INTRODUCING M/CHIP MOBILE SIMPLIFYING THE DEPLOYMENT OF SECURE ELEMENT MOBILE PAYMENTS

OCTOBER 2015

GLOBAL MOBILE PAYMENT TRANSACTION VALUE IS PREDICTED TO REACH USD 721 BILLION BY 2017.[1]

Research into customer behavior has shown a strong preference to use smart devices in nearly all aspects of our lives. When smart devices are coupled with the MasterCard payment infrastructure the results provide innovative, omni-channel shopping and payment experiences. To stay ahead of the digital demands, MasterCard has developed M/Chip Mobile, a secure EMV Chip application for mobile payments. When loaded on the Secure Element of a smartphone or other mobile device[2] it enables face-to-face contactless payments and remote payments, securely and conveniently.

TABLE OF CONTENTS

Purpose of this document

This Introducing M/Chip Mobile document is high level in scope and suitable for anyone new to the subject wishing to gain a broad understanding of M/Chip Mobile, the MasterCard secure element based payment application, how it works, why it is important and how to use it to build compelling payment propositions.

For Cloud-based solutions please refer to MasterCard Cloud-Based Payment product literature.

1 Source: Gartner report "Forecast: Mobile Payments, Worldwide, 2013 Update," June 2013.
2 "Mobile Device" is the generic term used here to denote any mobile phone, smartphone, watch, tablet or wearable device that includes NFC functionality and can be used as part of an M/Chip Mobile implementation.

OVERVIEW

What is M/Chip Mobile?

M/Chip Mobile is a MasterCard specification to enable payments using a mobile consumer electronic device in a similar way they would use a contactless card. In effect, it allows MasterCard Issuers and their customers to load a digitized version of any MasterCard card on to a Secure Element (SE) of the device where it interacts with features of the device such as the communications capability, display and keyboard to support a range of new payment scenarios, securely and conveniently. MasterCard recognizes SIM/UICC cards,[3] embedded SE built in to OEM handsets and devices and removable SE such as suitable micro SD cards as secure elements.

M/Chip Mobile supports face-to-face mobile payments via a contactless interface using Near Field Communications (NFC). It also supports remote payments using MasterCard Digital Secured Remote Payments (DSRP) protocol. Remote payments can be initiated in several ways: for example from a merchant application on the device, scanning a QR code in-store, from a PC screen, or poster to capture the transaction on to the mobile device and then complete the transaction securely using DSRP.

MasterCard also support an alternative to SE based mobile payment via the MasterCard Cloud-Based Payment program.

How Does It Work?

M/Chip Mobile leverages highly secure EMV Chip technology, already used throughout the world for face-to-face plastic card payments. At the core of the solution is MasterCard M/Chip EMV payment application.

For both face-to-face and remote payments the M/Chip Mobile payment transaction is dynamic and protected by a unique EMV cryptogram. This means the transaction can be uniquely authenticated and cannot be fraudulently reused or replayed.

Consumers may be authenticated by PIN, either online using the point of sale (POS) PIN pad, or offline by entering the mPIN on the mobile device which is an example of a Consumer Device Cardholder Verification Method (CDCVM). CDCVM is the generic term for validating the consumer via mPIN, a PIN entered into the mobile and validated by the M/Chip Mobile application, or future consumer device verifications methods such as biometric or mobile device unlocks capabilities. Further details on CDCVM can be found at MasterCard Connect.

CDCVM is the preferred method for securing high value contactless payments and all remote payments. CDCVM may also be used for non-payment authentication transactions.

CDCVM and other features of M/Chip Mobile offer an optimized user and merchant experience at the latest generation of contactless terminals (MasterCard MCL3 terminals). However, M/Chip Mobile is also compatible with the existing contactless infrastructure where transactions at earlier generation terminals will not use CDCVM. Similarly, M/Chip Mobile is also interoperable with contactless infrastructures in markets where Mag Stripe mode contactless transactions is used.

