M/Chip Functional Architecture for Debit and Credit

Christian Delporte, Vice President, Chip Centre of Excellence, New Products Engineering

Suggested routing: Authorization, Chargeback, Chip Technology, Clearing, Mail List, Principal, Programming, Risk Management, Security, and Settlement Contacts

Applies to: ☑ Issuers ☑ Acquirers

Summary: Effective January 2005, MasterCard will update the *M/Chip Functional Architecture for Debit and Credit* document. To help members to prepare their systems, this article lists significant changes that the document will include.

Action Indicator: **I** Informational only (no action required)

Effective Date: MasterCard will publish an updated version of the *M/Chip Functional Architecture* in January 2005.

Effective January 2005, MasterCard will introduce new features. To help members to prepare their systems, this article lists significant changes that the document will include.

Effective Date	Change
Immediately	MasterCard has made changes to type approval testing to correct interoperability issues. The new tests already apply to new implementations. The new version of the *M/Chip Functional Architecture for Debit and Credit* document will contain details about the changes.
1 January 2005	The new version of the *M/Chip Functional Architecture for Debit and Credit* document will be available. Type approval test tools will be available to test all of the new options in the document.
1 July 2005	MasterCard will conduct all new type approvals against the new functional architecture only. New terminals and cards must support all the new requirements as of this date.

Background

The *M/Chip Functional Architecture for Debit and Credit* manual is the main document explaining how members should implement credit and debit programs using EMV[1] smart cards. As part of the normal development cycle, MasterCard provides updated versions that contain corrections, clarifications, and additions to the previous versions.

Effect on members

The changes described in this article are divided into four categories, depending on their impact on members.

1) *Changes to existing requirements*—Changes that are a result of either:

- a) A policy change, or
- b) A clarification made because members have not correctly implemented the requirements in the past. Members that have implemented the requirements correctly will not be affected.

In some cases, MasterCard has already tested the new requirements in type approval. Therefore, MasterCard has already tested new implementations to conform to these requirements.

2) *New options*—Changes and additions made to implement completely new features. These options will be available in Type Approval testing beginning in January 2005.

3) *New requirements*—Additional features that members must implement. These requirements are mandatory and will be tested in type approval from July 2005.

4) *Clarifications and recommendations*—Expanded definitions where there have been misinterpretations or questions in the past. Clarifications require no action. There will be no impact on members that have already implemented the requirements correctly.

Member benefit

The purpose of the new version of the document is to make MasterCard requirements clearer and easier to implement. The benefits to members are:

- Clearer explanations and better guidelines so that implementation will be easier and less expensive
- Better definitions, leading to fewer interoperability problems
- Documentation support

[1] In 1996, Europay (now MasterCard Europe sprl), MasterCard, and Visa (EMV) developed standards for integrated circuit cards (ICCs), terminals, and applications. EMVCo, LLC, established in 1999, is the organization that oversees and maintains the EMV specifications.

Summary of changes

The following sections summarize the changes that MasterCard will make to the *M/Chip Functional Architecture for Debit and Credit* document.

The use of a single quote (') before a number indicates that the number is in hexadecimal format.

1a) Changes with immediate effect due to policy changes

Following are changes to existing rules that may have an impact on existing cards and terminals. Members should check the following points carefully to determine the impact on their operations.

New CVM condition codes from EMV

EMVCo has defined new Card Verification Method (CVM) condition codes to replace the existing "if cash or cashback" codes. The announcement is in *EMVCo Bulletin 16*.

The new CVM codes are:

- '01'—Unattended cash
- '02'—Not unattended cash, and not manual cash, and not purchase with cash back
- '04'—Manual cash
- '05'—Purchase with cash back

The intention is that, in the future, issuers will be able to use these codes to implement different card behavior for ATM withdrawals compared to other kinds of cash transactions.

The new version of the functional architecture will incorporate the new EMV codes and explain their impact on cards and terminals. Existing terminals will continue to work correctly with cards that use the new codes.

New Maestro CVM policy

In February 2004, the Debit Advisory Board decided that hybrid Maestro® cards must support both offline and online personal identification numbers (PINs).

1b) Changes with immediate effect due to requirements clarification

The following clarifications are effective immediately.

Use of the fallback indicator

Some acquirers using magnetic stripe-only technology have misunderstood the use of the fallback indicator. The new version of the document will clarify the Standard that only chip-approved acquirers may use the fallback indicator. Acquirers that do not accept MasterCard® chip cards internationally must not use the fallback indicator.

