visible in the UI if this feature is enabled:

1. Transaction Amount
2. Transaction Currency
3. Transaction Date

4.4.3 Consolidated Multiple Card/Account Transaction Log Display

UI Applications that interface with multiple Payment Applications within the Secure Element may display consolidated transaction history data from multiple Payment Applications.

4.4.3.1 Common Data Elements

Recommendation 4.4.3.1

For implementations that make use of this feature the same data elements as defined in 4.4.2 Single Card/Account Transaction Log Display shall be displayed.

4.4.3.2 Transaction List Order

Recommendation 4.4.3.2

Transactions should be listed in the correct chronological order based on the Transaction Date and the order in which the transaction log records appear in the payment application.

4.4.3.3 Transaction Identification

Recommendation 4.4.3.3

It must be transparent to the user which payment application/account was used for each transaction. There are two standard approaches to displaying this information:

- Each transaction could include the card or account name set by the end-user. (see 4.6.1.6)
- Alternatively every transaction shown needs to include reference to the corresponding issuer identifier, issuer product identifier and MasterCard product identifier for the card/account that was used to make the transaction.

4.5 Payment Application Management and Selection

All UI Applications that interact with at least one Payment Application in the Secure Element must include Payment Application Management functionality as defined below.

4.5.1 Payment Application Activation Function

Requirement 4.5.1

All UI Applications that interact with at least one Payment Application in the Secure Element shall include functionality that allows the end-user to activate the Payment Application for contactless payments.

4.5.2 Payment Application De-Activation Function

Requirement 4.5.2

All UI Applications that interact with at least one Payment Application in the Secure Element shall include functionality that allows the end-user to disable the Payment Application such that when disabled it cannot be used for contactless payments.

4.5.3 Blocked Payment Application View

Recommendation 4.5.3

It is recommended that Issuers make use of the block command to block payment applications on the Secure Element under certain circumstances. Whenever this function is implemented, the following requirements apply:

4.5.3.1 Identification of blocked Payment Applications

Conditional Requirement 4.5.3.1 – applicable if Payment Application blocking functionality is supported

Payment Applications that have been blocked shall remain visible within the User Interface Application, and shall be suitably marked so that it is clear to the end-user that the Card or Account they are viewing is not available for use.

Where an image of the card is being displayed within the User Interface Application for example (as per the Card Layout Description feature), the image may be greyed out and/or can include an overlay of a suitable icon which indicates the card is not usable.

4.5.3.2 Blocked Payment Application Advice

Conditional Requirement 4.5.3.2 – applicable if Payment Application blocking functionality is supported

User Interface Applications shall include an option, which allows the end-user to read a more detailed description of the status of the blocked Card/Account, including instructions for having the Card/Account unblocked. This could be a customer support telephone number which can be selected directly from within the User Interface Application.

4.5.4 Multiple Payment Application Management

The following requirements and recommendations apply to UI Applications that include functionality that enables the end-user to manage multiple Payment Applications within the Secure Element. If the UI application does not support Multiple Payment Application Management, this section does not apply.

4.5.4.1 Default Function for Multiple Payment Applications

Requirement 4.5.4.1

All UI Applications that include functionality that enable end-users to manage multiple Payment Applications on the Secure Element must include a function to set a Default Payment Application, which (when activated) will be the Payment Application that automatically responds when the device is presented to a contactless payment reader to make a payment.

4.5.4.2 One-Time Override of Default Function

Recommendation 4.5.4.2 a

All UI Applications that include functionality that enable end-users to manage multiple Payment Applications on the Secure Element should include a function to override the Default Payment Application for a single payment transaction or limited time period.

Condition Requirement 4.5.4.2 b – applicable if Recommendation 10 is supported

If this functionality is implemented the Payment Application that was previously set as the Default, must revert to being the Default when the Override conditions have been fulfilled (i.e., once the transaction has completed, when the Override time has elapsed or if the end-user has cancelled the Override).

4.5.4.3 Multiple Payment Application Display Format

Any UI Application supporting multiple payment applications shall display MasterCard and Issuer identifiers as detailed in the following requirements.

