INTRODUCTION TO
MASTERCARD CONTACTLESS READER v3.0
Contents

1. Introduction .................................................................................................................2

2. Background ..................................................................................................................3
   2.1 Reader Applications .................................................................................................3
   2.2 Built on Solid Foundations ......................................................................................3
   2.3 Contactless Cards, Data Storage, and Mobile NFC Devices .........................4
   2.4 Introducing MCL 3.0 .............................................................................................5

3. Close Integration with Mobile NFC Payment ............................................................6
   3.1 On Device Cardholder Verification (ODCV) .........................................................6
   3.2 Two-Tap Transactions—Optimized Use of NFC Device Security Features .......................7
   3.3 Enhanced CVM Selection Mechanism ..................................................................9

4. Data Exchange and Data Storage ..............................................................................10
   4.1 Data Exchange—Data Interaction with the POS System .....................................10
   4.2 Data Storage—Innovative On-Card Data Storage Capabilities ......................10
   4.3 Standalone Data Storage (SDS) .............................................................................10
   4.4 Integrated Data Storage (IDS) ...............................................................................11

5. Enhanced Payment Features .......................................................................................12
   5.1 Torn Transaction Recovery ......................................................................................12
   5.2 Balance Reading and Display ...............................................................................13
   5.3 Zero-Amount Transaction on Online-Only Reader .............................................13
   5.4 Offline Card Authentication Without Payment Transaction .........................13
   5.5 Transaction Amount Management .........................................................................14
   5.6 Enabling the Use of the POS Certificate Revocation List ...............................14

6. Contact .........................................................................................................................15

7. Appendix 1. MasterCard Contactless Reader v3.0
   and EMV Book C-2 .....................................................................................................16
1. Introduction

This document is an introduction to MasterCard Contactless Reader v3.0 (“MCL 3.0,” formerly referred to as “PayPass Reader v3.0”), the new version of MasterCard’s payment specification for contactless acceptance devices. MCL 3.0 is an evolution from the previous application “PayPass—M/Chip Reader v2.0” (or “PayPass Reader v2.0”) and has been developed by MasterCard in response to the significant innovation in the contactless payments landscape over the past few years. The document describes the new features and functionality of MCL 3.0, which reflect this change and enable MasterCard customers to take advantage of new contactless payment opportunities such as mobile NFC and data storage, whilst preserving the simplicity of the contactless POS experience.

The scope of this document is restricted to the new features introduced in MCL 3.0. It describes the “what,” not the detailed “how.”

The primary intended audience for this document is acquirers and merchants.
2. Background

2.1 Reader Applications

When an EMV transaction takes place, there is a dialogue between the payment application on the card and the one on the reader, the payment application on the reader being called the “kernel.”

For contact transactions, although the EMV standard, maintained by EMVCo, defines this dialogue through a common kernel, each payment scheme has its own card application specification.

These contact card applications are designed in different ways and may support additional proprietary features but they are all fully compliant with the EMV kernel. The MasterCard family of applications is called M/Chip, and M/Chip is now established as the MasterCard core EMV platform supporting all MasterCard-branded payment products.

As the payments market evolves, these applications also evolve. In MasterCard’s case, there has been an evolution of the M/Chip family of card applications from M/Chip 2, through M/Chip 4 to M/Chip Advance.

For contactless transactions, however, there is no common kernel and each payment scheme requires the use of its own kernel to work with their proprietary contactless card application. MCL 3.0 is the latest and most advanced version of MasterCard’s contactless kernel. The relationship between MCL 3.0 and the “EMV Contactless Specifications for Payment Systems” is described in Appendix 1.

The subsequent sections in this chapter describe how the MasterCard contactless kernel evolved into MCL 3.0, in parallel with the emergence of contactless payments and the evolution of the M/Chip family of card applications into M/Chip Advance and Mobile MasterCard PayPass.

2.2 Built on Solid Foundations

While contact EMV payments rely on an architecture designed by EMVCo, MasterCard launched in 2003 a brand new proprietary specification to facilitate contactless payments: the PayPass specification.