For more information about the fallback indicator, refer to *Europe Edition Operations Bulletin* No. 6, June 2003.

Implications of an empty Candidate List

A "Candidate List" is the list of possible applications which can be used to make a payment. It is a list of the applications that are present on both the card and the terminal.

The updated document will clarify that MasterCard considers an empty Candidate List (i.e. a situation where there is no common application supported by both the chip and the terminal) a failure of chip technology, and fallback to magnetic stripe is applicable.

The MasterCard Terminal Integration Process already ensures that terminals comply with this requirement.

Printing transaction information

In the January 2003 version of the functional architecture, to help resolve any future acceptance problems, MasterCard required new terminals to support printing or to display the details of the terminal application's parameters, and the details of the last transaction performed.

MasterCard will begin enforcing this requirement immediately.

The displayed data must include:

- Application Identifier (AID) or the file name of the application used
- Card primary account number (PAN)
- Card PAN sequence number
- Integrated Circuit Card (ICC) System-Related Data (Data Element [DE] 55) produced by the transaction
- Terminal and issuer action codes (TACs and IACs)

Inconsistency of Track 2 data

MasterCard has clarified the Standards concerning Track 2 data and Track 2 Equivalent data.

A MasterCard EMV application must contain a data element (tag '57) called Track 2 Equivalent data. This data element should contain the same PAN and application expiry date as that present in the chip data Application PAN (tag '5A) and the Application Expiration Date (tag '5724). If the values of these data elements are not the same, the terminal must terminate the chip transaction. The terminal may process the transaction as a fallback to magnetic stripe.

This Standard protects acquirers from possible liability if they use the wrong PAN to clear the transaction or to check the Warning Bulletin.

The Terminal Integration Process ensures that terminals comply with this requirement.

Fallback on CATs

Cardholder-activated terminals (CATs) with separate readers now will accept the first technology that the cardholder tries to use, and will not prompt to use chip if the technology is magnetic stripe. It is too confusing to prompt the cardholder to continue their transaction using the magnetic stripe if the chip does not work, especially if the cardholder is not familiar with the language of the terminal.

DE 23 in authorization and clearing messages

MasterCard clarified requirements for including Card Sequence Number (DE 23). If Point of Service Data Code (DE 22) has the value '05x and the Application PAN Sequence Number (tag '5F34) is present on the chip, then DE 23 must be present and contain the Application PAN Sequence Number in both the authorization and clearing messages.

A migration period will help satisfy this long term requirement. During the migration period, DE 23 may be forbidden on some networks, if DE 55 is not present.

The MasterCard Card Type Approval process already checks that the Application PAN Sequence Number (tag '5F34) is present on the chip.

Default value of authorization response code

The default value of the authorization response code is value 58 if a terminal does not receive the exact value of the issuer response code for online-declined transactions.

The Terminal Integration Process ensures that terminals comply with this requirement.

Settings for Stand-In

Issuers using Stand-In services for their smart cards should be aware of certain limitations of these services that may increase authorization risk. MasterCard will provide more detailed guidance for issuers using Stand-In services, and new recommendations for the setting of the Issuer Action Codes (IACs).

The Card Type Approval ensures that cards comply with this requirement.

AID support at ATMs

The *Cirrus Worldwide Operating Rules* define the ATM rules for cards bearing the Cirrus®, MasterCard®, and Maestro® logos. Most ATMs accept all three brands. ATM vendors that want to complete Type Approval only once must undergo chip certification while supporting all the chip AIDs corresponding to the card products that are accepted on their ATMs.

Hybrid terminal definition

MasterCard will clarify in the updated document the definition of hybrid terminals to express the fact that they must be type-approved to accept MasterCard smart cards. If the hybrid terminals are not type-approved, MasterCard considers the terminals to be magnetic stripe-only.

2) New options

Following are new options in the functional architecture.

CVC1

Issuers should use a different value of the CVC 1 on the chip and on the magnetic stripe. Issuers may determine the method of calculating the chip CVC 1.

Technology selection and fallback

Following are revisions and clarifications about technology selection and fallback:

- Acquirers may now apply for a waiver to support fallback on online-capable CATs in the Europe region.
- Fallback requirements for manual cash advance terminals are the same as for point-of-sale (POS) terminals.
- Fallback is now possible for offline-only terminals, using voice authorization.
- A terminal that detects a chip technology failure after having requested a decline (by asking the card for an Application Authentication Cryptogram [AAC]) may decline the transaction without fallback.
- A terminal that detects a chip technology failure after the card replied with a request for online authorization (by responding with an Authorization ReQuest Cryptogram [ARQC]) may terminate the smart card transaction without falling back to magnetic stripe.

