Return to Menu

MasterCard International



Information about this Replacement

Replacement

The December 2004 *M/Chip 4 Issuer Guide to Debit and Credit Parameter Management* replaces your existing manual.

What is in the new version?

This manual describes how to use the main features of the M/Chip Select 4 and the M/Chip Lite 4 applications.

Please refer to:

- "Summary of Changes" for a comprehensive list of changes reflected in this update.
- "Using this Manual" for a complete list of the contents of this manual.

Questions?

If you have questions about this manual, please contact the Customer Operations Services team or your regional help desk. Please refer to "Using this Manual" for more contact information.

MasterCard is Listening…

Please take a moment to provide us with your feedback about the material and usefulness of the *M/Chip 4 Issuer Guide to Debit and Credit Parameter Management* using the following e-mail address:

publications@mastercard.com

We continually strive to improve our publications. Your input will help us accomplish our goal of providing you with the information you need.

MasterCard International



Summary of Changes

***M/Chip 4 Issuer Guide to Debit and Credit Parameter Management*, December 2004**

Change Summary	Description of Change	Where to Look
Addition of MasterCard Electronic brand supported	The M/Chip Select 4 and M/Chip Lite 4 applications now offer certain issuer-specific features to enhance the MasterCard Electronic brand.	Chapter 6

OV Loop Inc.
Ex. 2021 - Page 2

MasterCard International



M/Chip 4 Issuer Guide to Debit and Credit Parameter Management

December 2004

Copyright

The information contained in this manual is proprietary and confidential to MasterCard International Incorporated (MasterCard) and its members.

This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of MasterCard.

To the extent permitted by law, neither MasterCard nor any of its affiliates, employees or officers shall be liable to any recipient of this manual, or any other third party, for any loss, damages (including direct, special, punitive, exemplary, incidental or consequential damages) or costs (including attorneys' fees) which arise out of, or are related to this manual. The foregoing limitation of liability shall apply to any claim or cause of action under law or equity whatsoever, including contract, warranty, strict liability, or negligence, even if MasterCard has been notified of the possibility of such damages or claim.

Trademarks

Trademark notices and symbols used in this manual reflect the registration status of MasterCard trademarks in the United States. Please consult with the Customer Operations Services team or the MasterCard Law Department for the registration status of particular product, program, or service names outside the United States.

All third-party product and service names are trademarks or registered trademarks of their respective owners.

Media

This document is available:

- On MasterCard OnLine®
- On the *MasterCard Electronic Library* (CD-ROM)

MasterCard International Incorporated
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

1-636-722-6100

www.mastercard.com

Using this Manual

Purpose 1

Audience 1

Overview 2

Excerpted Text 3

Language Use 3

Times Expressed 4

Revisions 4

Related Information 5

Support 6
- Member Relations Representative 7
- Regional Representative 7

Abbreviations 8
- Notational Conventions 10

Chapter 1 Introduction

1.1 Overview of M/Chip Select 4 and M/Chip Lite 4 1-1
- 1.1.1 Uniform Behavior across Multiple Implementations 1-1
- 1.1.2 M/Chip Select 4—the High Security Application 1-2
- 1.1.3 M/Chip Lite 4—the Light Version of M/Chip Select 4 1-2
- 1.1.4 Simple Yet Powerful Card Risk Management 1-2
- 1.1.5 How You Control Offline Risk 1-4
- 1.1.6 Migration Facilities 1-7
- 1.1.7 Offline PIN Management Facilities 1-7
- 1.1.8 Acceptance on CAT Level 3 Terminals 1-8
- 1.1.9 Post-issuance Updates and Maintenance 1-9
- 1.1.10 Transaction Log 1-9
- 1.1.11 Specific Behavior for Domestic or International Transactions 1-9
- 1.1.12 Additional Functionality 1-9

1.2 M/Chip Select 4, M/Chip Lite 4 and EMV 2000 1-10

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 5

1.2.1 EMV 2000 Session Key Derivation 1-10
1.2.2 Combined DDA/AC Generation 1-10

Chapter 2 Card Risk Management

2.1 Introduction 2-1
2.1.1 Offline Card Risk Management 2-1
2.1.2 Online Card Risk Management 2-2

2.2 Card Verification Results 2-2

2.3 Card Issuer Action Codes 2-6
2.3.1 Content of the Card Issuer Action Codes 2-7
2.3.2 Card Issuer Action Code—Decline 2-10
2.3.3 Card Issuer Action Code—Online 2-11
2.3.4 Card Issuer Action Code—Offline 2-11

2.4 Offline Counters and Offline Limits 2-12
2.4.1 Offline Counters 2-12
2.4.2 Offline Limits 2-13
2.4.3 Comparison between Offline Counters and Offline Limits 2-14

2.5 Card Risk Management Algorithm 2-16
2.5.1 First Occurrence of GENERATE AC 2-16
2.5.2 Second Occurrence of GENERATE AC 2-21

Chapter 3 Configuring the M/Chip 4 Application

3.1 Overview 3-1

3.2 Configuring the Application Control Data Element 3-1
3.2.1 Application Control Coding 3-1
3.2.2 Application Control Usage 3-4

3.3 Configuring Card Risk Management Data Elements 3-8
3.3.1 Card Issuer Action Codes 3-8
3.3.2 CRM Country Code 3-8
3.3.3 CRM Currency Code 3-9
3.3.4 Lower Cumulative Offline Transaction Amount 3-9
3.3.5 Upper Cumulative Offline Transaction Amount 3-9

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 6

3.3.6 Lower Consecutive Offline Limit 3-10
3.3.7 Upper Consecutive Offline Limit 3-10
3.3.8 Currency Conversion Table and Currency Conversion Parameters 3-10
3.3.9 Default ARPC Response Code 3-11
3.3.10 Additional Check Table 3-12
3.3.11 CDOL 1 and CDOL 2 Related Data 3-12
3.3.12 Offline PIN, PIN Try Counter and PIN Try Limit 3-13
3.3.13 Previous Transaction History 3-13
3.3.14 Application Control 3-13

3.4 Selecting Cryptographic Features 3-14
3.4.1 Session Key Derivation 3-14
3.4.2 Key for Offline Encrypted PIN 3-15
3.4.3 Offline Counters Encryption 3-17
3.4.4 Offline Counters inclusion in AC 3-17
3.4.5 Cryptogram Version Number 3-18

Chapter 4 Issuer Host Processing of Transactions

4.1 Online Authorization 4-1
4.1.1 Verifying the ARQC 4-1
4.1.2 Interpreting the Issuer Application Data 4-1
4.1.3 Making The Decision 4-5
4.1.4 Building The Issuer Authentication Data 4-5
4.1.5 Script Processing 4-9
4.1.6 Issuer Referral 4-10

4.2 Clearing 4-11
4.2.1 Check that Transactions Were Approved Online 4-11
4.2.2 Potential De-synchronization between AC and Terminal Verification Results 4-11

4.3 Update of Application Status 4-13
4.3.1 Reset of Script Counter 4-13
4.3.2 Setting of “Go Online on Next Transaction” Bit 4-13
4.3.3 Setting of “Issuer Authentication Failed,” “Script Received”, “Script Failed” Bits 4-14
4.3.4 Update of Offline Counters 4-14

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 7

Chapter 5 Advanced Features

5.1 Synchronization between Online and Offline PIN Try Counters 5-1

5.2 Support of Magstripe Grade Issuer Mode 5-2
5.2.1 Magstripe Grade Issuer Mode Not Activated 5-2
5.2.2 Magstripe Grade Issuer Mode Activated 5-3

5.3 Behavior on CAT Level 3 Terminals 5-6

5.4 Swapping Application File Locator Configurations 5-7
5.4.1 AFL Swap Mechanism 5-7
5.4.2 PIN De-synchronization on New Cards and Offline PIN Post-activation 5-8

5.5 Consulting the Log of Transactions 5-11

5.6 Retrieving the Offline Balance 5-12

5.7 Post-Issuance Maintenance 5-13
5.7.1 PUT DATA to Modify Data Elements 5-13
5.7.2 UPDATE RECORD to Modify Records 5-14
5.7.3 GET DATA to Retrieve Data 5-14
5.7.4 GET PROCESSING OPTIONS to Retrieve Data 5-15
5.7.5 Retrieving Records In The Transaction Log 5-16
5.7.6 Sending Script Commands to the Card 5-16

5.8 Additional Check Table 5-17
5.8.1 How the M/Chip Application Checks the Additional Check Table 5-17
5.8.2 Additional Check Table Content 5-19
5.8.3 Example of Additional Check Table Value 5-21

Chapter 6 Personalizing the M/Chip 4 Application

6.1 Personalization Commands and Values 6-1

6.2 Data Element Personalization Values 6-2
6.2.1 Persistent Data Elements for Application Selection 6-2
6.2.2 Persistent Data Elements Referenced in the AFL 6-2
6.2.3 Persistent Data Elements For Card Risk Management 6-4
6.2.4 Secret Keys—Triple DES Keys 6-5

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 8

6.2.5 Miscellaneous 6-7
6.2.6 Get Processing Options Response 6-7
6.2.7 Counters and Previous Transaction 6-8
6.2.8 PIN Information 6-8
6.2.9 Data Elements With a Fixed Initial Value 6-9
6.2.10 Additional Data Elements 6-10

6.3 Common Profiles 6-10
6.3.1 Profile Assumptions 6-10
6.3.2 Full Grade Profiles 6-16
6.3.3 Magstripe Grade Profiles 6-55

Chapter 7 Migration from M/Chip Lite 2.1

7.1 Overview 7-1

7.2 Authorization Request and Clearing Data Handling 7-1
7.2.1 Application Interchange Profile 7-2
7.2.2 Application Cryptogram 7-2
7.2.3 Cryptogram Information Data 7-4
7.2.4 Issuer Application Data 7-4
7.2.5 Terminal Verification Results 7-7
7.2.6 Unpredictable Number 7-7
7.2.7 Remaining Data Elements 7-7