This specification has been licensed to all leading terminal manufacturers around the world, from which they have created the contactless readers currently used with all MasterCard branded contactless card programs worldwide.

Following a first generation of releases, PayPass Reader v2.0, published in 2008, introduced a mature payment infrastructure for MasterCard contactless card programs and remains today a proven and reliable platform for merchants. This application was upgraded in 2010 into v2.1 by adding refund functionality to the core payment function.
2.3 Contactless Cards, Data Storage, and Mobile NFC Devices

Since the launch of contactless cardholder devices, there have been a number of significant market developments that are driving demand for enhancements and innovation through two main product initiatives: on-card data storage capability and mobile NFC payments.

As payments trend towards a commodity product, issuers and acquirers are constantly searching for ways to add value to the core payment functionality. Issuers need marketing options that make their cards more likely to be chosen, activated, and remain top of wallet whilst acquirers seek opportunities to support merchants with speed and customer loyalty. Using the payment device as a secure token to carry customer information—which can be dynamically updated in a secure way—offers new opportunities for added value created by issuers and acquirers. This can range from carrying loyalty information to ticketing or simply customer identifiers.

To address these emerging needs in the market MasterCard released in 2009 the powerful M/Chip Advance specification. M/Chip Advance encompasses a contact and contactless integrated chip card specification and related solutions and services. It delivers the latest functionality demanded by MasterCard issuers around the world, protects existing issuer M/Chip investments, facilitates issuers’ entry into new markets, and facilitates the migration from previous M/Chip card platforms.

Besides these plastic card products, the emergence of smartphones and cost effective NFC implementations led to the development of NFC payment solutions embedded into mobile devices.

Supporting innovation in the mobile space, MasterCard released in 2011 Mobile MasterCard PayPass, which is the first contactless payment specification for mobile NFC devices. This new payment application enhances the payment features of traditional contactless only devices by leveraging the use of a screen, a virtual keypad, and a network connection. These capabilities allow a Mobile MasterCard PayPass application to display specific information, such as the list of available payment products or transaction history. They also allow the mobile device holder to interact with the device by, for example, entering a PIN on the mobile device (“mPIN”) to authenticate the cardholder, or choosing a payment product to pay with, or to communicate Over-The-Air with the issuer host to load, update, and manage the payment application and security parameters.
2.4 Introducing MCL 3.0

In 2011 MasterCard introduced “PayPass—M/Chip Reader Card Application Interface Specification v3.0” (PayPass Reader v3.0). In 2014 this product was renamed MasterCard Contactless Reader v3.0 (MCL 3.0)—the subject of this document. This was in line with MasterCard’s decision to align MasterCard® PayPass™ brand standards to support the company’s digital product convergence strategy, resulting in the August 2015 retirement of the PayPass brand and, instead, the use of the more descriptive word “contactless” to describe the term (along with the MasterCard and Maestro brands).

This latest version in the MasterCard contactless reader family leverages the proven stability and efficiency of PayPass Reader v2.0 and v2.1 by building a new architecture around its payment core. It offers an acceptance infrastructure that benefits from the innovations introduced in the latest cardholder device specifications, including specific functionality for the use of mobile NFC devices as contactless payment devices and the availability of Integrated Data Storage for M/Chip Advance products.

Through these new features and mechanisms described in this document, MCL 3.0 enhances your existing contactless payment assets by enabling new business opportunities.

As the new contactless payments landscape has evolved, especially with respect to mobile payments, a wide range of possible payment processes and experiences has emerged which, if not managed carefully, might undermine the inherent simplicity of the tap & go™ experience. MCL 3.0 is designed to address this potential complexity. MCL 3.0 is a powerful application which supports a wide range of configuration options to meet the increasingly distinct needs of different merchants and acquirers in different markets. Whilst terminal vendors all have to implement the full set of options, MCL 3.0 enables merchants and acquirers to choose between these configuration options in a straightforward manner, allowing them to configure any product to meet their special circumstances. In this way vendors have the widest opportunity to market their products while merchants and acquirers have a wide range of available suppliers that can meet their market needs. In addition, several of the new features of MCL 3.0 have been designed to result in a more streamlined and intuitive POS experience, building on the lessons learned with PayPass Reader v2.0 in markets around the world.