4.5.4.3.1 Text Only Format

Conditional Requirement 4.5.4.3.1 – applicable for text based UIs

In UI Applications that are programmable in a text-only format (such as STK) the minimum requirement is for the correct full MasterCard Product, Issuer and Issuer Product Identifiers (in words) to be used when displaying the account details to which they correspond. If the UI has technical limitations to the number of characters that can be displayed, suitable abbreviations can be used if agreed by MasterCard.

4.5.4.3.2 Graphical Format

Conditional Requirement 4.5.4.3.2 – applicable for graphics based UIs

In UI Applications that are programmable in a visual format and that include the use of graphical images, the minimum requirement is for the correct full MasterCard Product, Issuer and Issuer Product Identifiers (in graphical format) to be used when displaying the account details to which they correspond.

This will also be subject to Branding Review to ensure the use of the Issuer image in conjunction with the relevant MasterCard Product identifier (as detailed above) is in accordance with [*MasterCard PayPass Branding Standards*] or [*Maestro PayPass Branding Standards*] as applicable.

As Mobile MasterCard Payment Applications must always be companions to standard card products, it is permissible to use images of the ID1 format card design as long as these have already been approved.

Note **In cases where a full card image is displayed in a User Interface Applications (including the full PAN, expiry date and CVC2), the requirements 4.6.1.2 Sensitive Account Information Display will apply.**

4.6 Account Detail Display

This section is concerned with the display, within the UI, of account related details as defined in "Types of Account Data" below.

For any UI that is designed to access any MasterCard Payment Application within the Secure Element and to display any details stored therein, the requirements defined in this section apply.

4.6.1 Account Data

4.6.1.1 MasterCard Product Identifier

In UI Applications that include the function to display account holder data stored in a Payment Application, the relevant MasterCard Product Identifier must always be used, when displaying account information or data i.e.,

- MasterCard *PayPass* or
- Maestro *PayPass*

4.6.1.1.1 Text Only Format

Conditional Requirement 4.6.1.1.1 – applicable for text based UIs that display account data

In UI Applications that are programmable in a text-only format (such as STK) the minimum requirement is for the correct MasterCard Product Identifier (in words) to be used when displaying the account details to which it corresponds. If the UI has technical limitations to the number of characters that can be displayed, suitable abbreviations can be used if agreed by MasterCard,

4.6.1.1.2 Graphical Format

Conditional Requirement 4.6.1.1.2 – applicable for graphics based UIs that display account data

In UI Applications that support a graphical display the minimum requirement is for the correct MasterCard Product Identifier (in image format) to be used when displaying the account details to which it corresponds.

This will also be subject to Branding Review to ensure the use of the image is in accordance with [*MasterCard PayPass Branding Standards*] or [*Maestro PayPass Branding Standards*] as applicable.

4.6.1.2 Sensitive Account Information Display

Issuers may wish to enable their account holders to view sensitive account data within the User Interface Application, such as full PAN, CVC2 and Expiry Date, which may be used for Card Not Present (CNP) transactions such as online or Mail Order and Telephone Order (MOTO) purchases. These requirements apply throughout the UI Application to any point that sensitive account holder data is displayed, be it in text or graphics formats.

Note

Issuers should refer to the Security Guidelines for Mobile Payments for further guidance on the handling and display of assets within User Interface Applications on mobile devices.

The display of sensitive account data is dependent on what level of user verification has taken place in order to determine the authenticity of the user as the legitimate owner of the account. Three levels of user verification are possible.

- The user is not verified as the account owner
- The user has been verified as the account owner by a password or passcode mechanism.
- The user has been verified as the account owner by mPIN entry and verification, using the Mobile MasterCard PayPass application.

Table 1 — Summary of the ways sensitive account information can be displayed

	User authentication verification method			
	None (variation 1)	None (variation 2)	Password/ Passcode	mPIN
PAN display	First four digits and last four digits maximum (Recommendation is to only show the last four digits)	Full Pan display is allowed	Full Pan display is allowed	Full Pan display is allowed
Expiry Date display	Allowed (Recommendation is to not show)	Not allowed	Allowed (Recommendation is to not show)	Allowed
CVC2 display	Not allowed	Not allowed	Not allowed	Allowed

4.6.1.2.1 Use of Card Layout Description

Recommendation 4.6.1.2.1 a

It is recommended that the PAN and Expiry Date are stored in the Card Layout Description in the Mobile MasterCard PayPass application.