7.3 Preparing the Authorization Response 7-8
7.3.1 Issuer Authentication Data 7-8
7.3.2 Issuer Script 7-9

7.4 Personalization 7-10
7.4.1 Overview 7-10
7.4.2 Step 1: Build the Personalization Values 7-10

Chapter 8 Migration from M/Chip Select 2

8.1 Overview 8-1

8.2 Authorization Request and Clearing Data Handling 8-1
8.2.1 Application Interchange Profile 8-2
8.2.2 Application Cryptogram 8-2

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 9

8.2.3 Cryptogram Information Data 8-4
8.2.4 Issuer Application Data 8-4
8.2.5 Terminal Verification Results 8-6
8.2.6 Unpredictable Number 8-6
8.2.7 Remaining Data Elements 8-7

8.3 Preparing the Authorization Response 8-7
8.3.1 Issuer Authentication Data 8-7
8.3.2 Issuer Script 8-8

8.4 Personalization 8-9
8.4.1 Overview 8-9
8.4.2 Step 1: Build the Personalization Values 8-9

Chapter 9 Migration from M/Chip Lite 4 to M/Chip Select 4

9.1 Overview 9-1

9.2 Authorization Request and Clearing Data Handling 9-1

9.3 Online Interface 9-1

Appendix A Data Dictionary

A.1 Additional Check Table A-1

A.2 Application Control A-3

A.3 Application Interchange Profile A-6

A.4 Application Life Cycle Data A-7

A.5 Application Transaction Counter Limit A-9

A.6 ARPC Response Code A-10

A.7 Card Issuer Action Code—Decline, Default, Online A-12

A.8 CDOL 1 (Card Risk Management Data Object List 1) A-15

A.9 CDOL 1 Related Data Length A-17

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 10

A.10 CDOL 2 (Card Risk Management Data Object List 2) A-18

A.11 Consecutive Offline Transactions Number A-19

A.12 CRM Country Code A-19

A 13 CRM Currency Code A-20

A.14 Cryptogram Information Data A-20

A.15 Cryptogram Version Number A-21

A.16 Cumulative Offline Transaction Amount A-22

A.17 Currency Conversion Parameters A-23

A.18 Currency Conversion Table A-24

A.19 CVR (Card Verification Results) A-25

A.20 Default ARPC Response Code A-31

A.21 DDOL (Dynamic Data Authentication Data Object List) A-33

A.22 ICC Dynamic Number A-33

A.23 Issuer Action Code – Default, Denial, Online A-34

A.24 Issuer Application Data A-36

A.25 Issuer Authentication Data A-37

A.26 Key Derivation Index A-37

A.27 Lower Consecutive Offline Limit A-38

A.28 Lower Cumulative Offline Transaction Amount A-38

A.29 Log Format A-39

A.30 Offline Balance A-40

A.31 PIN Try Counter A-40

A.32 PIN Try Limit A-41

A.33 Previous Transaction History A-42

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 11

A.34 Script Counter A-43

A.35 Consecutive Offline Limit A-44

A.36 Cumulative Offline Transaction Amount A-44

Appendix B Currency Conversion

B.1 Currency Conversion Process B-1

Appendix C Offline Counters Exception Processing

C.1 Overview C-1

C.2 Cumulated Transactions Limit C-1

C.3 Consecutive Offline Transactions Limit C-1

C.4 How to Prohibit Offline Transactions Based on Transaction Currency ... C-2

Appendix D Interpreting the Card Verification Results

D.1 Interpreting the Card Verification Results D-1

D.1.1 Cryptogram TC in Response to First GENERATE AC D-1

D.1.2 Cryptogram ARQC in Response to First GENERATE AC D-5

D.1.3 Cryptogram TC in Response to Second GENERATE AC D-8

Appendix E Non-critical Script Data Examples

E.1 Examples E-1

E.1.1 Example 1 ..... E-1

E.1.2 Example 2 ..... E-2

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 12

Using this Manual

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

Purpose 1

Audience 1

Overview 2

Excerpted Text 3

Language Use 3

Times Expressed 4

Revisions 4

Related Information 5

Support 6
- Member Relations Representative 7
- Regional Representative 7

Abbreviations 8
- Notational Conventions 10
  - Hexadecimal Notation 10
  - Binary Notation 10
  - Decimal Notation 10
  - Data Element Notation 10

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 13

Purpose

The M/Chip Select 4 and M/Chip Lite 4 applications offer the card issuer a wide range of possibilities for configuring the application and setting the parameters in the card.

The *MasterCard M/Chip 4 Issuer Guide to Debit and Credit Parameter Management* describes how you use the main features of M/Chip Select 4 and M/Chip Lite 4. It also provides you with specific information about how to customize and manage these applications.



Note

This publication is a guide for both the M/Chip Select 4 and the M/Chip Lite 4 applications. However, we describe common application behavior or parameterization with the general term "The M/Chip 4 application…." When behavior is specific to one of the applications, we use the application name, i.e. "The M/Chip Lite 4 application…." or "The M/Chip Select 4 application…." In all cases the references in this publication are to the features and behaviors relevant in an application that fully and correctly implements the M/Chip 4 Car Application Specifications for Debit and Credit.

Dec 2004



Note

M/Chip Select 2 represents all versions of M/Chip Select v2.0.1 to v2.0.5 currently implemented on MULTOS.

Audience

MasterCard provides this manual for members and their authorized agents. Specifically, the following personnel should find this manual useful:

- M/Chip Select 4 and/or M/Chip Lite 4 card issuer staff
- M/Chip Select 4 and/or M/Chip Lite 4 personalization bureau staff
- M/Chip Select 4 and/or M/Chip Lite 4 support staff

Dec 2004

The terms "you" and "your" in the text refer to the card issuer.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 14

The information given in this manual in relation to customization, data elements, parameter management, application or issuer profiles, and any other matters, is given in order to assist in the production and operation of cards by or on behalf of the issuer. Except where any item is indicated as mandatory by MasterCard hereunder it is for the issuer to determine what action it deems appropriate in light of its own circumstances and any suggestion or recommendation in this manual should only be treated as a guide for assistance.

Dec 2004

Overview

The following table provides an overview of this manual:

Chapter	Description
Table of Contents	A list of the manual's tabbed sections and subsections. Each entry references a section and page number.
Using this Manual	A description of the manual's purpose and its contents.
1 Introduction	This chapter introduces the M/Chip Select 4 and the M/Chip Lite 4 applications.
2 Card Risk Management	This chapter describes Card Risk Management for the M/Chip 4 application.
3 Configuring the M/Chip 4 Application	This chapter describes the features of the M/Chip 4 application that you configure to define the application behavior.
4 Issuer Host Processing of Transactions	This chapter describes the processing performed by your host as part of online authorization and clearing. It also describes the conditions when the application status is updated.
5 Advanced Features	This chapter describes advanced features of the M/Chip 4 application.
6 Personalizing the M/Chip 4 Application	This chapter describes the different types of personalization. It then identifies the data elements that require personalization and the different M/Chip 4 application profiles.
7 Migration from M/Chip Lite 2.1	This chapter describes the migration of your authorization and clearing system from M/Chip Lite 2.1 to M/Chip Select 4 or M/Chip Lite 4.
8 Migration from M/Chip Select 2	This chapter describes the migration of your authorization and clearing system from M/Chip Select 2 to M/Chip Select 4.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 15

Chapter		Description
9	Migration from M/Chip Lite 4 to M/Chip Select 4	This chapter describes the migration your authorization and clearing system from M/Chip Lite 4 to M/Chip Select 4.
A	Data Elements Dictionary	This appendix provides a dictionary of data element definitions.
B	Currency Conversion	This appendix describes the currency conversion process used by the M/Chip 4 application.
C	Offline Counters Exception Processing	This appendix introduces how the M/Chip 4 application manages the offline counters.
D	Interpreting the Card Verification Results	This appendix describes how you interpret the Card Verification Results.
E	Non-critical Script Data Examples	This appendix provides examples of non-critical script data.

Excerpted Text

At times, this document may include text excerpted from another document. A note before the repeated text always identifies the source document. In such cases, we included the repeated text solely for the reader's convenience. The original text in the source document always takes legal precedence.

Language Use

The spelling of English words in this manual follows the convention used for U.S. English as defined in *Merriam-Webster's Collegiate Dictionary*. MasterCard is incorporated in the United States and publishes in the United States. Therefore, this publication uses U.S. English spelling and grammar rules.

An exception to the above spelling rule concerns the spelling of proper nouns. In this case, we use the local English spelling.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 16

Times Expressed

MasterCard is a global company with locations in many time zones. The MasterCard operations and business centers are in the United States. The operations center is in St. Louis, Missouri, and the business center is in Purchase, New York.

For operational purposes, MasterCard refers to time frames in this manual as either "St. Louis time" or "New York time." Coordinated Universal Time (UTC) is the basis for measuring time throughout the world. You can use the following table to convert any time used in this manual into the correct time in another zone:

	St. Louis, Missouri USA	Purchase, New York USA	UTC
	Central Time	Eastern Time	
Standard time (last Sunday in October to the first Sunday in April [a])	9:00	10:00	15:00
Daylight saving time (first Sunday in April to last Sunday in October)	9:00	10:00	14:00

[a] For Central European Time, last Sunday in October to last Sunday in March.

Revisions

MasterCard periodically will issue revisions to this document as we implement enhancements and changes, or as corrections are required.

With each revision, we include a "Summary of Changes" describing how the text changed. Revision markers (vertical lines in the right margin) indicate where the text changed. The month and year of the revision appears to the right of each revision marker.

Occasionally, we may publish revisions or additions to this document in a *Global Operations Bulletin* or other bulletin. Revisions announced in another publication, such as a bulletin, are effective as of the date indicated in that publication, regardless of when the changes are published in this manual.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 17

Related Information

The following documents and resources provide information related to the subjects discussed in this manual. Please refer to the *Quick Reference Booklet* for descriptions of these documents.

- *EMV 2000, Version 4.0 December 2000*
- *M/Chip Functional Architecture for Debit and Credit*
- *Modification to Combined Dynamic Data Authentication and Application Cryptogram Generation, EMVCo Bulletin No. 6, December 14 2001*
- *M/Chip Lite Card Profile, Version 2.1 October 2000*
- *M/Chip 4 Security & Key Management*

Members that use the Cirrus® service and logo or that process online debit transactions should refer to the debit processing manuals recommended by the Customer Operations Services team.