The next chapters describe the key features of MCL 3.0, which address the changing contactless payment business considerations discussed above. Each chapter includes use cases to illustrate how these features might be used by innovative merchants and acquirers to develop new payment products and leverage new business opportunities. The new features are grouped under the following headings:

- Close Integration with Mobile NFC Payment
- Data Exchange and Data Storage
- Enhancing Offline Prepaid
- Enhanced Payment Features
3. Close Integration with Mobile NFC Payment

Mobile PayPass is the MasterCard program that empowers MasterCard and Maestro payment products for use with mobile devices in a face-to-face environment. This allows MasterCard and Maestro payment products to be loaded onto a mobile phone or other portable device. Multiple payment products can be loaded on the same phone, acting for the cardholder as a traditional wallet or purse.

Payment can be made by tapping the phone onto the reader in a similar manner to the “tap & go” process used with a contactless card.

And whilst using the mobile phone for payments is as simple as tapping a card, there are many more opportunities available for secure, controlled, flexible and creative payments.

3.1 On Device Cardholder Verification (ODCV)

Higher value transactions are more susceptible to fraud, therefore cardholders, issuers and merchants want the security of verified payments. As well as supporting the familiar online PIN, the availability of a keypad and screen on a mobile device enables new opportunities.

On Device Cardholder Verification (ODCV) is based on an interaction between the cardholder1 and the mobile NFC device. At the end of the verification the mobile device itself provides confirmation of the successful verification to the contactless reader.

MasterCard Contactless Reader v3.0 (MCL 3.0) supports a mechanism that allows the mobile device to authenticate the cardholder through ODCV, thus enabling fast and secure payments for the merchant.

The primary use of ODCV implemented by MasterCard is “mPIN.” This involves simply entering a special PIN on the mobile device, normally using a virtual keypad displayed on the device screen. As MCL 3.0 does not need to know the method used by the mobile NFC device to verify the cardholder, innovative on-device methods of cardholder verification can be integrated into the mobile capabilities palette without impacting the ODCV mechanism.

This new feature brings important added value to the stakeholders in the mobile NFC payment ecosystem. The following use cases illustrate how MCL 3.0 with ODCV makes possible several new payment options for High Value Transactions2:

Markets that do not support High Value Transactions for contactless cards can be enabled for High Value Transactions for mobile NFC devices

In a market where the POS acceptance environment does not support Online PIN, High Value Transactions are sometimes limited to the use of signature or are not supported at all.

An acceptance infrastructure supporting ODCV provides cardholders the ability to perform High Value Transactions using their mobile NFC device.

---

1. The generic term “cardholder” is, for convenience, used throughout this document to refer to a payer using either a plastic card or any other payment device such as an NFC-enabled mobile phone.

2. A High Value Transaction is a contactless transaction where the amount is higher than the CVM Limit. A transaction below or equal to the CVM Limit (Low Value Transaction) does not require any Cardholder Verification while a High Value Transaction requires a Cardholder Verification.
**Terminals without PIN Entry Device can be enabled for High Value Transactions**

Unattended terminals that do not carry a PIN Entry Device, such as vending machines, are normally limited to Low Value Transactions.

Deploying contactless readers loaded with MCL 3.0 and supporting ODCV enables High Value Transactions in such environments.

This may ultimately allow similar payment options with other unattended terminal types such as parking tolls.

**ODCV enables more secure offline High Value Transactions**

High Value Transactions based on amounts between the CVM Limit and the Floor Limit can be performed offline using appropriate Cardholder Verification Methods.

While cards may be limited to signature as a CVM for offline High Value Transactions, which is not an ideal user experience in a Chip & PIN market, mobile NFC devices provide the opportunity to use PIN-based ODCV which is more secure than signature.