The digitized card may use "Tokens" instead of "real" card account numbers (PANs) for additional security. A token is simply a surrogate PAN, used so that the real PAN is not exposed to the merchant. MasterCard provides a service for issuing tokens and mapping them back to real PANs. Refer to EMVCo Payment Tokenization for further details.

A "Wallet" or User Interface application allows the cardholder to interact with the payment application by, for example, choosing a card to pay with, entering a mPIN, responding to on-screen instructions or reading transaction details on payment completion. The wallet also supports over-the-air (OTA) communication with the M/Chip Mobile issuer, for application loading, updating and management – in other words, all the actions which would be carried out via script messaging with a contact chip card, and more.

M/Chip Mobile works with a wide range of wallets, from simple, single card applications to sophisticated, multi-card wallets. MasterCard MasterPass wallet is an example of the latter. MasterCard supports wallet developers with a User Interface Software Development Kit (UI SDK).

Delivering Safer Mobile Payments

According to Deloitte,[4] among UK adults that have not yet used their phone to pay in-store the most common reason given – cited by 42% – was "I don't think they are secure enough."

The M/Chip Mobile Specification is designed with the same EMV dynamic cryptogram technology to deliver safer mobile payment transactions.

3 UICC (Universal Integrated Circuit Card) is the new generation of SIM (Subscriber Identification Module) supporting multiple applications such as payment via one or more M/Chip Mobile applications.
4 Source: Deloitte, "The Mobile Consumer 2015: The UK cut Game of Phones," September 2015.

Benefits of M/Chip Mobile

M/Chip Mobile enables a new payments landscape of simple, secure digital transactions across any channel using any device. Bringing together the power and security of EMV chip with the ubiquity of the smartphone and other digital consumer devices, M/Chip Mobile is a flexible, standards-based platform which allows multiple stakeholders to work together to build attractive, easy-to-use and scalable new mobile payments solutions. MasterCard customers can use M/Chip Mobile to drive profitable business growth through cash displacement, product differentiation, access to new markets and reduced costs. Key benefits include:

- The convenience of low value tap & go™ contactless transactions without the need for either cash or plastic cards.
- Secure high value tap & go™ transactions above the contactless limit using CDCVM.
- Secure e-commerce payments over the internet with the same strong, two-factor authentication technology as already used for EMV chip face-to-face transactions worldwide.
- Support for alternative user checkout experiences such as "tap and wireless" (a payment initiated with NFC and completed remotely) or the use of QR codes.
- The choice of multiple payment accounts on the same phone, similar to a cardholder's traditional wallet or purse.
- The capability to interact with the information capture, display, storage and processing power of the mobile device to support a wide range of additional payments-related propositions such as confirmations, transaction histories, vouchers, location-based services and many more.
- Cost reduction – less need to manufacture, issue, and replace plastic cards.

Implementing M/Chip Mobile Products

Mobile payments can involve new stakeholders such as network operators, handset manufacturers and wallet providers in addition to traditional issuers, acquirers and merchants. M/Chip Mobile has been designed to be highly flexible and robust in order to accommodate this diversity, with multiple options to meet the needs of all stakeholders in all markets. M/Chip Mobile implementation is challenging and requires careful planning and execution to be successful. MasterCard has therefore put in place processes, procedures and support services to assist customers at every stage of the product lifecycle, including certification, user interface development, tokenization and the provisioning of digital credentials onto mobile devices. MasterCard acts as the trusted partner of both issuers and other stakeholders in the mobile ecosystem and provides end-to-end support and scalability.

Additionally, MasterCard has also developed a complete set of on-behalf-of (OBO) services called MasterCard Digital Enablement Service (MDES) covering all aspects of M/Chip Mobile product implementation and management. In support of mobile device-based payments, MDES provides issuers and wallet providers with a secure, simple, globally scalable platform, and integrated end-to-end OBO services for tokenization and digitization, all supported by the reliability and global reach of the MasterCard network. MDES will be particularly attractive to issuers wishing to launch M/Chip Mobile products without the resources to maintain compatibility with the latest mobile handsets and technology. For more details, please refer to:

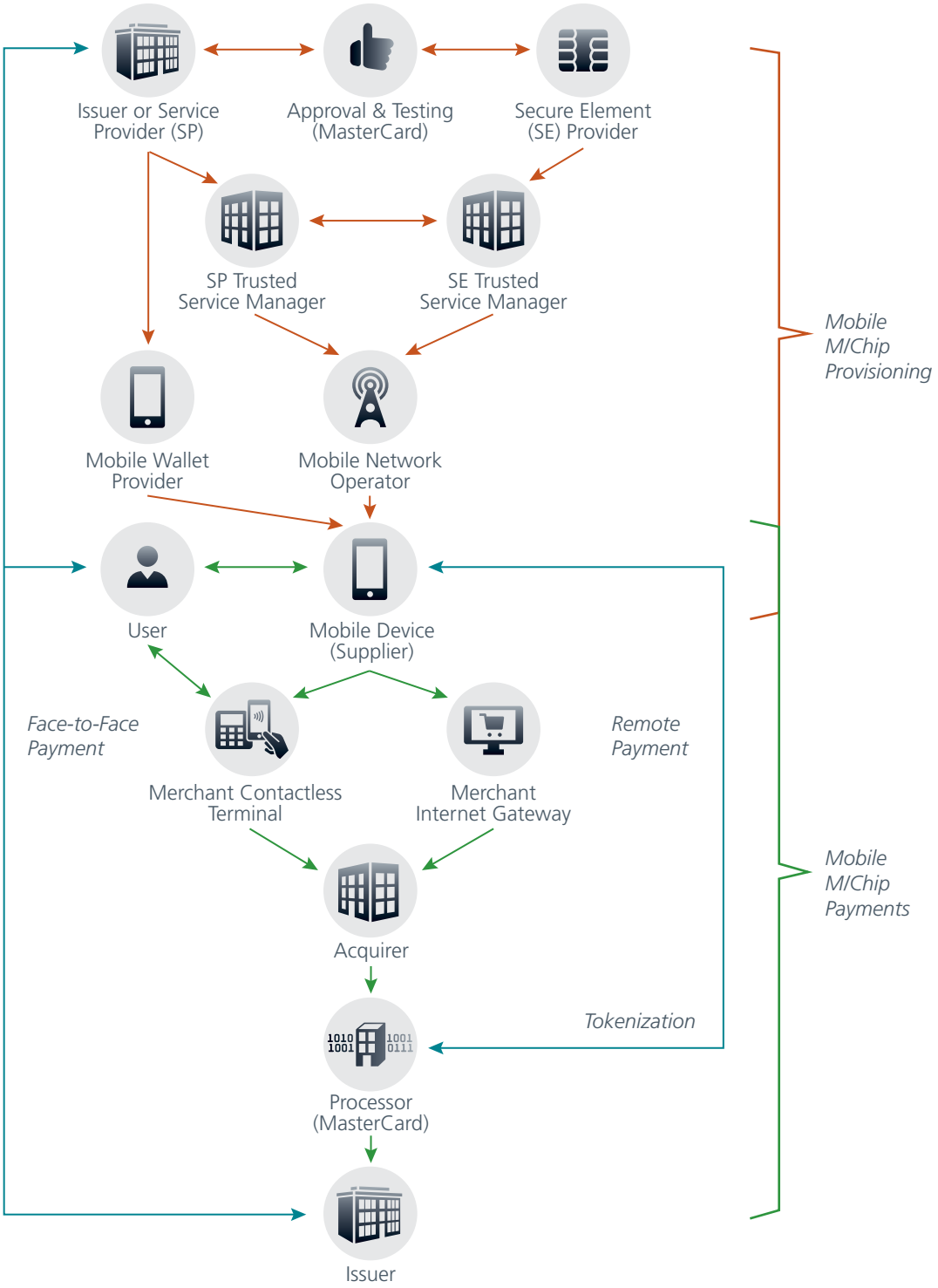
- *Mobile Digital Enablement Service, Issuer Implementation Guide*