For definitions of key terms used in this document, please refer to the *MasterCard Dictionary* on the Member Publications home page (on MasterCard OnLine® and the MasterCard Electronic Library CD-ROM). You also may access the MasterCard Dictionary from the main menu and bookmark pane of most manuals.

To order MasterCard manuals, please use the Ordering Publications service on MasterCard OnLine®, or contact the Customer Operations Services team.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 18

Support

Please address your questions to the Global Member Operations Services Support team as follows:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

Fax: 1-636-722-7192

E-mail: member_support@mastercard.com

Address: MasterCard International Incorporated
Customer Operations Services
2200 MasterCard Boulevard
O'Fallon MO 63368-7263
USA

Telex: 434800 *answerback*: 434800 ITAC UI

Customer Support Services

Phone: +32 2 352 5304

Fax: +32 2 352 5949

E-mail: css@mastercard.com

Address: MasterCard Europe
Chaussée de Tervuren
B-1410 Waterloo
Belgium

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 19

Member Relations Representative

Member Relations representatives assist U.S. members with marketing inquiries. They interpret member requests and requirements, analyze them, and if approved, monitor their progress through the various MasterCard departments. This does not cover support for day-to-day operational problems, which the Customer Operations Services team addresses.

To find out who your U.S. Member Relations representative is, contact your local Member Relations office:

Atlanta	1-678-459-9000
Chicago	1-847-375-4000
Purchase	1-914-249-2000
San Francisco	1-925-866-7700

Regional Representative

The regional representatives work out of the regional offices. Their role is to serve as intermediaries between the members and other departments in MasterCard. Members can inquire and receive responses in their own language and during their office's hours of operation.

To find out the location of the regional office serving your area, call the Customer Operations Services team at:

Phone: 1-800-999-0363 or 1-636-722-6176

1-636-722-6292 (Spanish language support)

For members in the Europe region, please contact your Regional Manager.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 20

Abbreviations

Table 1—Abbreviations

Abbreviation	Description
AAC	Application Authentication Cryptogram
AC	Application Cryptogram
ADF	Application Definition File
AFL	Application File Locator
AID	Application Identifier
AIP	Application Interchange Profile
an	Alphanumeric characters
ans	Alphanumeric and Special characters
APDU	Application Protocol Data Unit
ARPC	Authorization Response Cryptogram
ARQC	Authorization Request Cryptogram
ATC	Application Transaction Counter
b	Binary
BER	Basic Encoding Rules
CDOL	Card Risk Management Data Object List
CIAC	Card Issuer Action Code
CID	Cryptogram Information Data
cn	Compressed Numeric
CRM	Card Risk Management
CVR	Card Verification Results
DDOL	Dynamic Data Authentication Data Object List
DES	Data Encryption Standard
EMV	Europay MasterCard Visa
EPI	Europay International
FCI	File Control Information
IAD	Issuer Application Data
ICC	Integrated Circuit Card

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 21

Abbreviation	Description
LCOL	Lower Consecutive Offline Limit
M	Mandatory
MAC	Message Authentication Code
MCI	MasterCard International
MK_{AC}	AC Master Key
MK_{IDN}	ICC Dynamic Number Master Key
MK_{SMC}	SM for Confidentiality Master Key
MK_{SMI}	SM for Integrity Master Key
n	Numeric Characters
O	Optional
PAN	Primary Account Number
PDOL	Processing Options Data Object List
PIN	Personal Identification Number
PIX	Proprietary Application Identifier Extension
PSE	Payment System Environment
RFU	Reserved for Future Use
RID	Registered Application Provider Identifier
SDL	Specification and Description Language
SFI	Short File Identifier
SHA	Secure Hash Algorithm
SW1 - SW2, SW12	Status bytes 1-2
TC	Transaction Certificate
TLV	Tag Length Value
TVR	Terminal Verification Results
UCOL	Upper Consecutive Offline Limit
var.	Variable

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 22

Notational Conventions

Hexadecimal Notation

Values expressed in Hexadecimal form are enclosed in single quotes (i.e. ‘ ’). For example, 27509 decimal is expressed in hexadecimal as ‘6B75’.

Binary Notation

Values expressed in binary form are followed by a b and enclosed in single quotes (i.e. ‘ b’). For example, ‘08’ hexadecimal is expressed in binary as ‘00001000b’.

Decimal Notation

Values expressed in decimal form are not enclosed in single quotes. For example, ‘08’ hexadecimal is expressed in decimal as 8.

Data Element Notation

Data elements used for this specification are written in a specific font to distinguish them from the text:

This is CS_Italic used for data elements.

To refer to a specific byte of a multi-byte data element, a byte index is used under brackets (i.e. [ ]). For example, *Card Verification Results* [4] represents the 4th byte of the *Card Verification Results*. The first byte of a data element has index 1.

To refer to a specific bit of a multi-bit data element, a bit index is used under brackets[ ]. For example, *PIN Verification Status* [7] represents the 7th bit of the *PIN Verification Status*. The first bit of a data element has index 1.

To refer to a specific bit of a multi-byte data element, a byte index and a bit index are used under brackets (i.e. [ ][ ]). For example, *Card Verification Results* [2][4] represents the 4th bit of byte 2 of the *Card Verification Results*.

Ranges of bytes or bits are expressed with the following equivalent notations:

- *Card Verification Results* [1-5]
- *Card Verification Results* [1 to 5]

Both of these bullets represent bytes 1, 2, 3, 4, and 5 of the *Card Verification Results*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 23

1 Introduction

This chapter introduces the M/Chip Select 4 and M/Chip Lite 4 applications.

1.1 Overview of M/Chip Select 4 and M/Chip Lite 4 1-1
1.1.1 Uniform Behavior across Multiple Implementations 1-1
1.1.2 M/Chip Select 4—the High Security Application 1-2
1.1.3 M/Chip Lite 4—the Light Version of M/Chip Select 4 1-2
1.1.4 Simple Yet Powerful Card Risk Management 1-2
1.1.5 How You Control Offline Risk 1-4
1.1.6 Migration Facilities 1-7
1.1.7 Offline PIN Management Facilities 1-7
1.1.7.1 Update of Offline PIN Try Counter 1-8
1.1.7.2 Personalization as 'No Offline Signature Application" 1-8
1.1.7.3 Protections against Wedge Device Attacks 1-8
1.1.8 Acceptance on CAT Level 3 Terminals 1-8
1.1.9 Post-issuance Updates and Maintenance 1-9
1.1.10 Transaction Log 1-9
1.1.11 Specific Behavior for Domestic or International Transactions 1-9
1.1.12 Additional Functionality 1-9

1.2 M/Chip Select 4, M/Chip Lite 4 and EMV 2000 1-10
1.2.1 EMV 2000 Session Key Derivation 1-10
1.2.2 Combined DDA/AC Generation 1-10

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 24

1.1 Overview of M/Chip Select 4 and M/Chip Lite 4

The M/Chip Select 4 and M/Chip Lite 4 applications are EMV 2000-compliant applications, designed primarily to carry the MasterCard, Maestro, or Cirrus brands. These applications offer certain issuer-specific features, to enhance the MasterCard, MasterCard Electronic, Maestro, or Cirrus brands. Dec 2004

Refer to the *M/Chip 4 Card Application Specifications for Debit and Credit* for a definition of the M/Chip 4 applications.

1.1.1 Uniform Behavior across Multiple Implementations

The *M/Chip 4 Card Application Specifications for Debit and Credit* aims to provide an unambiguous definition of the behavior of the M/Chip 4 applications. Therefore, once personalized:

- All implementations compliant with the M/Chip Select 4 specifications should behave in exactly the same way with regard to the matters set out in the specifications. Dec 2004
- All implementations compliant with the M/Chip Lite 4 specifications should behave in exactly the same way with regard to the matters set out in the specifications.

These specifications cover the complete card to terminal interface used for offline and online EMV transactions, describing the behavior defining:

- The card interface
- At the application layer (C/R-APDUs)
- The behavior of the application in relation to the personalization values Dec 2004

This approach offers the following benefits for Type Approval services and for your selection of an implementation provider:

- The test case definition is independent of the actual implementation. Implementations are validated against the M/Chip 4 applications "standard" test cases.
- All implementations compliant with these specifications should behave in the same way with regard to the matters set out in the specifications. You should therefore be able to manage several implementations of the same application, originating from different card application developers, without seeing any difference between them in such regard. You may therefore develop a single host system, to process all cards irrespective of their origin. Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 25

1.1.2 M/Chip Select 4—the High Security Application

Dec 2004

The M/Chip Select 4 application offers the following features to support a high level of security for debit or credit transactions:

- For cardholder security, the M/Chip Select 4 application supports the offline encrypted PIN verification.
- For issuer security, the M/Chip Select 4 application supports the EMV 2000 session key derivation.
- For both acquirer and issuer security, the M/Chip Select 4 application supports DDA and Combined DDA/AC generation.

1.1.3 M/Chip Lite 4—the Light Version of M/Chip Select 4

The M/Chip Lite 4 application is essentially the M/Chip Select 4 application, without the features requiring RSA computational power. The M/Chip Lite 4 application can therefore be implemented on DES-only cards.

RSA computations are only used for offline messages (e.g. the offline CAM). The differences between the M/Chip Select 4 and the M/Chip Lite 4 are therefore almost entirely limited to the interface between the card and the terminal. The M/Chip Lite 4 application is the equivalent of the M/Chip Select 4 application, without the support of:

- DDA
- Combined DDA/AC generation
- Offline encrypted PIN verification

The following features are almost identical for the M/Chip Select 4 and M/Chip Lite 4 applications:

- Card Risk Management
- Interface for online messages

1.1.4 Simple Yet Powerful Card Risk Management

The definition of Card Risk Management for the M/Chip 4 applications has received special attention. The mechanism used has similarities with EMV-defined Terminal Risk Management, as follows:

- The *Card Verification Results* play the role of the *Terminal Verification Results*
- The *Card Issuer Action Codes* play the role of the *Issuer Action Codes* and *Terminal Action Codes*.