Conditional Requirement 4.6.1.2.1 b – applicable if CVC2 is used in the UI

The CVC2 shall be stored in the Card Layout Description of the Mobile MasterCard PayPass application.

4.6.1.2.2 No User Verification, variation 1

These requirements and recommendations allow the UI Application to display an Expiry Date, partial PAN and no CVC2.

Requirement 4.6.1.2.2 a

Where the Account Data stored in the Payment Application is being displayed without any form of verification (such as an mPIN or other code), the display

of PAN data must be limited to, at maximum, the first and last four digits (eight in total), if the expiry date is displayed.

Recommendation 4.6.1.2.2 b

Where the Account Data stored in the Payment Application is being displayed without any form of verification (such as an mPIN or other code), it is recommended that only the last four digits of the PAN are displayed. The display of the first four digits is to accommodate card images that show the BIN/IIN in the image background.

Recommendation 4.6.1.2.2 c

Where the Account Data stored in the Payment Application is being displayed without any form of verification (such as an mPIN or other code), it is recommended that the Expiry Date is not shown.

4.6.1.2.3 No User Verification, variation 2

This requirement allows the UI Application to display the full PAN but no Expiry Date or CVC2.

Requirement 4.6.1.2.3

Where the Account Data stored in the Payment Application is being displayed without any form of verification (such as an mPIN or other code), the display of the Expiry Date is not allowed if a full PAN is displayed.

4.6.1.2.4 User Verified by Password/Passcode entry

These requirements and recommendations allow the UI Application to display the full PAN and Expiry Date but no CVC2.

Requirement 4.6.1.2.4 a

The display of Full Pan and Expiry Date but not CVC2 is permitted after the user has been verified as the account owner by a password or passcode authentication mechanism.

Recommendation 4.6.1.2.4 b

It is recommended that the Expiry Date is not shown with this authentication mechanism, and that mPIN entry is used when Full PAN and Expiry Date are to be displayed.

4.6.1.2.5 User Verified by mPIN entry

This requirement allows the UI Application to display the full PAN, Expiry Date and CVC2.

Requirement 4.6.1.2.5

The display of Full Pan, Expiry Date and CVC2 is only permitted after the user has been verified as the account owner by use of the mPIN verification mechanism.

4.6.1.2.6 Incorrect Account Information Display

Requirement 4.6.1.2.6

Any account information displayed by UI application must be the correct information for the account. In other words it is not allowed to display fake or substitute information on card images or text. Account data must accurately reflect the true account details within the bounds of the requirements for the display of sensitive data, such as either displaying data or displays masking characters like an asterisk. For example, the display of a card image with a fake PAN or a PAN of 0000 0000 0000 0000, would not be allowed.

4.6.1.3 Issuer Identifier

In UI Applications that include the function to display account data stored in a Payment Application, the relevant Issuer Identifier, e.g.: "AnyBank", must always be used, as detailed in the following requirements.

4.6.1.3.1 Text Only Format

Conditional Requirement 4.6.1.3.1 – applicable for text based UIs

In UI Applications that are programmable in a text-only format (such as STK) the minimum requirement is for the correct Issuer Identifier (in words) to be used when displaying the account details to which it corresponds. If the UI has technical limitations to the number of characters that can be displayed, suitable abbreviations can be used if agreed by MasterCard,

4.6.1.3.2 Graphical Format

Conditional Requirement 4.6.1.3.2 – applicable for graphics based UIs

In UI Applications that support graphical images the minimum requirement is for the correct Issuer Identifier (in graphical format) to be used when displaying the account details to which it corresponds.

This will also be subject to Branding Review to ensure the use of the Issuer image in conjunction with the relevant MasterCard Product Identifier (as detailed above) is in accordance with [*MasterCard PayPass Branding Standards*] or [*Maestro PayPass Branding Standards*] as applicable.

4.6.1.4 Account/Issuer Product Identifier

In UI Applications that include the function to display data stored in a Payment Application, the relevant Issuer Product Identifier must always be used to identify the account with which the data is associated, as detailed in the following requirements.