THE MOBILE PAYMENTS ECOSYSTEM

Mobile payments involve several new stakeholders, traditionally not involved in the payments industry. Moreover, these stakeholders need to connect to multiple partners for example an issuer may need to work across several digital wallets and on a range of handsets, which typically have short lifecycles. The mobile payments ecosystem may be quite complex and presents new challenges. M/Chip Mobile has been designed to meet such challenges. It is a highly flexible platform with multiple implementation options. In order to ensure interoperability, all components of the platform are based on established standards, including EMV. EMVCo, the body which maintains the EMV standard, has now published specifications covering many aspects of mobile payments including contactless operation and tokenization for example. Other important standards include NFC, Java Card, GlobalPlatform, ETSI and other commonly used technologies surrounding the secure element and contactless interface. This interoperability from M/Chip Mobile standardization allows these stakeholders to support new partners quickly and scale.

Stakeholders

The diagram below illustrates the main stakeholders in a mobile payments program.



In practice, the same organization may fulfil multiple roles, each stakeholder function is logically distinct, as follows:

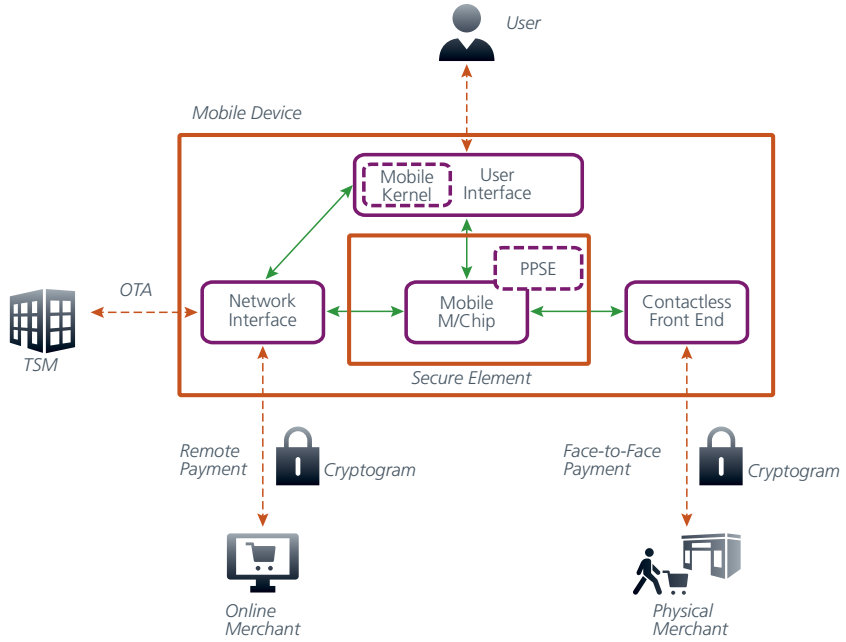
- **Issuer (or "Service Provider").** This entity, normally a bank, is ultimately responsible for providing the payment service to the cardholder and authorizing transactions. It is the bank with which the cardholder (user) has an account.
- **Service Provider (SP) Trusted Service Manager (SP-TSM).** A Trusted Service Manager (TSM) is an entity which interconnects payments industry and mobile communications industry stakeholders, typically several on both sides, to coordinate and simplify the provisioning and management of mobile payment solutions. The SP-TSM is similar to the Personalization Bureau in a card payments ecosystem.
- **Secure Element Provider.** This entity provides the Secure Element (SE) platform, and is responsible for the overall control of the SE. Examples of Secure Element Providers include a Mobile Network Operator (MNO) providing a UICC as the SE, a handset manufacturer providing an embedded SE, and a bank providing a microSD card with an SE.
- **Secure Element Issuer Trusted Service Manager (SEI-TSM).** A second TSM is used to manage the SE platform on behalf of the Secure Element Provider. The SE TSM manages the accesses to the Secure Element for Service Provider TSMs. Once again, the aim is to manage the complexity of the mobile payments ecosystem.
- **Mobile Network Operator (MNO).** The MNO may connects the mobile device to the TSM(s) alternatively this could achieved via the internet.
- **Mobile Wallet Provider.** The entity that provides and operates the User Interface or wallet application on the mobile device.
- **Mobile Device Supplier.** The handset manufacturer or other mobile device supplier. Typically, a mobile payment product will be required to work on a wide range of devices, which represents another challenge.
- **Consumer.** The consumer, or user of the payment product, often still referred to as the "cardholder."