© 2004 MasterCard International Incorporated

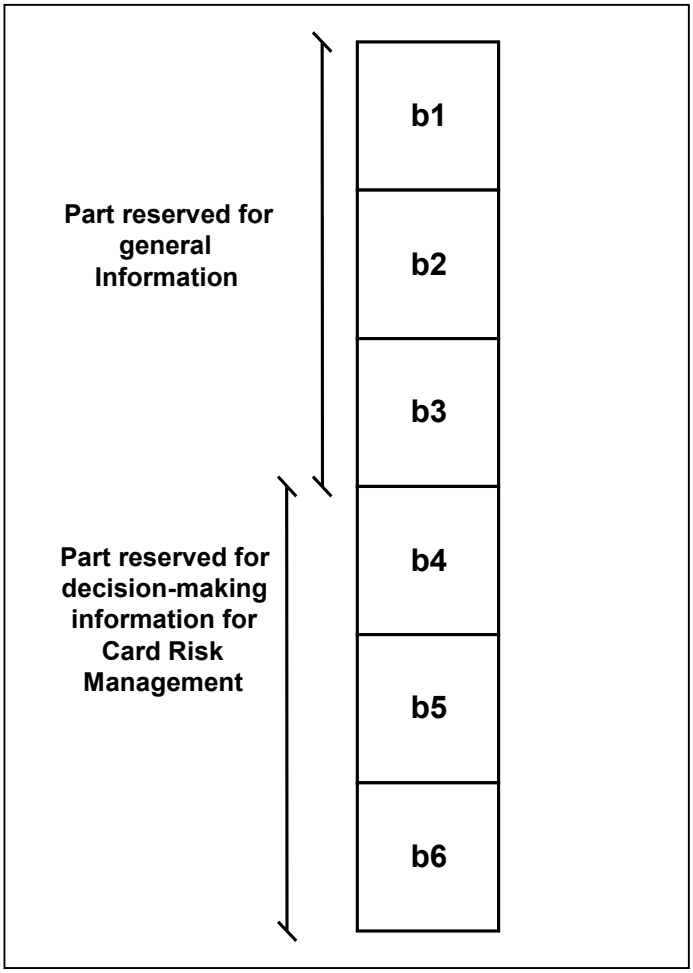
OV Loop Inc.
Ex. 2021 - Page 26

The *Card Verification Results* is a transaction-dependent data element, which reflects the current status of the M/Chip 4 applications and the results of various internal checks performed on the current transaction parameters. It is composed of two parts, containing the following:

- Three bytes for information (part 1)
- Three bytes for Card Risk Management (part 2)

Figure 1.1 illustrates the two parts of the *Card Verification Results* data element.

Figure 1.1—Parts 1 and 2 of the Card Verification Results



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 27

The entire *Card Verification Results* is included in the *Issuer Application Data* communicated to you:

- During an online transaction, when it is possible to connect to the issuer.
- In the clearing message for a transaction, if chip data is included in clearing messages.

The second, decision-making part of the *Card Verification Results* is used for Card Risk Management. It is internally compared to the *Card Issuer Action Codes* to decide which cryptogram to give in the response to the **GENERATE AC** (i.e. whether to decline or accept a transaction, or whether to go online to the issuer.)

This organization of the *Card Verification Results* simplifies the following:

- Customization of the application behavior during the personalization, as only the decision-making part of the *Card Verification Results* is relevant.
- Interpretation of a transaction's *Card Verification Results* value.

1.1.5 How You Control Offline Risk

The M/Chip 4 applications offer you powerful tools to manage the risk presented by offline cardholder transactions. As there is no connection to the issuer for such transactions, it is the M/Chip 4 application that decides whether to accept transactions offline, on your behalf. You only acknowledge such offline transactions during the transaction clearing.

The M/Chip 4 applications limit offline risk using two counters for transactions accepted offline. When these counters exceed certain limits, the M/Chip 4 applications can take risk management decisions.

These counters are as follows:

- *Cumulative Offline Transaction Amount*

  The *Cumulative Offline Transaction Amount* represents the cumulative value of transactions accepted offline. The M/Chip 4 applications add the transaction value to the *Cumulative Offline Transaction Amount* when:

  – The transaction is in the counter currency.

  – The transaction is in a currency that can be converted into the counter currency.

  The M/Chip 4 applications support currency conversion for five currencies that you define at personalization.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 28

- *Consecutive Offline Transactions Number*

  The *Consecutive Offline Transactions Number* represents the number of transactions accepted offline, for which the value was not added to the *Cumulative Offline Transaction Amount*. This is the case for transactions performed in a currency not recognized by the M/Chip 4 applications. In such cases, the *Consecutive Offline Transactions Number* counter is incremented.

When an offline counter does not fall within one of its limits, the M/Chip 4 applications enable you to modify the application behavior, with typical modifications as follows:

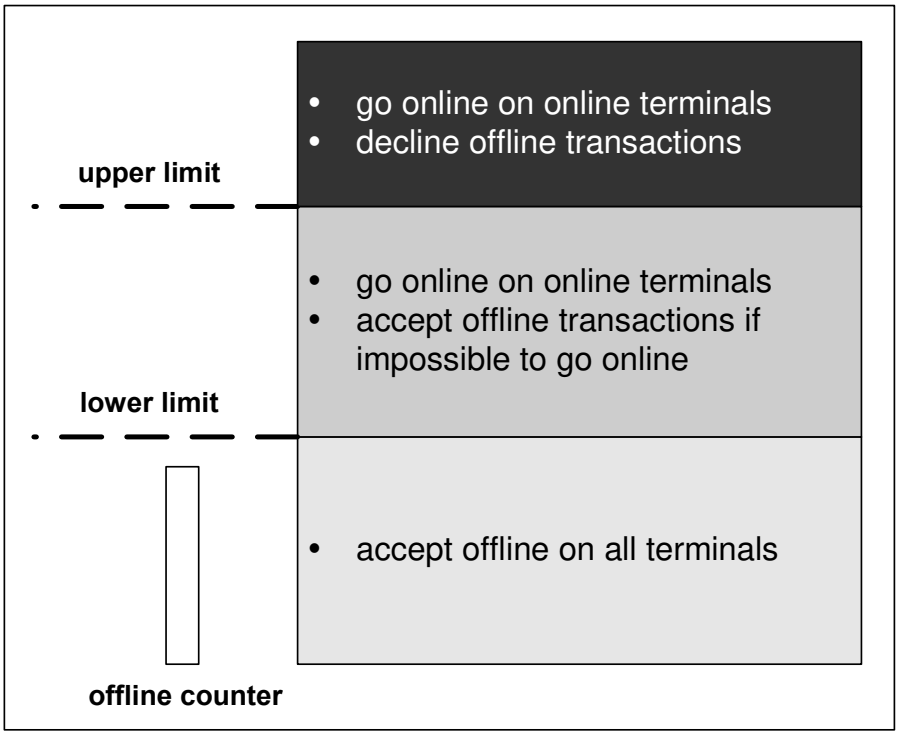
- If the offline counter is less than or equal to the lower limit, the transaction is accepted offline even on an online capable terminal.
- If the offline counter is above the lower limit, the transaction goes online to the issuer on an online capable terminal, but is still accepted if it is not possible to go online (i.e. the terminal is offline only or it was not possible to go online to the issuer).
- If the offline counter is above the upper limit, the transaction goes online to the issuer on an online capable terminal, but is declined if it is not possible to go online.

Figure 1.2 illustrates typical usage of the offline limits and offline counters.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 29

Figure 1.2—Typical Usage of Offline Limits and Offline Counters



You receive the values of the offline counters during online transactions. Based on the amount already spent offline by the cardholder and on the cardholder's account balance, you can choose to accept the online transaction and, when appropriate:

- Reset the offline counters to zero.
- Set the counters to the upper limits.
- Add the current transaction to the offline counters.
- Leave the counters unchanged.

During personalization, you determine the following:

- Whether offline counters are sent in clear or encrypted
- Whether to include the offline counters as input to the Application Cryptogram

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 30

1.1.6 Migration Facilities

The M/Chip 4 applications offer you various migration facilities as follows:

- Migration to chip
- Migration from M/Chip Lite 2.1 to M/Chip 4 applications
- Migration from M/Chip Select 2 to M/Chip Select 4
- Migration from M/Chip Lite 4 to M/Chip Select 4

To support the migration of issuers and acquirers to chip, the M/Chip 4 applications support the magnetic stripe grade mode. If you support the magnetic stripe grade issuer mode, you are able to perform online transactions without cryptography. This feature is useful in situations where:

- You use the Chip to Magnetic Stripe Conversion service.
- You do not use a security module for online transactions (except for the online PIN verification module).

For the migration from M/Chip 2 to M/Chip Select 4 or to the M/Chip Lite 4, both M/Chip 4 applications support EPI/MCI session key derivation.

Dec 2004



Note **This publication uses the following naming conventions. The EMV 96 session key derivation method is called "EPI/MCI session key derivation." The session key derivation defined in EMV 2000 is called "EMV 2000 session key derivation."**



Note **M/Chip 2 supports only EPI/MCI session key derivation**

Dec 2004

However, there are minor modifications to the input to the ARQC, TC, and AAC resulting from the extension of the length of the *Card Verification Results* to six bytes. For the migration from M/Chip Lite 4 to M/Chip Select 4, the M/Chip Select 4 application supports the same online messages, including the cryptograms.

1.1.7 Offline PIN Management Facilities

The following sections describe the offline PIN management facilities offered by the M/Chip 4 applications.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 31

1.1.7.1 Update of Offline PIN Try Counter

The M/Chip 4 applications allow you to update the card internal PIN Try Counter, the offline *PIN Try Counter*, during an online transaction. This counter represents the number of PIN tries remaining in offline mode whereas the online *PIN Try Counter* represents the number of PIN tries remaining in online mode and you store this counter as for magnetic stripe-based transactions.

The offline *PIN Try Counter* is included in the information part of the *Card Verification Results*, and is therefore sent to you in an online transaction. In the response, you may request the M/Chip 4 application to update the offline *PIN Try Counter* and thereby synchronize the two counters.

1.1.7.2 Personalization as 'No Offline Signature Application"

The M/Chip 4 applications can be personalized as a 'no offline signature' application. In this case, when the PIN is not verified offline, the application performs the transaction online.