This feature brings increased payment options for merchants and cardholders and promotes the use of mobile NFC device as the best top-of-wallet option.

**3.2 Two-Tap Transactions—Optimized Use of NFC Device Security Features**

One of the enhancements introduced in the Mobile MasterCard PayPass application is the opportunity for the cardholder to control the transaction by acknowledging steps in the transaction processing through a button push or an mPIN entry. Depending on the sequence of operations, “two taps” might be required to complete a transaction.

The security features that can be addressed by the cardholder through the Mobile PayPass User Interface of the mobile NFC device are as follows:

- Acknowledgement of the activation of the application and of the amount of the transaction
- Reset of Financial Risk Management counters
- Reset of Lost & Stolen Management counters.

These features can be configured to be validated through the use of an mPIN and/or by a button push.

Using MCL 3.0 ensures a smoother user experience for both the cardholder and the merchant during a two-tap transaction.

- The merchant does not have to interact in any way with the MCL 3.0 reader between the two taps, thereby avoiding the potential for concern by the merchant that there is a problem with the payment after the first tap.
- Screen messages on the reader prompt the cardholder to check the instructions on their phone.
- The cardholder can complete the mobile security verification steps without having to explain any details to or involve the merchant (e.g., why this is the regular behavior of the mobile device).
An MCL 3.0 reader supporting ODCV recognizes that mPIN has been entered at the beginning of the transaction for acknowledgement, and does not require the cardholder to enter it again for CVM purposes when applicable.

**A smoother user experience**

The following example describes the user experience for a cardholder performing a Low Value Transaction, which does not require any Cardholder Verification. The mobile is configured to require the acknowledgement of the amount by the cardholder for each transaction, whatever the value.

- When invited by the merchant, the cardholder taps the mobile NFC device on the contactless reader.
- During the tap the reader transmits the transaction details to the mobile and recognizes during the exchange the specific information returned by the mobile indicating that a button push or a PIN entry is required on the mobile before completing the transaction. Based on this request the reader stops the transaction and displays to the cardholder a message informing them to look at the display of the mobile.
- When looking at the display of the mobile, which operates the Mobile PayPass User Interface, the cardholder understands that they must acknowledge the amount of the transaction by pushing the OK button. Once acknowledged, the cardholder can tap the mobile a second time.
- During the second tap the reader resumes the transaction and recognizes that all conditions are now fulfilled for the mobile to proceed with the transaction completion.

The request for the two-tap interaction comes from the mobile and is therefore fully independent of the contactless reader.

**MasterCard Contactless Reader 3.0 supporting ODCV removes the risk of a double PIN Entry**

Prior to MCL 3.0, complications might arise from the following situation:

- The mobile NFC device supports both mPIN and Online PIN and is configured to always request an acknowledgement for the transaction amount through mPIN
- The reader is not MCL 3.0 or is MCL 3.0 but only supports Online PIN and Signature as CVM (no ODCV support)
- The cardholder wants to perform a High Value Transaction

In such a case the cardholder has to acknowledge through mPIN the amount of the transaction after the first tap while he also has to enter the Online PIN on the PIN Entry Device of the reader as Online PIN was selected as the transaction CVM.

An MCL 3.0 reader supporting ODCV recognizes that mPIN has been entered at the beginning of the transaction for acknowledgement, and does not require the cardholder to enter it again for CVM purposes when applicable. This benefit is not valid for other acknowledgements done through the push of a button.
3.3 Enhanced CVM Selection Mechanism

The CVM Selection mechanism used during a transaction involving a mobile NFC device and MCL 3.0 is different from the standard selection for cards since the mobile can be used to authenticate the cardholder.

- If MCL 3.0 is configured not to support ODCV or if the cardholder device does not indicate support for mPIN, then the reader performs CVM processing based on the CVM List for an EMV mode transaction, and optionally can delegate CVM processing to the terminal for a mag-stripe mode transaction.