The stakeholders above are all involved in M/Chip Mobile provisioning, a process which is subject to strict testing and approval processes to meet MasterCard standards. The following additional stakeholders are involved in mobile transactions, just as they are in traditional card payments:

- **Merchant.** The merchant may be a physical merchant where the mobile device is used to make a payment at a contactless terminal. Or it may be an online merchant where the mobile device is used to make a remote payment over the internet via the merchant's payment gateway.
- **Acquirer.** The bank which acts as the merchant acquirer. Note that there may be one or more specialized Payment Service Providers interposed between the merchant and the acquirer.
- **Payment Network.** This entity is normally MasterCard and involves several roles in addition to physically processing transactions, including optionally providing a Token Service, other customer services and of course managing the branded scheme. Apart from scheme management, all these roles may be undertaken by third parties in some circumstances.
- **Issuer.** The bank or other "card issuer" with which the user has an account (normally the same as the M/Chip Mobile Application Issuer).

INSIDE THE MOBILE DEVICE

The diagram below illustrates the main components of a mobile device configured for mobile payments.



The main components are as follows:

- **Secure Element.** A secure element (SE) is a tamper-resistant platform (typically a one-chip secure microcontroller) capable of securely hosting payment applications and their confidential and cryptographic data. The SE can be a UICC, or a microSD card, or embedded within the device hardware. It must have been approved within MasterCard's Compliance Assessment and Security Testing (CAST) process.
- **M/Chip Mobile Application.** The MasterCard M/Chip application, just as in a plastic card, is responsible for several critical functions such as generating transaction information including the cryptogram, mPIN verification and risk management. The M/Chip family has evolved through various versions, which has been designed to support full integration of contactless payments. There may be several instances of M/Chip within the SE, each one supporting one "card" in the mobile wallet.
- **Proximity Payment System Environment (PPSE).** If the device supports contactless payments, the SE also contains the PPSE, an application that points to the currently selectable payment application(s) within the SE in the form of Application Identifiers (AIDs) and their associated priority order.
- **Mobile Kernel.** A virtual contactless terminal on the mobile device that interfaces to the M/Chip application and constructs the DSRP data.
- **Contactless Front End.** This comprises the NFC controller and antenna for communicating with a contactless terminal.
- **Network Interface.** This uses the mobile device's wireless connectivity for normal access to the internet in order to:
  - Communicate with an online merchant via a payment gateway
  - Communicate directly or indirectly with the SP-TSM "over-the-air" (OTA) for application loading, updating and management, and other functions

- **Wallet.** The User Interface enables cardholder interaction with the payment application and other device features in order to select a payment method, or enter a PIN for example. There may be several User Interfaces, one for each payment application, or there may be just one in the form a mobile wallet such as MasterPass.

These components can be integrated, that is, built into the handset at manufacture, or semi-integrated with one or more components in the form of a plug-in module.

M/CHIP MOBILE TRANSACTIONS

M/Chip Mobile supports two types of payment:

- MasterCard contactless face-to-face payments
- Remote payments using MasterCard Digital Secure Remote Payment (DSRP)

Key features of M/Chip Mobile payments, which apply to both these types of payment, are:

- Every EMV transaction results in a unique, dynamic cryptographic code called a cryptogram, which proves the payment application on the mobile device is genuine and means the transaction cannot be fraudulently replayed. In countries with a magnetic stripe card infrastructure, a contactless mobile transaction will result in a dynamic Card Verification Code, in this case called the dCVC3.
- Apart from low value contactless transactions, an M/Chip Mobile transaction will normally involve a strong Cardholder Verification Method (CVM), this can be achieved using Consumer Device Cardholder Verification Method (CDCVM): A PIN entered on the device and verified by M/Chip Mobile application is called an "mPIN". It may be different from the PIN used with plastic cards to reduce the risk of cross-channel contamination. The result of Consumer-Device Cardholder Verification is signed in the transaction cryptogram, which hence becomes a proof of cardholder authenticity. Transactions can also be approved by the consumer terminal based CVM processing, such as online PIN.
- M/Chip Mobile uses a set of EMV counters and accumulators to force CDCVM verification whenever the number or accumulated value of non-verified transactions reaches pre-set limits. This prevents repeated use of a lost or stolen mobile device for low value transactions.