The M/Chip 4 applications provide a means of efficiently solving the problem raised by offline PIN and online PIN de-synchronization at card issuance. This situation occurs when a new card is issued with an offline PIN value that differs from the current online PIN value. For example, the cardholder modifies the online PIN value of his current card, before he receives a new card that has already been personalized with his old PIN value.

1.1.7.3 Protections against Wedge Device Attacks

The M/Chip 4 applications check that the terminal is not misled about the result of the offline PIN verification. Combined with the CDA supported by M/Chip Select 4, this feature helps to protect against wedge device attacks to avoid offline PIN validation.

Dec 2004

1.1.8 Acceptance on CAT Level 3 Terminals

Category 3 Cardholder Activated Terminals (CAT Level 3) are unattended, offline-only terminals (e.g. toll gates). On such terminals, transactions can only be performed offline and must have a low value. You can personalize the M/Chip 4 application so that on CAT Level 3 terminals, the check on the CIAC-default is skipped. You can use this facility to ensure that service delivery is not compromised by the strict respect of the offline limits.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 32

1.1.9 Post-issuance Updates and Maintenance

A large number of the M/Chip 4 data elements set at personalization can be updated after card issuance, under your control. This feature is particularly useful if you plan to modify the personalization settings during the card's lifetime.

1.1.10 Transaction Log

Dec 2004

The M/Chip 4 applications contain a log of transactions. This log keeps track of the ten most recent transactions completed with a TC or an AAC, and is accessible to the cardholder.

1.1.11 Specific Behavior for Domestic or International Transactions

The M/Chip 4 applications allow you to define card behavior dependent on whether a transaction is domestic or international. You can use this functionality to:

- Send all domestic transactions online to the issuer
- Send all international transactions online to the issuer

1.1.12 Additional Functionality

The M/Chip 4 applications also support some functionality that is not aimed at the traditional MasterCard or Maestro products. This functionality is partially presented in this document but the envisaged usage is not explained. MasterCard anticipates that future versions of this document will incorporate these explanations.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 33

1.2 M/Chip Select 4, M/Chip Lite 4 and EMV 2000

The M/Chip Select 4 application implements the new features defined in the 2000 version of the EMV standard as follows:

- EMV 2000 session key derivation
- Combined DDA/AC generation

The M/Chip Select 4 application is fully compliant with the EMV 2000 standard.

The M/Chip Lite 4 application implements the EMV 2000 session key derivation, but does not support the Combined DDA/AC generation.

The M/Chip Lite 4 application is fully compliant with the EMV 2000 standard.

1.2.1 EMV 2000 Session Key Derivation

The EMV 2000 standard defines a session key derivation algorithm primarily intended to protect against statistical attacks, such as the Differential Power Analysis (DPA). The use of this session key derivation algorithm is optional in EMV 2000.

The M/Chip 4 applications implement this session key derivation algorithm, alongside the EPI/MCI session key derivation algorithm. The EPI/MCI session key derivation algorithm has been kept to facilitate your migration from earlier applications to the M/Chip 4 application.

You select the EMV 2000 or the EPI/MCI session key derivation algorithm when the M/Chip 4 application is personalized.

1.2.2 Combined DDA/AC Generation

The EMV 2000 standard defines how to combine the Dynamic Data Authentication with the generation of the application cryptogram. This Combined DDA/AC generation mechanism protects against attacks on the card to terminal interface. Card application support for this mechanism is optional in EMV 2000.

The M/Chip Select 4 application supports the Combined DDA/AC generation as defined in *EMV 2000 Specifications*, and in the bulletins updating these specifications as listed in the "Related Publications" section of "Using this Manual."

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 34

2 Card Risk Management

This chapter describes Card Risk Management for the M/Chip 4 application.

2.1 Introduction 2-1
2.1.1 Offline Card Risk Management 2-1
2.1.2 Online Card Risk Management 2-2

2.2 Card Verification Results 2-2

2.3 Card Issuer Action Codes 2-6
2.3.1 Content of the Card Issuer Action Codes 2-7
2.3.2 Card Issuer Action Code—Decline 2-10
2.3.3 Card Issuer Action Code—Online 2-11
2.3.4 Card Issuer Action Code—Offline 2-11

2.4 Offline Counters and Offline Limits 2-12
2.4.1 Offline Counters 2-12
2.4.2 Offline Limits 2-13
2.4.3 Comparison between Offline Counters and Offline Limits 2-14

2.5 Card Risk Management Algorithm 2-16
2.5.1 First Occurrence of GENERATE AC 2-16
2.5.1.1 Terminal Requests an AAC at First GENERATE AC 2-17
2.5.1.2 Terminal Requests a TC at First GENERATE AC 2-17
2.5.1.2.1 Online-Capable Terminals 2-20
2.5.1.2.2 Non-online Capable Terminals 2-20
2.5.1.3 Terminal Requests an ARQC at First GENERATE AC 2-21
2.5.2 Second Occurrence of GENERATE AC 2-21
2.5.2.1 Unable to Go Online. 2-24
2.5.2.2 Issuer Authentication Data Present 2-26
2.5.2.2.1 Issuer Authentication Data Verification Succeeds 2-27
2.5.2.2.2 Issuer Authentication Data Verification Fails 2-27
2.5.2.3 Issuer Authentication Data Not Present 2-27

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 35

2.1 Introduction

Card Risk Management is the process the M/Chip 4 applications use to determine how to respond to the application cryptogram (AC) request sent by the terminal.

Card Risk Management has two components:

- Offline Card Risk Management
- Online Card Risk Management

2.1.1 Offline Card Risk Management

Offline Card Risk Management is the process whereby the M/Chip 4 applications approve the transactions without online authorization from the issuer. Offline Card Risk Management therefore defines the conditions you specify under which the M/Chip 4 applications:

- approve the transactions offline on your behalf
- decide to send a transaction online to the issuer for online authorization on an online-capable terminal
- decline the transaction offline on your behalf.

You define these conditions at card personalization and can modify them later. The M/Chip 4 applications consider a transaction from various perspectives, including the following:

- Has offline PIN verification been performed?
- Has offline PIN verification failed?
- Has the PIN Try Limit been exceeded?
- Is this a domestic or international transaction?
- Has the terminal erroneously considered that the offline PIN is OK?
- Has the offline consecutive limit been exceeded?
- Has the offline cumulative amount been exceeded?
- Should the transaction go online because the 'Go Online on Next Transaction' bit was set?
- Did issuer authentication fail in a previous transaction?
- Was the issuer script received or failed in a previous transaction?
- Was a match found in the additional check table?

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 36

- Is the terminal a CAT level 3 terminal?
- Was the transaction unable to go online?

You can use the response to each of these questions to determine Offline Risk Management, i.e. to take one of the following decisions:

- To approve the transactions offline, on your behalf
- To send a transaction online to the issuer for online authorization on an online-capable terminal
- To decline the transaction offline, on your behalf.

2.1.2 Online Card Risk Management

Online Card Risk Management is the process whereby you accept or decline an online transaction. During the online transaction, you receive information from the M/Chip 4 application that you use to make the final decision whether to approve or decline.

2.2 Card Verification Results

Card Risk Management in the M/Chip 4 applications shows similarities with the EMV 2000 Terminal Risk Management as follows:

- The *Card Verification Results* play the role of the *Terminal Verification Results*.
- The *Card Issuer Action Codes* play the role of the *Issuer Action Codes* and *Terminal Action Codes*.

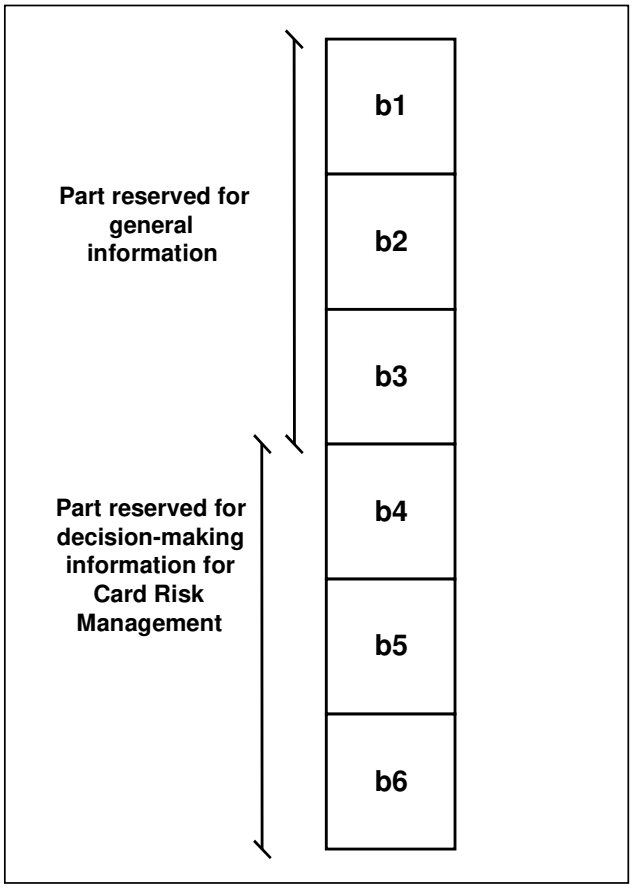
The *Card Verification Results* is a six-byte internal data element divided in two parts:

- Part 1 (bytes 1 to 3) is for information
- Part 2 (bytes 4 to 6) is for Card Risk Management

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 37

Figure 2.1—Parts 1 and 2 of the Card Verification Results



You receive the complete *Card Verification Results* included in the *Issuer Application Data*:

- During an online transaction, if the connection to the issuer is possible
- In the clearing record of a transaction, when chip data is cleared

The information part of the *Card Verification Results* provides you with information. It plays no role in Card Risk Management.

The decision-making information part of the *Card Verification Results* is used for Card Risk Management. It is internally compared to the *Card Issuer Action Codes* to decide which cryptogram is given in the response to the **GENERATE AC**, i.e. to decide between:

- Declining a transaction
- Going online to the issuer
- Accepting a transaction

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 38

The *Card Verification Results* is a transaction-dependent data element reflecting the current status of the M/Chip 4 application and the results of several internal checks done on the current transaction parameters.

Tables 2.1 – 2.3 provide the content of the decision-making information part of the *Card Verification Results* for the M/Chip 4 application.