Examples of Issuer Product Identifiers are;

- "Cashback Credit" or
- "Current Account" or
- "Prepaid Account"

4.6.1.4.1 Text Only Format

Conditional Requirement 4.6.1.4.1 – applicable for text based UIs

In UI Applications that are programmable in a text-only format (such as STK) the minimum requirement is for the correct Issuer Product Identifier (in words) to be used when displaying the account details to which it corresponds. If the UI has technical limitations to the number of characters that can be displayed, suitable abbreviations can be used if agreed by MasterCard,

4.6.1.4.2 Graphical Format

Conditional Requirement 4.6.1.4.2 – applicable for graphics based UIs

In UI Applications that support graphical images the minimum requirement is for the correct Issuer Product Identifier (in graphical format) to be used when displaying the account details to which it corresponds.

This will also be subject to Branding Review to ensure the use of the Issuer Product Identifier image in conjunction with the relevant MasterCard Product identifier (as detailed above) is in accordance with *[MasterCard PayPass Branding Standards*] or [*Maestro PayPass Branding Standards*] as applicable.

4.6.1.5 Card Layout Display

The Mobile MasterCard *PayPass* M/Chip 4 Technical Specifications provide a facility for displaying a card image in the User Interface Application. Proprietary solutions for displaying card images or data are also permissible using existing MasterCard payment application specifications providing, they comply with the requirements set out in this document. Where sensitive account holder data is to be displayed, the requirements detailed in section 4.6.1.2 (Sensitive Account Information Display) apply.

Recommendation 4.6.1.5

For implementations based on Mobile MasterCard *PayPass* M/Chip 4, MasterCard recommends the use of the Card Layout Description feature to display the image of the card within the User Interface Application.

4.6.1.6 Card/Account Name set by Account holder

Recommendation 4.6.1.6

MasterCard recommends the use of a name for each account or card that is accessible from User Interface Applications which can be created by the account holder.

Note **MasterCard takes no responsibility for possible infringement of copyright or patents held by third parties relating to requirements or recommendations laid out in this document, including, but not limited to, the use of payment card images in User Interface Applications.**

4.7 Pre-Acknowledgement Quick Payment Access

The Mobile MasterCard *PayPass* M/Chip 4 Technical Specifications include a function to allow end-users to pre-acknowledge every transaction (to provide an additional control layer) even for Low Value Transactions.

4.7.1 Pay Now Button Recommendation

Recommendation 4.7.1

Where this feature, or an equivalent proprietary feature, has been implemented, MasterCard recommends the use of a "Pay Now" button as high up the menu structure of the User Interface Application as possible. The number of clicks the user has to make in order to pay should be kept to a minimum.

4.7.2 Differentiation between Two-Tap and failure to Pre-acknowledge

Recommendation 4.7.2

MasterCard recommends that UI Applications that include pre-acknowledgement should clearly distinguish between the PIN request following a failure to pre-acknowledge and the PIN required as part of a two-tap High Value Transaction.

The messaging in the first case should inform the user that the application is configured to require pre-acknowledgement or pre-signing and that the user should enter the PIN before attempting a transaction.

This recommendation is designed to avoid confusion between the "Two-Tap High Value Transaction" user experience and the "error case for failed pre-acknowledgement Low Value Transaction" user experience.

4.8 CVM and mPIN Administration

This section is concerned with the use of Cardholder Verification Method (CVM) solutions using an mPIN for High Value Transactions (HVT) and/or for Risk Management through a Risk Counter Reset Mechanism, as well as the administration of an mPIN using the UI.

For any UI that is designed to provide CVM through mPIN entry into the UI, and the administration of the mPIN (the mPIN is stored in the MasterCard Payment Application within the Secure Element), the requirements defined in this section apply.

4.8.1 Masking of mPIN

4.8.1.1 Payment

Requirement 4.8.1.1

When an mPIN is being entered for Payment (for example when the transaction amount exceeds the CVM limit, or in instances where the Issuer may require pre-signing for all transactions) the mPIN must always be masked when it is being entered into the UI (i.e. the digits should not be visible on the screen when they are being entered – instead symbols such as hash or star should be visible on the display).