Face-to-Face Payments at Contactless Terminals

For low value payments at a contactless POS terminal below the "contactless limit" (typically below $50), the mobile device is presented to the terminal and is used in exactly the same manner as a contactless plastic card. In other words, the user taps the mobile device on the terminal and the transaction completes.

For high value transactions above the contactless limit, a Cardholder Verification Method is required, either CDCVM or terminal based cardholder CVM processing, such as online PIN.

Online PIN verification, in those countries where it is supported, is exactly the same as an online PIN verification with a contactless plastic card. The consumer is prompted to enter a PIN on the POS PINpad, enters it, and the PIN is verified online by the issuer.

mPIN is a form of CDCVM and involves the user entering the PIN on a keyboard on the mobile device where it is verified offline by the M/Chip Mobile application. Two use cases are supported:

- **Pre-PIN Entry.** With Pre-PIN Entry, or One-Tap, the cardholder completes CDCVM, typically while waiting in the line or queue, before they tap it on the terminal or reader to pay.
- **Two-Tap.** With Two-Tap, the cardholder taps their device onto the terminal or reader to start the transaction, moves their phone away for CDCVM to be entered when prompted, and taps again to complete the transaction.

CDCVM will only work with new versions of the MasterCard contactless terminal – MCL V3 and above. These are being rolled out globally. With contactless terminals which have not been upgraded, the mobile device will be treated as a contactless plastic card. In some countries, signature verification by signing a receipt is supported.

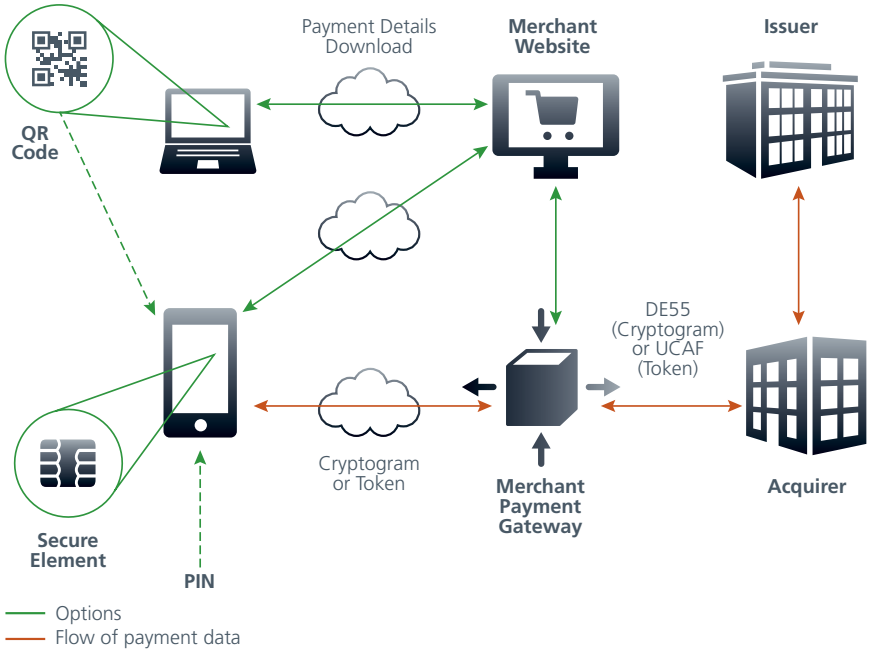
The particular procedures to be used for M/Chip Mobile contactless payments can be set by the issuer, optionally with some degree of cardholder control via the User Interface. In practice, the procedures used will vary from country to country according to local rules for contactless transactions and the type of terminals installed. MasterCard will advise on appropriate issuer strategy.