Table 2.1 describes the content of byte 4 of the *Card Verification Results*. Byte 4 contains decision-making information for the current transaction.

Table 2.1—Card Verification Results, Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								**Reserved**
0								Other Value RFU
	x							**Unable To Go Online Indicated**
	0							Unable To Go Online Not Indicated
	1							Unable To Go Online Indicated
		x						**Offline PIN Verification Not Performed**
		0						Offline PIN Verification Performed
		1						Offline PIN Verification Not Performed
			x					**Offline PIN Verification Failed**
			0					No Failure Of Offline PIN Verification
			1					Offline PIN Verification Failed
				x				**PTL Exceeded**
				0				*PTL* Not Exceeded
				1				*PTL* Exceeded
					x			**International Transaction**
					0			Domestic Transaction
					1			International Transaction
						x		**Domestic Transaction**
						0		International Transaction
						1		Domestic Transaction
							x	**Terminal Erroneously Considers Offline PIN OK**
							0	Terminal Does Not Erroneously Consider Offline PIN OK
							1	Terminal Erroneously Considers Offline PIN OK

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 39

Table 2.2 describes the content of byte 5 of the *Card Validation Results*. Byte 5 contains decision-making information from the current transaction and from the transaction that preceded it (i.e. current transaction – 1).

Table 2.2—Card Verification Results, Byte 5

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								**Lower Consecutive Offline Limit Exceeded**
0								*Lower Consecutive Offline Limit Not Exceeded*
1								*Lower Consecutive Offline Limit Exceeded*
	x							**Upper Consecutive Offline Limit Exceeded**
	0							*Upper Consecutive Offline Limit Not Exceeded*
	1							*Upper Consecutive Offline Limit Exceeded*
		x						**Lower Cumulative Offline Limit Exceeded**
		0						*Lower Cumulative Offline Limit Not Exceeded*
		1						*Lower Cumulative Offline Limit Exceeded*
			x					**Upper Cumulative Offline Limit Exceeded**
			0					*Upper Cumulative Offline Limit Not Exceeded*
			1					*Upper Cumulative Offline Limit Exceeded*
				x				**Go Online On Next Transaction Was Set** [a]
				0				*Go Online On Next Transaction Was Not Set*
				1				*Go Online On Next Transaction Was Set*
					x			**Issuer Authentication Failed** [a]
					0			*No Issuer Authentication Failed*
					1			*Issuer Authentication Failed*
						x		**Script Received** [b]
						0		*No Script Received*
						1		*Script Received*
							x	**Script Failed** [b]
							0	*No Script Failed*
							1	*Script Failed*

[a] In this transaction or in a previous one.

[b] In a previous transaction.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 40

Table 2.3 describes the content of byte 6 of the *Card Validation Results*. Byte 6 contains decision-making information from the current transaction.

Table 2.3—Card Verification Results, Byte 6

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			**Reserved**
0	0	0	0	0	0			*Other value RFU*
						x		**Match Found In Additional Check Table**
						0		*No Match Found In Additional Check Table*
						1		*Match Found In Additional Check Table*
							x	**No Match Found In Additional Check Table**
							0	*Match Found In Additional Check Table*
							1	*No Match Found In Additional Check Table*

2.3 Card Issuer Action Codes

The *Card Issuer Action Codes* are three-byte internal data elements set at personalization and are transaction independent. There are three types as follows:

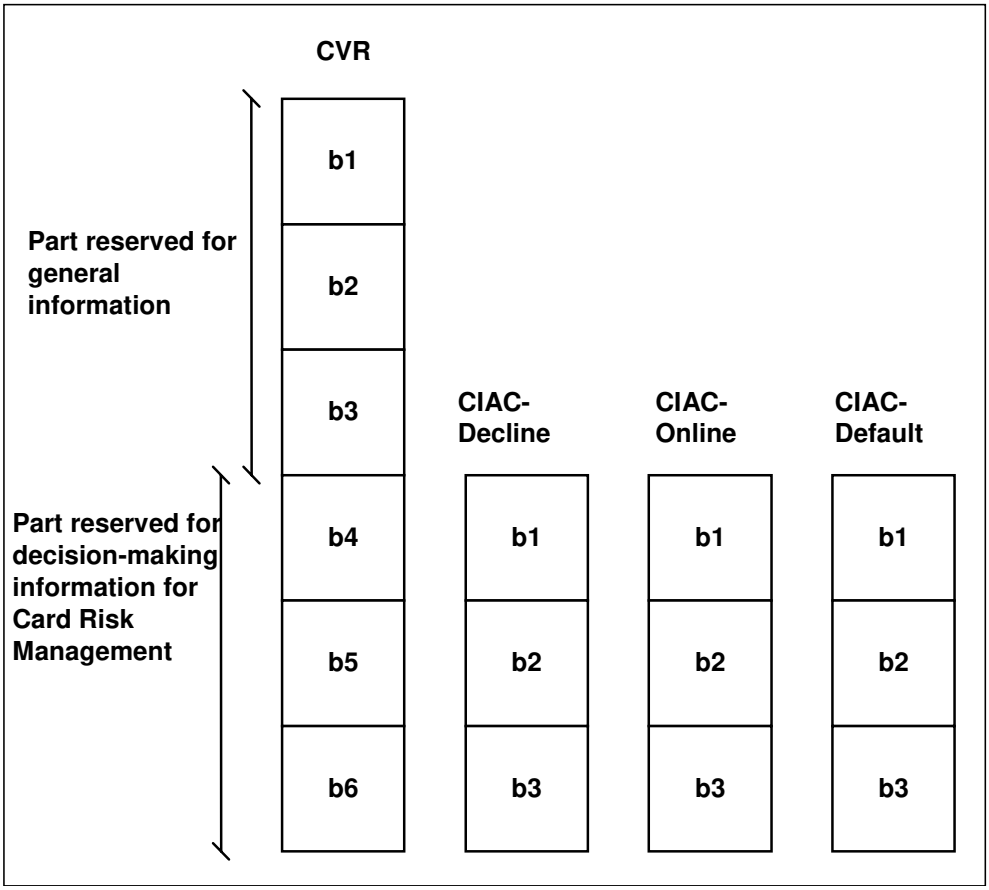
- *Card Issuer Action Code—Decline*
- *Card Issuer Action Code—Online*
- *Card Issuer Action Code—Default*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 41

The M/Chip 4 applications compare the *Card Issuer Action Codes* with the decision-making information part of the *Card Verification Results* in Figure 2.2.

Figure 2.2—Card Verification Results and Card Issuer Action Codes



The following sections provide the content and a description of the functionality of the *Card Issuer Action Codes*.

2.3.1 Content of the Card Issuer Action Codes

Tables 2.4 – 2.6 provide the content of the *Card Issuer Action Codes* for the M/Chip 4 applications.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 42

Table 2.4 describes the content of byte 1. Byte 1 contains information for the current transaction.

Table 2.4—Card Issuer Action Code, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								**Reserved-No Meaning**
	x							**Unable To Go Online Indicated**
	0							*Do Not Take Action If Unable To Go Online Indicated*
	1							*Take Action If Unable To Go Online Indicated*
		x						**Offline PIN Verification Not Performed**
		0						*Do Not Take Action If Offline PIN Verification Not Performed*
		1						*Take Action If Offline PIN Verification Not Performed*
			x					**Offline PIN Verification Failed**
			0					*Do Not Take Action If Offline PIN Verification Failed*
			1					*Take Action If Offline PIN Verification Failed*
				x				**PTL Exceeded**
				0				*Do Not Take Action If PTL Exceeded*
				1				*Take Action If PTL Exceeded*
					x			**International Transaction**
					0			*Do Not Take Action If International Transaction*
					1			*Take Action If International Transaction*
						x		**Domestic Transaction**
						0		*Do Not Take Action If Domestic Transaction*
						1		*Take Action If Domestic Transaction*
							x	**Terminal Erroneously Considers Offline PIN OK**
							0	*Do Not Take Action If Terminal Erroneously Considers Offline PIN OK*
							1	*Take Action If Terminal Erroneously Considers Offline PIN OK*

Table 2.5 describes the content of byte 2. Byte 2 contains information from the current transaction and from the transaction that preceded it (i.e. current transaction – 1).

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 43

Table 2.5—Card Issuer Action Code, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								**Lower Consecutive Offline Limit Exceeded**
0								*Do Not Take Action If Lower Consecutive Offline Limit Exceeded*
1								*Take Action If Lower Consecutive Offline Limit Exceeded*
	x							**Upper Consecutive Offline Limit Exceeded**
	0							*Do Not Take Action If Upper Consecutive Offline Limit Exceeded*
	1							*Take Action If Upper Consecutive Offline Limit Exceeded*
		x						**Lower Cumulative Offline Limit Exceeded**
		0						*Do Not Take Action If Lower Cumulative Offline Limit Exceeded*
		1						*Take Action If Lower Cumulative Offline Limit Exceeded*
			x					**Upper Cumulative Offline Limit Exceeded**
			0					*Do Not Take Action If Upper Cumulative Offline Limit Exceeded*
			1					*Take Action If Upper Cumulative Offline Limit Exceeded*
				x				**Go Online On Next Transaction Was Set**
				0				*Do Not Take Action If Go Online On Next Transaction Was Set*
				1				*Take Action If Go Online On Next Transaction Was Set*
					x			**Issuer Authentication Failed**
					0			*Do Not Take Action If Issuer Authentication Failed*
					1			*Take Action If Issuer Authentication Failed*
						x		**Script Received**
						0		*Do Not Take Action If Script Received*
						1		*Take Action If Script Received*
							x	**Script Failed**
							0	*Do Not Take Action If Script Failed*
							1	*Take Action If Script Failed*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 44

Table 2.6 describes the content of byte 3. Byte 3 contains decision-making information from the current transaction.

Table 2.6—Card Issuer Action Code, Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			**Reserved-No Meaning**
						x		**Match Found in Additional Check Table**
						0		*Do Not Take Action if Match Found in Additional Check Table*
						1		*Take Action if Match Found in Additional Check Table*
							x	**No Match Found in Additional Check Table**
							0	*Do Not Take Action if No Match Found in Additional Check Table*
							1	*Take Action if No Match Found in Additional Check Table*

2.3.2 Card Issuer Action Code—Decline

The *Card Issuer Action Code—Decline* codes the reasons for declining a transaction. If the terminal requests a TC or an ARQC in the first **`GENERATE AC`**, as a first step in its Card Risk Management the M/Chip 4 application always checks the *Card Issuer Action Code—Decline* against the decision-making information part of the *Card Verification Results*.