Definitions of CAT levels

Members often program CATs to behave differently depending on circumstances. For example, an unattended petrol pump may act as a CAT Level 1 terminal if a cardholder inserts a Maestro card (which has a zero floor limit and online PIN as the CVM). However, the same petrol pump may act as a CAT Level 2 terminal (with a zero floor limit, limited amount, and no CVM) when a cardholder uses a MasterCard card.

Similarly, online capable CATs with "No CVM" may act as a CAT 2 terminal if the transaction is sent for online approval, or as a CAT 3 terminal if the transaction is approved offline.

A number of existing terminals are a mix of CAT 1, CAT 2, or CAT 3. This does not pose any problem as long as the authorization and clearing messages carry the appropriate CAT level identification.

In the new version of the document, the terms for CAT levels will refer to ***transactions***, not to the ***terminals*** that process the transactions. This revision simplifies the definition of terminals, which may be online or offline, and may or may not support PINs.

The following table explains the definitions of CAT transactions.

CVM	Online Authorization	Offline Approval
PIN	CAT Level 1	CAT Level 1
Other than PIN	CAT Level 2	CAT Level 3

Terminal Risk Management

MasterCard does not require online-only terminals to support terminal risk management.

RSA[2] key requirements

Key index 03 is now due to expire in 2009 (not in 2008).

MasterCard has accepted the new EMV recommendations for keys with indices of:

- 05 (length 1,408 bits, expiry 2014)
- 06 (length 1,984 bits, expiry 2016)

All new and existing keys use exponent 3.

CAM requirements

Full grade, online-capable CAT terminals do not need to support an offline Card Authentication Method (CAM).

Hybrid cards may support Dynamic Data Authentication (DDA) only.

CVM policy

MasterCard will revise the section detailing allowable CVMs to reflect the revised Standards. These changes include the following:

- MasterCard allows online PIN instead of signature for MasterCard card transactions at a POS.

[2] Rivest, Shamir, and Adleman

- Maestro now accepts hybrid terminals that use offline PIN only.
- For transactions using a signature as the CVM, MasterCard allows either "Apply next CVM" ('1E03) or "Fail CVM processing" ('5E03).

MasterCard Electronic

M/Chip Functional Architecture for Debit and Credit will define the Standards for using chip technology to support MasterCard Electronic™ cards.

The MasterCard AID identifies MasterCard Electronic chip transactions. The AID eases the migration from MasterCard card acceptance to MasterCard Electronic acceptance. Once a merchant has signed up for MasterCard Electronic, it may acquire MasterCard Electronic transactions without changing its chip terminal.

The issuer must program their MasterCard Electronic chip applications to be online only. A cardholder cannot use a MasterCard Electronic card without a CVM on a CAT terminal.

Issuers will indicate in the card settings whether they allow the use of MasterCard Electronic cards at ATMs.

Quasi-cash disbursements

The functional architecture will define the chip impact on "quasi-cash" transactions. These transactions involve instruments that are convertible to cash directly, but are not legal tender in the country where they are issued. Examples include traveler's cheques, foreign currency, money orders, and gambling chips.

Payment of gratuities

Currently, when cardholders use MasterCard payment cards, it is normal for the cardholder be able to add a gratuity or tip to the total amount of the card transaction. The functional architecture will explain the Standards and guidelines for these types of payments, particularly when a PIN is used as CVM.

Chip support for QPS

The Quick Payment Service (QPS) is a program for merchants in the United States that need very fast checkouts, whereby acquirers may approve transactions without a signed receipt or an online authorization.

In practice, the terminal is set up with a QPS floor limit, which may be different from the normal terminal floor limit. Acquirers may approve transactions below the QPS floor limit with no CVM and without online authorization. Acquirers can obtain this approval by varying the terminal capabilities, so that below the QPS floor limit the terminal will support either "No CVM" or "No CVM and offline PIN".

The document is available electronically in the Member Publications product on MasterCard OnLine.

Smart card use does not affect chargeback rights or other Standards for QPS. For full details, refer to the *Quick Payment Service Program Guide*.