- If ODCV is supported by the reader and mPIN by the cardholder device, then the reader delegates the CVM processing to the mobile device and does not refer to the CVM List.

Introducing Terminal Risk Management Data

The Terminal Risk Management Data data object is used to inform the cardholder device about the availability of certain functionality on the terminal. It covers generic functionality on both the contact and contactless interfaces of the terminal such as CVM capabilities for contact and contactless transactions.

Terminal Risk Management Data may be requested by the cardholder device at the beginning of the transaction processing.


Enabling Online PIN as the preferred Issuer CVM

An issuer may support both online PIN and mPIN on a device and prefer online PIN. Such CVM configuration is possible by using this new mechanism, which provides issuers with superior control over the CVM that will be used during the transaction. It is available on selected implementations of mobile NFC devices.
4. Data Exchange and Data Storage

4.1 Data Exchange—Data Interaction with the POS System

Data Exchange is a mechanism that allows for a richer interaction between MCL 3.0 and the POS system, and allows the POS to influence the transaction flow.

Depending on the POS implementation and the contactless reader configuration, certain transaction parameters (e.g., transaction amount) can be updated by the POS during the transaction flow while the contactless cardholder device is still present in the contactless reader field.

A straightforward use case for merchants is an enhanced transaction flow that would modify transaction parameters based on data read from the card. For example, the merchant application could retrieve a loyalty ID from the card and request the reader to use a discounted amount.

4.2 Data Storage—Innovative On-Card Data Storage Capabilities

MCL 3.0 along with M/Chip Advance introduce innovative on-card data storage capabilities allowing issuers and acquirers to operate or participate in data driven card based programs such as transit entitlement, ticketing, card driven loyalty schemes, government entitlement schemes, community cards and many more.

The Data Storage solution is highly flexible, supporting many different data ownership models, imposes no restrictions on data format and enables multiple entities to read, update and write data to the card under policies set by the issuer. Access to all of this data storage functionality can be incorporated within the transaction flow of a payment transaction thus optimizing the process for time critical transactions such as with a contactless transit card. This opens up the possibility of new partnerships and synergies between card issuers, acquirers, merchants and third-party operators—bringing greater value to the payment process.

Data Storage functionality has been designed to meet many operational and security aspects necessary for the secure storage of data on a payment card or device implementing M/Chip Advance.

MCL 3.0 together with M/Chip Advance support two different data storage mechanisms, each offering different levels of security, transaction performance, and flexibility.

1. The Standalone Data Storage (SDS) mechanism is targeting implementations with a single operator.

2. The Integrated Data Storage (IDS) mechanism is the more advanced and innovative data storage solution. This mechanism is tightly integrated with the payment for both speed and reliability and can be used by multiple operators.

4.3 Standalone Data Storage (SDS)

Standalone Data Storage (SDS) provides for the simple storage of data in up to 10 different data stores on a card. These data stores are accessed using standard card commands during a transaction. Some of these data stores are freely writeable; some have write access control.
During an EMV transaction, the reader may read or write data to or from any of the 10 data stores. The card and issuer play no part in the format or structure of the data; it is treated merely as a sequence of binary characters up to a maximum length defined by the issuer at personalization. In a transport application, for example, the data might contain entitlement information or transitory journey data (for example recording when a cardholder got on or off a bus).

4.4 Integrated Data Storage (IDS)

Integrated Data Storage (IDS) is designed to integrate data storage into a payment transaction as well as providing additional features. Data on a card is organized into data stores called “slots,” each slot being identified by an operator ID. An operator can either be the issuer or a delegated third party. The Data Storage functionality allows for a high degree of flexibility with respect to aspects such as; data slot allocation, format of data, size of data, and read and write controls.

The card is personalized to support a limited number of slots. The slots supported by the card are of two types: permanent slots are not subject to re-allocation; volatile slots as their name implies may be over-written by any operator and at any time. This overwrite may either be because new data is given by the same operator, or it may also be because the card has “run out” of free slots and the slot is re-allocated to the new operator.