4.8.1.2 Counter Reset

Requirement 4.8.1.2

When an mPIN is being entered for Counter Reset the mPIN must always be masked when it is being entered into the UI.

4.8.2 CVM for Payment using mPIN

Requirement 4.8.2

For transactions where the amount exceeds the CVM limit (or where the Payment Application is configured to always require pre-signing as defined below) the mPIN, as stored in the Payment Application, must always be used.

It is not acceptable to use any form of verification code that is stored within the UI or any other application running on the non-secure memory of the Mobile Device.

The mPIN must always be verified by the corresponding Payment Application.

Note

It is particularly important that requirement 4.1.3 Clear Cache Requirement is complied with wherever mPIN entry is supported/required by the User Interface Application.

4.8.3 Risk Management using mPIN (Counter Reset)

4.8.3.1 When Counter Limit has been reached, Automatic Initiation

Requirement 4.8.3.1

For User Interface Applications that interact with Payment Applications which include an Over The Air Counter Reset functionality the following requirement applies:

A means of automatically initiating the launch of the User Interface Application based on a payment related event must be supported, in order to enable user confirmation/verification of the counter reset request.

The most critical point at which this feature is needed is when the counter limit has been reached and a reset is required in order for further purchases to be possible.

4.8.3.2 Manual Initiation of Counter Reset

Requirement 4.8.3.2

All UI Applications that include user interaction to enable OTA Counter Reset, must also offer a function for the end-user to initiate a Counter Reset at any time that they choose (i.e. at any time after a transaction has taken place, in particular if the end-user has chosen to ignore a Counter Reset request that may have appeared immediately after a transaction which caused the Counter to reach its limit).

4.8.3.3 User Friendly Language

Requirement 4.8.3.3

User friendly language shall be used to describe the process, such that the end-user is not confused by the terminology they may not be familiar with. “Counter Reset” for example should not be used.

4.8.4 Security Word Display

Conditional Requirement 4.8.4 – applicable if the Security Word has been personalized in the Payment Application

MasterCard has defined a new data element for Mobile MasterCard *PayPass* M/Chip 4 Payment Applications: the “Security Word” which, when available in the Payment Application, must always be displayed when the end-user is being asked to enter their mPIN.

This is designed as an additional assurance feature for the benefit of the account holder.

4.8.5 Administration of mPIN

All UI Applications that include the use of an mPIN as a CVM should include mPIN administration functionality as defined below:

4.8.5.1 Create mPIN Function using Verification Mandatory

Requirement 4.8.5.1

Payment applications may be deployed without an mPIN having been set, to allow the end-user to create their own preferred mPIN at the point of activation. In such cases an additional verification is required to ensure that the end-user is the valid card/account holder. This can be done by using an additional numeric code that has been set by, or provided to, the end-user by the issuer or its agent. Other options include mailers with verification codes or call center-based processes with other customer verification methods.

4.8.5.2 Update mPIN Function

Recommendation 4.8.5.2 a

All UI Applications that include the use of an mPIN as a CVM should include functionality that enables an mPIN stored in a Payment Application to be changed.

Conditional Requirement 4.8.5.2 b – applicable if Update mPIN functionality is supported

Where manual mPIN update is supported, this must be implemented by asking the end-user to enter the existing mPIN once, followed by entry of the new mPIN twice before the mPIN in the Payment Application can be overwritten by the UI.

4.8.5.3 Unblocking mPIN using PUK

All implementations that include CVM functionality will include functionality that enables a blocked mPIN (i.e. when the mPIN retry counter limit has been reached) to be unblocked by means of an unblocking script which the issuer can send over the air.

Recommendation 4.8.5.3 a

It is recommended that all UI Applications that are used in implementations that include CVM functionality should also include functionality that enables a blocked mPIN (i.e. when the mPIN retry counter limit has been reached) to be unblocked by means of an unblocking code: PIN unblock code (PUK).

The PUK will typically be set by the issuer of the Payment Application.

Conditional requirement 4.8.5.3 b – applicable if the use of PUK is supported

The PUK should be entered once and the new mPIN shall then be entered twice before the mPIN in the Payment Application can be overwritten by the UI

Appendix A Requirements and Recommendations Summary

The following section contains a summary of the Requirements (REQ), Conditional Requirements (CREQ) and Recommendations (RECO) in a tabular format.