Issuer country code as part of the signed static application data

When cards have a domestic and an international application on the chip, MasterCard recommends that members include the issuer country code as part of the signed static application data (SSAD), ensuring that its value cannot be changed. This helps prevent possible fraud opportunities.

Balance inquiry on ATM

MasterCard has clarified the requirements for ATMs supporting balance inquiry transactions for smart cards. The functional architecture will provide guidance on how to implement the function.

3) New requirement

Following is a new requirement in the functional architecture.

Processing domestic transactions

Processing foreign cards with a service code of '6XX (domestic use) is the same as for cards with a service code of '2XX.

4) Clarifications and recommendations

Following are clarifications about existing options and recommended best practices.

Applying brand-specific fallback rules

The fallback decision should occur at the acquirer host. If the chip technology fails, the terminal will send the transaction data and the magnetic stripe track-2 data to the acquirer host system. The acquirer will then use the acquirer BIN tables to identify the card brand. The host system then may decide if the transaction continues in fallback mode, or if the transaction is declined because fallback is not allowed in the specific program rules.

This process will allow acquirers the flexibility to adapt to new fallback requirements that MasterCard may introduce in the future.

Cash disbursements

MasterCard has clarified the rules relating to cash withdrawals as they relate to chip cards.

Fallback Rules for Domestic Cards

The *M/Chip Functional Architecture for Debit and Credit* document will state that acquirers that process domestic transactions as international transactions must follow the same fallback requirements for their domestic cards (service code = '6XX) as for international cards (service code = '2XX).

Emergency card replacement

MasterCard has clarified that the Emergency Card Replacement service will only deliver a replacement magnetic stripe card, even if the original card was issued with a chip.

Pre-authorizations, referrals, refunds, and voice authorization

The functional architecture now provides more guidance to acquirers as to how they should implement these functions in the chip environment.

Amount Other field

Members use the Amount Other field when there is a disbursement as part of a purchase transaction. MasterCard has:

- Clarified the Standards governing cash disbursement transactions
- Explained how members can use the Amount Other field to support this function

Script terminology

The current use of the terms "critical" and "non-critical" scripts is not consistent with EMV use. Therefore, MasterCard replaced the term "critical scripts" with "scripts template 1," and the term "non-critical scripts" with "scripts template 2."

Use of DE 22 in clearing messages

MasterCard will explain the meaning and use of the different subfields in DE 22 in the functional architecture.

Chip to magnetic stripe conversion service

As a service to issuers during their migration, MasterCard has developed a service that converts chip authorization requests to magnetic stripe requests. This service allows issuers to begin issuing smart cards without upgrading their authorization systems.

Data in clearing records

With the revised document, Integrated Product Messages (IPM) clearing records may contain Issuer Authentication Data (Private Data Subelement [PDS] 91) within DE 55.

M/Chip documentation

The *M/Chip Functional Architecture for Debit and Credit* manual will explain more clearly the structure and contents of the documents supporting the range of M/Chip™ products:

- M/Chip Lite 2.1
- M/Chip Select 2.0
- M/Chip 4 Lite
- M/Chip 4 Select

CDA support

MasterCard expanded the possible responses to the "Generate AC" command to include the responses generated while performing a Combined Dynamic Data Authentication-Application Cryptogram Generation (CDA) transaction.

Variable CVM capabilities

MasterCard allows terminal and additional terminal capabilities to vary according to the card application that the cardholder uses for a payment. This means that terminals may support CVM capabilities that MasterCard does not allow (e.g. domestic debit product support), but the terminal must not provide these options when processing a MasterCard card.

CVM substitution

MasterCard will clarify the *M/Chip Functional Architecture for Debit and Credit* manual to explain when MasterCard allows CVM substitution (e.g. the use of a signature when the card PIN did not work).

Application PAN and application expiry date

MasterCard clarified that the PAN and the expiry date, which are printed on the ticket, used in Primary Account Number (DE 2) and Date, Expiration (DE 14) in the authorization and clearing messages, must be the Application PAN (tag '5A) and the Application Expiration Date (tag '5724).

Online only cards

MasterCard has clarified the card settings that must be used to ensure that a card always goes online for authorizations.

Acquirer authorization below international floor limit

MasterCard has clarified the requirements for acquirers that authorize below floor limit transactions offline.

For more information

For additional details about the *M/Chip Functional Architecture for Debit and Credit* document or its impact on members, please contact:

Chip Help Desk

E-mail: chip_help@mastercard.com