If ...	Then the M/Chip 4 application ...
A bit in the *Card Issuer Action Code—Decline* **and** its corresponding bit in the *Card Verification Results* [4-6] [a] are both set	• Declines the transaction. • Computes an AAC.
The bits do not match	• Verifies the *Card Verification Results* [4-6] against either the *Card Issuer Action Code—Online* **or the** *Card Issuer Action Code—Default* depending on the terminal online/offline capability.[b]

[a] Decision-making information—current transaction, current + last online transaction.

[b] As described in the "Terminal Requests a TC at First GENERATE AC" and in the "Terminal Requests an ARQC at First GENERATE AC" sections.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 45

There are few reasons for declining a transaction before attempting to go online to the issuer. In a standard configuration the *Card Issuer Action Code—Decline* is likely to be personalized with a value of zeros. See section 6.3.3.3.1 for the explanation of other settings.

Dec 2004

2.3.3 Card Issuer Action Code—Online

This *Card Issuer Action Code—Online* codes the reasons for sending a transaction online to the issuer. If the terminal is online capable and requests a TC in the first **GENERATE AC**, as part of Card Risk Management the M/Chip 4 application checks the *Card Issuer Action Code—Online* against the decision-making part of the *Card Verification Results*.

If ...	Then the M/Chip 4 application ...
A bit in the *Card Issuer Action Code—Online* **and** its corresponding bit in the *Card Verification Results* [4-6] [a] are both set	• Computes an ARQC.
The bits do not match	• Approves the transaction. • Computes a TC.

[a] Decision-making information—current transaction, current transaction, current + last online transaction.

2.3.4 Card Issuer Action Code—Offline

This *Card Issuer Action Code—Offline* codes the reasons for declining a transaction if the terminal is not online capable. The M/Chip application uses the *Card Issuer Action Code—Offline* for Card Risk Management in two situations:

- At first **GENERATE AC**, if the terminal is offline only
- At second **GENERATE AC**, if the terminal cannot go online, but still requests a TC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 46

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code—Default* **and** its corresponding bit in the *Card Verification Results* [4-6] [a] are both set	• Declines the transaction • Computes an AAC
The bits do not match	• Approves the transaction • Computes a TC

[a] Decision-making information—current transaction, current transaction, current + last online transaction.

2.4 Offline Counters and Offline Limits

The offline counters are two internal counters used to limit your offline risk. This risk is the amount spent by the cardholder in offline mode. Since there is no connection to the issuer for offline transactions, it is the M/Chip 4 application that decides whether to accept the transactions offline on your behalf. You only acknowledge offline transactions when they are cleared.

To limit offline risk, the offline counters count the transactions accepted offline and enable you to make decisions if the counters have reached certain limits.

2.4.1 Offline Counters

The *Cumulative Offline Transaction Amount* represents the cumulative value of transactions accepted offline. The value of transactions are accumulated when they meet one of the following criteria:

- They are in the counter currency.
- They are in a currency that can be converted into the counter currency by the M/Chip 4 application.

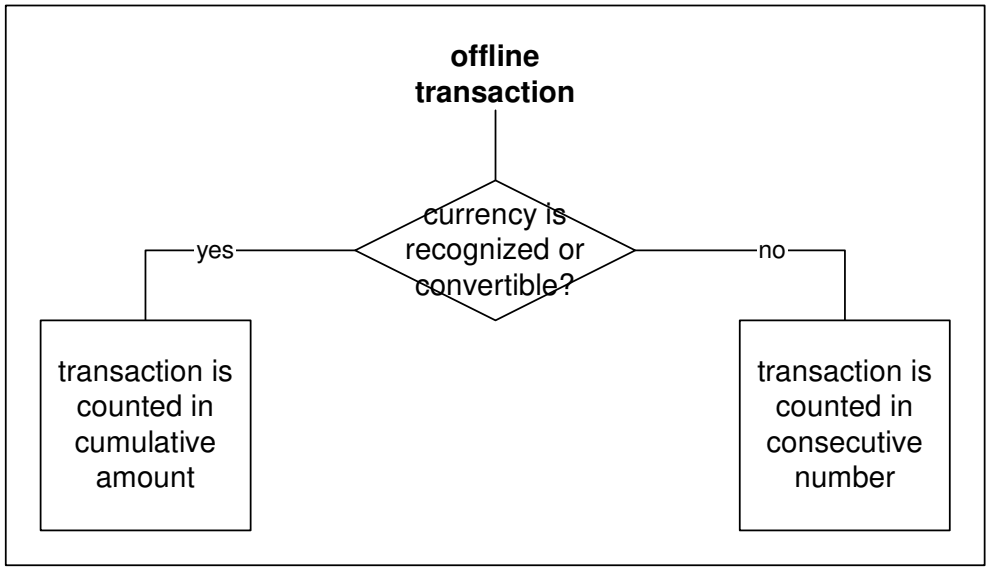
If the transaction is performed in a currency not recognized by the M/Chip 4 application, the transaction value cannot be accumulated. In this case, the M/Chip 4 application counts the transaction using the second offline counter: the *Consecutive Offline Transactions Number*. The *Consecutive Offline Transactions Number* represents the number of transactions accepted offline without being accumulated in the *Cumulative Offline Transaction Amount*.

Each time a transaction is accepted offline, the M/Chip 4 application only updates one of the counters.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 47

Figure 2.3—Usage of Offline Counters



2.4.2 Offline Limits

In addition to offline counters, the M/Chip 4 application uses offline limits. Offline limits are parameters that you set at personalization. When one of the offline counters has reached a limit, the M/Chip 4 application takes specific actions that you customized at personalization. Table 2.7 lists the four offline limits.

Table 2.7—Enter caption text

Offline Limit
Lower Consecutive Offline Limit [a]
Upper Consecutive Offline Limit [a]
Lower Cumulative Offline Transaction Amount [b]
Upper Cumulative Offline Transaction Amount [b]

[a] Checked against the *Consecutive Offline Transactions Number*.

[b] Checked against the *Cumulative Offline Transaction Amount*.

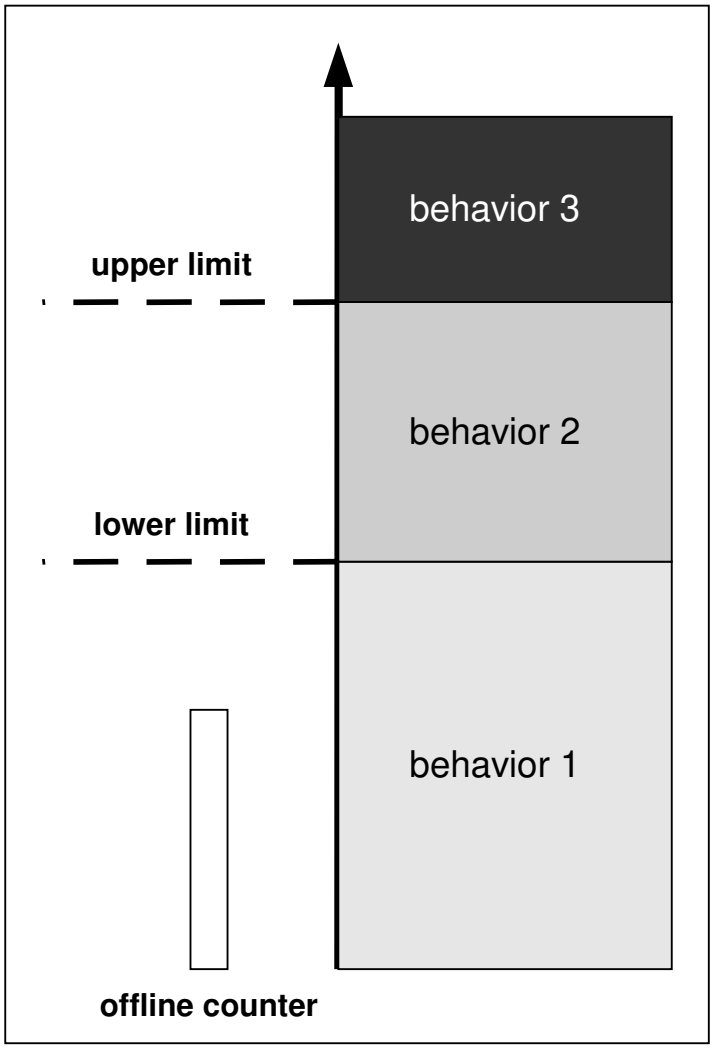
© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 48

2.4.3 Comparison between Offline Counters and Offline Limits

The offline counters are compared internally with the offline limits. If a counter has reached its lower or upper limit, a specific action can be triggered, as illustrated in Figure 2.4.

Figure 2.4—Offline Limits and Offline Counters



The M/Chip 4 application enables you to modify the M/Chip 4 application behavior if an offline counter reaches one of its limits.