Remote Payments using DSRP

M/Chip Mobile can also be used for secure remote payments over the internet at online merchants using MasterCard Digital Secure Remote Payment (DSRP). Payments may be mobile browser-based or "In-App", meaning that the payment is initiated from an app on the mobile device. The cardholder can then be authenticated using CDCVM. M/Chip Mobile application then generates an EMV cryptogram, which is returned by the mobile device to the merchant. The merchant submits this cryptogram as part of the authorization request message.

DSRP can be extended to other use-cases such as remote shopping via a PC, tablet, TV or even printed posters or in-store displays. In this case, the transaction details are retrieved by a mobile application by for example simply scanning a QR code or tapping an NFC tag. Note that these techniques may be used at a POS to initiate a face-to-face payment that is then concluded using DSRP.

The DSRP process is illustrated in the diagram below.



M/Chip Mobile with DSRP represents a major step forward for the card payments industry by extending highly secure EMV chip processing from face-to-face contact and contactless to remote payments and as such is a milestone in the battle against rising levels of e-commerce fraud.

Authentication Transactions

Optionally, mobile devices can be configured to support non-payment Authentication transactions using a mechanism similar to DSRP, provided the issuer has installed a suitable authentication server.

Management Transactions

A key advantage of M/Chip Mobile over M/Chip-enabled plastic cards is the availability of over-the-air (OTA) communication via the mobile network between the payment application and the issuer or SP-TSM. With EMV plastic cards, communication is only possible, during the transaction, while the card is inserted in the contact reader. For M/Chip Mobile, OTA communication, is however always available, providing another channel for a user with a suitably configured User Interface to carry out a wide range of useful functions such as balance reporting, viewing past transactions, unblocking PINs, and more.

RISK MANAGEMENT

Mobile payments are a relatively new phenomenon and cardholders are naturally nervous about the security implications. M/Chip Mobile has therefore been designed to be highly secure; in fact in several respects the security features are arguably superior to those available with a chip and PIN plastic card transaction.

EMV chip technology

Security is, of course, underpinned by the EMV technology embedded at the core of the M/Chip Mobile platform. This means that M/Chip Mobile transactions, both face-to-face and remote, can be protected by the same risk management features which apply to EMV chip plastic card transactions at the physical point of sale, including:

- **EMV Card Authentication Methods (CAM)**, resulting in a unique cryptogram. This protects against counterfeit mobile payment applications and ensures that transactions cannot be replayed.
- **EMV Cardholder Verification Methods (CVM)**, including CDCVM. This protects against fraudulent use of lost or stolen mobile devices. The option of No-CVM is also available for low value transactions, and CDCVM means that utilized for remote payments.
- **EMV offline risk management.** While offline transactions are generally quicker and therefore more convenient, online transactions allows issuers to decline transactions for accounts when the consumer has reported a card or device stolen, or when the issuer suspects fraud is occurring. Issuers may configure the frequency of online transactions; they may even choose to require systematic online authorization.

Use of Counters and Accumulators

The M/Chip application in an EMV plastic card makes use of counters and accumulators for offline risk management. An issuer can set these counters to force an online authorization whenever the number – or cumulative amount – of offline transactions has reached certain limits. Whilst online, the counters of the plastic card counters and accumulators can then set to zero. These EMV counters are also used for risk management within M/Chip Mobile, with the enhancement that the counter reset command does not occur during the payment transaction, but is be applied over-the-air (OTA) at any time.

In addition, M/Chip Mobile makes use of another set of "No-CDCVM Counters" which periodically force CDCVM after a certain number – or accumulated amount – of No-CDCVM transactions. In contrast to the EMV counters, the No-CDCVM counters are locally controlled and require no online or OTA script to be reset: they are reset following a successful CDCVM. This limits the potential loss from a lost or stolen mobile device being fraudulently used repeatedly for low value transactions without access to the PIN or other CDCVM.