Table 4.1—Summary of the UI Requirements and Recommendations

General UI Application Requirements	
REQ 4.1.1	All UI applications must demonstrate stable operation and must not give unexpected errors or timeouts or show instability.
REQ 4.1.2	All visible functions and features must be active or operable. 'dead' links or menus are not allowed
REQ 4.1.3	For UIs that access and/or display any data from the Payment Application: Clear Cache Requirement
REQ 4.1.4	UI applications shall be assigned unique version numbers that must be user accessible
Provisioning support	
REQ 4.2	User authentication shall take place before OTA personalization
CREQ 4.2.1.1 a	If a Verification Code is used, it shall be a minimum of four characters long
RECO 4.2.1.1 b	Verification codes should be numeric
CREQ 4.2.1.2	If a Verification Code is used, it shall be masked during entry
Access Controls	
RECO 4.3 a	User Interface Applications should not have an additional access control "password" or "passcode"
RECO 4.3 b	When UI Access Control (by means of a Password that is not the mPIN) is implemented, the Password must not be referred to using the term "PIN"
RECO 4.3 c	Non-mPIN UI Passwords to different format to local "standard" or common PIN format
REQ 4.3 d	Non-mPIN Passwords must not be used as CVM for HVT
CREQ 4.3 e	Authentication must be performed before setting UI passwords (non mPIN)
Payment Application Activity Display	
REQ 4.4.1	Transaction Notification Requirement
RECO 4.4.1.1	In User Interface Applications where the user has the option to name the account or card, this name should also be displayed in the Transaction

	Notification.
CREQ 4.4.1.1.1	For Text only UIs that access and/or display any Payment Application: Text Only Display Format in Transaction Notification Requirement
CREQ 4.4.1.1.2 a	For Graphical UIs that access and/or display any Payment Application: Graphical Display Format in Transaction Notification Requirement
RECO 4.4.1.1.2 b	Text format can be used is technical limitation prevent graphical formats from being used
REQ 4.4.1.2	For UIs that access and/or display any Payment Application: Transaction Notification Prompt Display Speed Requirement
REQ 4.4.1.3	For UIs that access and/or display any Payment Application: Transaction Notification Display Duration Requirement
Single Card/Account Transaction Log Display	
RECO 4.4.2	For UIs that access and/or display any data from the Payment Application: Minimum Data Elements Displayed in Transaction Log View (Transaction Amount, Transaction Currency, Transaction Date) Recommendation
Consolidated Multiple Card/Account Transaction Log Display	
RECO 4.4.3.1	For UIs that access and/or display any data from the Payment Application: Minimum Data Elements Displayed in Transaction Log View (Transaction Amount, Transaction Currency, Transaction Date) Recommendation
RECO 4.4.3.2	For UIs with consolidated multiple Card/Account Transaction Log Display: Transaction List Order Recommendation
RECO 4.4.3.3	For UIs with consolidated multiple Card/Account Transaction Log Display: Transaction Identification Recommendation
Payment Application Management and Selection (single and multiple accounts)	
REQ 4.5.1	For UIs that access and/or display any Payment Application: Payment Application “Enable” Function Requirement
REQ 4.5.2	For UIs that access and/or display any Payment Application: Payment Application “Disable” Function Requirement
RECO 4.5.3	Support of the Payment Application blocking
CREQ 4.5.3.1	If Payment Application blocking is supported the Payment Application should be suitably marked
CREQ 4.5.3.2	If Payment Application blocking is supported the account holder should be given suitable information about the blocked application and information about any unblocking procedure
Multiple Payment Application Management	
REQ 4.5.4.1	For UIs that access and/or display multiple Payment Application: Default Function for Multiple Payment Applications Requirement
RECO 4.5.4.2 a	Support of one-time override of default Payment Application
CREQ 4.5.4.2 b	If one-time override of default Payment Application is supported, the default must revert to the original default Payment Application
CREQ 4.5.4.3.1	For Text based UIs that access and/or display multiple Payment