Reading and writing of data can be integral to a contactless payment transaction, which enables access to the data storage services with a single card interaction offering speed and convenience, critical for certain applications such as contactless transit and retail loyalty.

A typical use of permanent data storage slots would involve the assignment of a slot for the storage of transit entitlement data, such as a season ticket. Less critical short term data, such as details of an individual journey, may be stored in a volatile slot.

The IDS functionality also incorporates many security features, including:

» Anti-skimming to prevent data from one card being used on another card
» Prevention of replaying previously used data from the same card
» Control over writing of data to a card
» Ability to have multiple operators’ data stored on a card with separate access controls
» Issuer delegation of slots to operators

The flexibility of the IDS functionality means that it opens up many business applications enabling the combination of payment card functionality together with cardholder orientated services from issuers and third-party organizations.

Examples of business applications include the following:

» Payment cards used for transit payment and entitlement to travel
» Payment cards with on-card loyalty
» Payment cards with third-party co-brand entitlement (e.g., Government benefits, Campus cards, Social cards, Community cards, etc.)
» Payment cards used with open schemes not requiring agreement with the issuer (e.g., loyalty, short term ticket storage, proof of purchase, etc.)
» Electronic receipts for contactless transactions delivered to mobile devices
» Data delivered to Display Cards used for contactless transactions
5. Enhanced Payment Features

MCL 3.0 provides merchants and acquirers with enhancements that strengthen contactless payments and offer added value to their acceptance infrastructure.

5.1 Torn Transaction Recovery

To minimize issues in the event of a torn transaction (i.e., where a contactless card was removed too soon from the reader resulting in the card and reader having a different outcome), the chip card application must be designed with due consideration for persistent data (accumulators, counters, transaction log records, etc.) such that any updates are made appropriately.

M/Chip Advance ensures that persistent data are updated in one single atomic transaction, just before sending the response to the reader. Optimization of the transaction flow and atomicity effectively creates a smaller window when a torn transaction can occur and helps to ensure that counters and accumulators are synchronized between the card and the issuer host. However, problems can still arise if the card sends the response (and the card has updated its balance accordingly) but the response is not received by the reader. The reader will then decline the transaction but the balance would already have been updated on the card. To address this potential risk a mechanism has been specified to recover from such a torn transaction.

MCL 3.0 supports a new command, Recover AC, that is designed to help M/Chip Advance cards to recover the last Generate AC response from a specific location in persistent memory in the event of a torn transaction.

The MCL 3.0 reader maintains, in a torn transaction log, the transaction data for which it sent a Generate AC but did not receive a response. At the next transaction which the reader has identified as involving the same card for which it has the required data in its torn transaction log, the terminal will initiate a recovery of last transaction signature and will complete the transaction without initiating a duplicate transaction.

This mechanism is useful for both the cardholder and the merchant as it allows transaction disputes to be avoided and/or resolved quickly.
5.2 Balance Reading and Display

The concept of a balance on a card is increasingly important for cards used for offline transactions, especially prepaid cards.

MCL 3.0 offers to M/Chip Advance issuers improved mechanisms for updating the offline balance of a prepaid card or mobile device resulting in increased accuracy of the recorded balance.

A balance on a card refers to an offline amount or number of offline transactions that can be conducted.

MCL 3.0 supports a specific mechanism that enables accurate and reliable balance management for preauthorized or prepaid products, i.e., the balance on the card being the same as the on-card balance held on the account.

The card offline balance can be made available to the cardholder either on a receipt or on a display.

5.3 Zero-Amount Transaction on Online-Only Reader

MCL 3.0 clarifies the definition of an online-only reader.

This information is now included in a specific data object (Terminal Type) while previous versions required a specific configuration of the floor limit to achieve this, with the limitation that it was not valid for zero-amount transactions.

The business benefit for merchants and acquirers is that an online-only terminal is truly online-only, and not just for non-zero amount transactions.