Use of Tokens

M/Chip Mobile can be tokenized. Payment tokens are aliases of the source account using an alternative Primary Account Number (PAN) linked back to the primary account during authorization de-tokenization. During de-tokenization the digital account is securely mapped back to the original PAN. The tokens are limited in their use to the particular channel of payment supported by the device, for example limited to contactless and DSRP transaction.

M/Chip Mobile complies with the Technical Framework for a Payment Tokenization Specification recently published by EMVCo.

Other M/Chip Mobile Risk Management Features

Other M/Chip Mobile risk management features which can be used to enhance security include the following:

- **Payment Activation – "Say When I Want To Pay."** This allows the cardholder to allow a contactless payment, whether low value or high value, only when they agree to make a payment.
- **Amount Acknowledgement – "Confirm Amount I Want To Pay."** This is the process of obtaining a positive action by the consumer, typically a single press to confirm that they approve the transaction

amount. When applicable, for instance for high value contactless transactions, Amount Acknowledgement can be combined with CDCVM entry between the first and second tap.

It is also worth reiterating that security features are embedded throughout the whole M/Chip Mobile ecosystem, particularly in terms of:

- The use of Secure Elements.
- The Trusted Service Manager function.
- Strict MasterCard testing and approval processes.

IMPLEMENTATION GUIDELINES

M/Chip Mobile is a very powerful platform which has been designed to be as flexible as possible in order to support a wide range of possible new payment products now and in the future. Implementation involves working within a new and extended payments ecosystem and choosing between options and concepts which may be relatively unfamiliar. MasterCard has therefore documented implementation options clearly and has put in place the tools and processes to assist customers and other stakeholders to the maximum extent. For details, please refer to:

- M/Chip Mobile Issuer Implementation Guide
- MasterCard Mobile Partner Website: mastercard-mobilepartner.com

The following guidelines summarize the main implementation considerations which need to be taken into account:

- **Launch planning.** The key to a successful implementation is to prepare thoroughly in advance by identifying impacts, assessing scope, choosing appropriate solutions, and translating these into a set of clear requirements and deliverables. Particular attention needs to be given to risk management strategy.
- **Consumer proposition.** Building the right cardholder proposition is a key contributor to the success of any program. The proposition for an M/Chip Mobile deployment must be aligned to the expectations of the target cardholders and designed accordingly.
- **Designing the user interface.** M/Chip Mobile enables a rich cardholder experience and designing a powerful but intuitive User Interface is particularly challenging. MasterCard has developed the Mobile UI Software Development Kit, a programmer-friendly set of functions that make it easy for today's application developers to rapidly deliver User Interface applications.
- **Issuer system impacts.** The M/Chip Mobile specification has been designed to minimize the impact on issuer systems, particularly for those issuers that already support contactless payment. The main impacts relate to application loading and personalisation.
- **Application loading and personalization.** A key benefit of mobile payments is the ability to instantly deliver a personalized payment application over-the-air to the cardholder. This raises a number of new issues that must be carefully managed, including: the sign-up process (Identification and Verification); ensuring handsets are compatible and identified; ensuring the Secure Element is compatible and identified; and reliability of loading. MasterCard provides support in all these areas.
- **Testing and approval process.** To ensure integrity and interoperability, all elements of an M/Chip Mobile implementation are required to be Type Approved by MasterCard. This extends not just to the traditional elements of a card payment product, but also to new components of the ecosystem such as the Secure Element, Mobile Device, User Interface, Contactless Front End and Trusted Service Manager(s).
- **M/Chip Mobile licensing.** MasterCard has developed a comprehensive licensing framework applicable to all stakeholders in the M/Chip Mobile ecosystem.

Additional Resources

Visit **mastercardconnect.com** and download the following resources:

M/Chip Mobile Issuer Implementation Guide

M/Chip Mobile Technical Specification

For details and specifications on MasterCard Cloud payment solutions contact MasterCard at **mcbp@mastercard.com**

We're ready to help. For more information, contact your MasterCard relationship manager.