	Application: Text Only Display Format Requirement
CREQ 4.5.4.3.2	For Graphics based UIs that access and/or display multiple Payment Application: Graphical Display Format Requirement
Account Data	
CREQ 4.6.1.1.1	For Text based UIs with Account Data Display Enabled: MasterCard Product Identifier Used Text Only Format Requirement
CREQ 4.6.1.1.2	For Graphics based UIs with Account Data Display Enabled: MasterCard Product Identifier Used in Graphical Format Requirement
RECO 4.6.1.2.1 a	Sensitive Account Data should be stored in the Card Layout Description in the Mobile MasterCard PayPass Application
CREQ 4.6.1.2.1 b	If the CVC2 is used, it shall be stored in the Card Layout Description in the Mobile MasterCard PayPass Application
REQ 4.6.1.2.2 a	With no user authenticity verification, the display of the PAN shall be limited to, at maximum, the first and last four digits (eight in total) if the expiry date is displayed
RECO 4.6.1.2.2 b	With no user authenticity verification, only the last four digits of the PAN should be displayed
RECO 4.6.1.2.2 c	With no user authenticity verification, the expiry date should not be shown
REQ 4.6.1.2.3	With no user authenticity verification, the display of the expiry date is not allowed if the full PAN is displayed
REQ 4.6.1.2.4 a	The full PAN and expiry date is permitted to be shown after the users authenticity has been verified by a Password or passcode mechanism
RECO 4.6.1.2.4 b	mPIN verification should be used instead of Password or Passcode mechanisms.
REQ 4.6.1.2.5	The full PAN, expiry date and CVC2 shall only be displayed after successful authentication of the user by the mPIN verification mechanism
REQ 4.6.1.2.6	The display of incorrect (inaccurate, fake, generic) account information is prohibited.
CREQ 4.6.1.3.1	For Text based UIs with Account Data Display Enabled: Issuer Identifier Display in Text Only Format Requirement
CREQ 4.6.1.3.2	For Graphics based UIs with Account Data Display Enabled: Issuer Identifier Display in Graphical Format Requirement
CREQ 4.6.1.4.1	For Text based UIs with Account Data Display Enabled: Account/Issuer Product Identifier Display in Text Only Format Requirement
CREQ 4.6.1.4.2	For Graphics based UIs with Account Data Display Enabled: Account/Issuer Product Identifier Display in Graphical Format Requirement
RECO 4.6.1.5	The UI Application should use the Card Layout Description feature of Mobile MasterCard PayPass application
RECO 4.6.1.6	The user should be able to name each account
Pre-Acknowledgement Quick Payment Access	

RECO 4.7.1	Pay Now Recommendation
RECO 4.7.2	Differentiation Two-Tap and Pre-Acknowledgement
CVM and mPIN Administration	
REQ 4.8.1.1	For UIs that support CVM: Masking of mPIN in Payment Mode Requirement
REQ 4.8.1.2	For UIs that support CVM: Masking of mPIN in Counter Reset Mode Requirement
REQ 4.8.2	For UIs that support CVM: CVM for Payment using mPIN Requirement
REQ 4.8.3.1	For UIs that support CVM: Risk Management using mPIN (Counter Reset), Automated Counter Reset Initiation When Counter Limit is Reached Requirement
REQ 4.8.3.2	For UIs that support CVM: Risk Management using mPIN (Counter Reset), Manual Initiation of Counter Reset Process Requirement
REQ 4.8.3.3	For UIs that support CVM: Risk Management using mPIN (Counter Reset): User Friendly Language
CREQ 4.8.4	If the personalization data in the Mobile MasterCard *PayPass* M/Chip 4 Applications contains the Security Word, it shall be displayed when the user is being asked to enter their mPIN
REQ 4.8.5.1	For UIs that support CVM: Create new mPIN Function Requirement
RECO 4.8.5.2 a	The UI Application should include a function to update the mPIN
CREQ 4.8.5.2 b	If the UI Application includes a mechanism for the user to update the mPIN. Update mPIN Function Process Flow Requirement (double mPIN entry)
RECO 4.8.5.3 a	The UI should use a PUK mechanism to unblock mPIN once blocked
CREQ 4.8.5.3 b	For UIs that support CVM and mPIN unblock using PUK: Unblock mPIN using PUK Process Flow Requirement (double mPIN entry)