5.4 Offline Card Authentication Without Payment Transaction

MCL 3.0 includes a feature that enables the use of an M/Chip Advance card for authentication purposes without increasing the offline counters.

The benefit for specific markets (e.g., transit, tollways) is the ability to authenticate the card offline without performing a payment transaction. This allows payment and access control functionalities to be combined in a single card.

---

3 This feature is available as of version 3.0.3 of the MCL specification.
5.5 Transaction Amount Management

MCL 3.0 provides acquirers with new options that facilitate the configuration of contactless readers.

Harmonization of Transaction Limits with product rules

While MasterCard product rules define a limit as the upper value of an allowed range, PayPass Reader v2.0 defines a limit as the lower value of the upper range that is not allowed.

Considering for example the CVM Required Limit, this means that when the rules define the CVM Limit at €25, the CVM Required Limit has to be defined at €25.01 for PayPass Reader v2.0.

MasterCard Contactless Reader v3.0 clarifies this definition by aligning the limits definition with the product rules.

Receipt indication

MCL 3.0 supports a mechanism that indicates to the POS the need for a receipt.

CVM Selection Mechanism for mag-stripe mode transactions

The CVM Selection mechanism that is used for a mag-stripe mode transaction is inherited from the legacy magnetic stripe world rather than from the EMV approach. The POS can choose the CVM according to its own existing process which may involve, for example, the service code read from the card. In such case, it would simply disregard the CVM selected by the contactless reader.

MCL 3.0 introduces options allowing the reader to support specific CVM capabilities for mag-stripe mode transactions or to invite the POS to select its preferred CVM.

This mechanism simplifies CVM management for a mag-stripe mode transaction.

5.6 Enabling the Use of the POS Certificate Revocation List

The Certification Revocation List (CRL) is a list of Issuer Public Key Certificates that payment systems have revoked for each Registered Application Provider Identifier (RID) supported by the contactless reader. As for the list of Certification Authority public keys, entries in the Certification Revocation List may be shared between different kernels as long as the applications using it support the same RID.

MCL 3.0 supports the management of a Certificate Revocation List that can be checked by the contactless reader during the transaction.

This new feature enables acquirers to share the CRL that is used for contact readers with their MCL 3.0 contactless readers.
6. Contact

For more information about MCL 3.0, please contact your MasterCard customer representative.
7. Appendix 1. MasterCard Contactless Reader v3.0 and EMV Book C-2

In 2010 the payment scheme members of EMVCo started to design a common contactless specification in order to replicate the contact EMV story and facilitate the adoption of contactless technology.

They developed a contactless terminal architecture described in four books where all payment schemes proprietary contactless kernels are shared with all terminal vendors. Book A defines the architecture and the general requirements, Book D defines a common contactless communication protocol specification and Book B defines the Entry Point, which is a common Application Selection Mechanism (ASM) capable of selecting one of the proprietary kernels depending on the cardholder device presented to the contactless reader. Besides Books A, B and D that are common to all payment schemes, there are multiple Books C, each one defining a different kernel. The kernel described in the MCL 3.0 specification is defined as EMV Book C-2.

![Figure: EMV C-2 vs. MCL 3.0 implementation](image)

Terminal vendors may decide to follow the EMVCo or the MasterCard implementation, the only difference being respectively the use of the Entry Point defined in Book B or of the MasterCard proprietary Application Selection Mechanism (ASM) defined in the MCL 3.0 specification.

Implementations using the MasterCard proprietary ASM must go through the MasterCard approval process, while implementations using the Entry Point can either go through the MasterCard or the EMVCo approval process, since MasterCard's ASM can be considered as a subset of the Entry Point.

Both EMVCo and MasterCard approval processes result in Letters of Approval that are valid for acquirer deployments using MasterCard brands.
MasterCard Worldwide is at the heart of commerce. Our understanding of how and why commerce is conducted allows us to create more advanced methods of payment that fuel economic connections and drive real business value.

©2014 MasterCard. Proprietary and Confidential. All rights reserved.

For more information, contact your MasterCard customer representative.