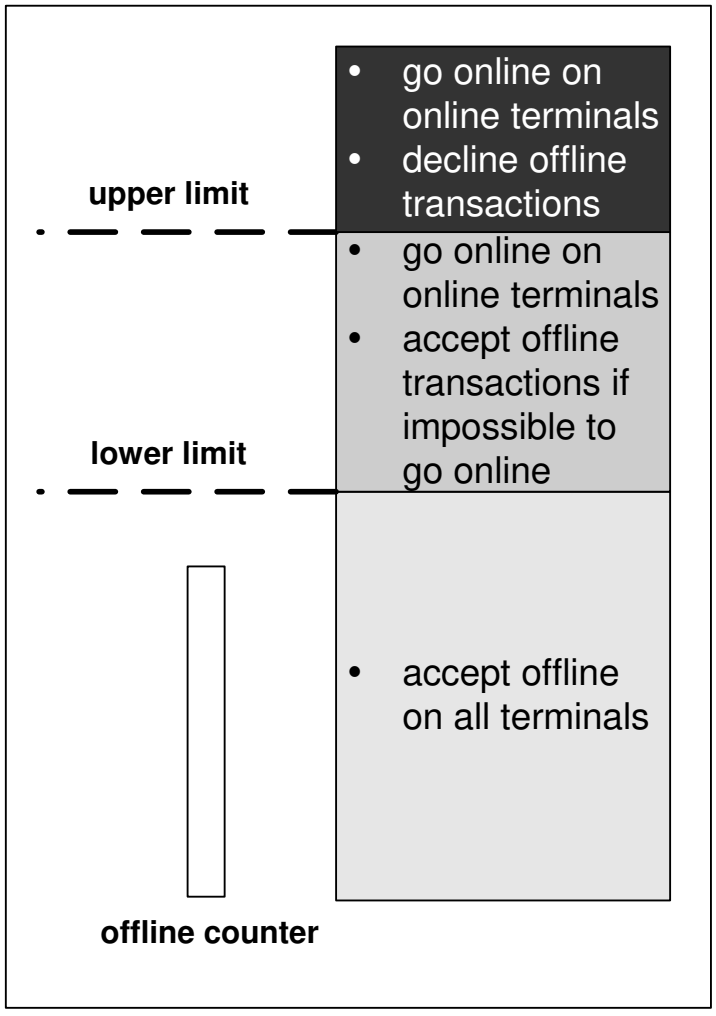
© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 49

Figure 2.5 illustrates typical ways in which offline limits are used:

- If the offline counter is below the lower limit, the transaction is accepted offline (i.e. the M/Chip 4 application computes a TC), even on an online capable terminal (behavior 1 in Figure 2.4).
- If the offline counter reaches the lower limit, the transaction goes online to the issuer on an online capable terminal. It is still accepted if it is not possible to go online (e.g. because the terminal is offline only or because it was not possible to go online to the issuer) (behavior 2 in Figure 2.4).
- If the offline counter reaches the upper limit, the transaction goes online to the issuer on an online capable terminal but the transaction is declined if it is not possible to go online (behavior 3 in Figure 2.4).

Figure 2.5—Typical Usage of Offline Limits and Offline Counters



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 50

You receive the offline counters during online transactions. Based on the amount already spent offline by the cardholder and on the cardholder's account balance, you can decide to accept the online transaction and optionally reset the counters.

2.5 Card Risk Management Algorithm

Card Risk Management occurs on two occasions as follows:

- In the first occurrence of the **GENERATE AC**
- In the second occurrence of the **GENERATE AC**

The following sections give an overview of the Card Risk Management performed by the M/Chip 4 applications. Refer to the *M/Chip 4 Card Application Specifications for Debit and Credit* for a detailed definition.

2.5.1 First Occurrence of GENERATE AC

Before Card Risk Management, the terminal performs Terminal Risk Management. In the first **GENERATE AC**, the terminal requests a decline (AAC), offline approval (TC) or online transaction (ARQC).

The following sections describe the Card Risk Management performed by the M/Chip 4 applications for each of these requests.

The first step of Card Risk Management is to fill the *Card Verification Results* with values reflecting the transaction. The M/Chip 4 applications then take decisions by comparing the decision-making information part of the *Card Verification Results* with the *Card Issuer Action Codes*.

The *Card Verification Results* is first updated to reflect:

- If offline PIN verification has been performed (in plaintext or in encrypted mode)
- The result of offline PIN verification
- If DDA has been performed (M/Chip Select 4 only)
- If one or more script commands has been performed
- The number of script commands processed on previous online transaction
- The number of offline PIN tries remaining
- If the PIN Try Limit has been exceeded
- If the terminal erroneously considers offline PIN is OK

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 51

- The international or domestic character of the transaction
- The state of the offline counters against the offline limits
- Your decision, when taken, to force the transaction online
- Any issuer authentication failure during a previous transaction
- Any failure during the processing of script commands during a previous transaction
- If a match was found in the additional check table

2.5.1.1 Terminal Requests an AAC at First GENERATE AC

If the terminal declines a transaction at first **GENERATE AC**, it indicates that something occurred in the previous steps of the transaction that was deemed critical for the issuer (through the Issuer Action Codes), or for the acquirer (through the Terminal Action Codes).

In this case, the Card Risk Management performed by the M/Chip 4 applications is limited to the following actions:

- Decline the transaction
- Compute an AAC

Such a declined transaction is not counted in the offline counters as it has no impact on the M/Chip 4 application status and therefore no impact on the Card Risk Management of the transactions that follow. The only traces of such a transaction in the M/Chip 4 applications are the incremented *Application Transaction Counter* (incremented in the **GET PROCESSING OPTIONS**), and the transaction details written in the chip transaction log file.



Note **It is unlikely that you would see such a transaction as clearing records are not sent for declined transactions.**

2.5.1.2 Terminal Requests a TC at First GENERATE AC

A terminal requests a TC at first **GENERATE AC** when there were no reasons:

- To decline the transaction or
- To send the transaction online to the issuer in the previous transaction steps.

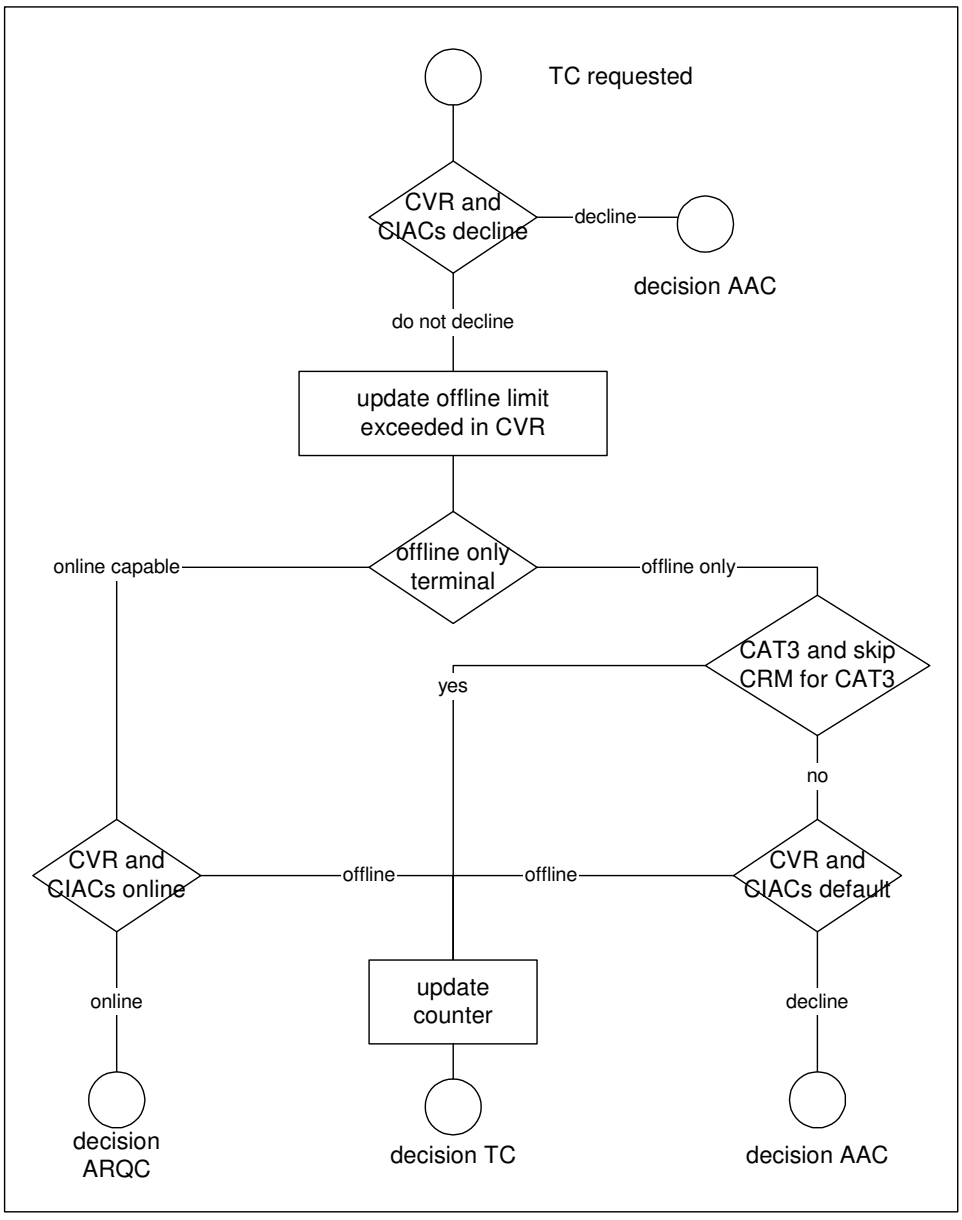
In this case, the terminal requests an offline approved transaction.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 52

Figure 2.6 illustrates the Card Risk Management performed by the M/Chip 4 application at first **GENERATE AC**, when the terminal requests offline approval of the transaction.

Figure 2.6—First GENERATE AC, TC Requested



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 53

The M/Chip 4 application first checks that there has not been a critical event by checking the *Card Verification Results* against the *Card Issuer Action Code – Decline*.

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code—Decline* **and** its corresponding bit in the *Card Verification Results* [4-6] are both set.	• Declines the transaction. • Computes an AAC.

Next, the M/Chip 4 application checks whether it can accept the transaction offline or whether it has to go online to the issuer. To do so, the M/Chip 4 application reflects the transaction value in either the *Cumulative Offline Transaction Amount* or the *Consecutive Offline Transactions Number* (depending on the transaction currency) and compares these values with the offline limits.

If …	Then the M/Chip 4 application …
The offline counters exceed the limits.	Updates the *Card Verification Results*: • *Lower Consecutive Offline Limit Exceeded* • *Upper Consecutive Offline Limit Exceeded* • *Lower Cumulative Offline Limit Exceeded* • *Upper Cumulative Offline Limit Exceeded*.

The next step depends upon the type of terminal used for the transaction. An "Offline Only" terminal has terminal types of '23', '26' or '36'. Any terminal type that is not of type '23', '26' or '36', is considered an "Online Capable" terminal.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 54

2.5.1.2.1 Online-Capable Terminals

The M/Chip 4 application checks the *Card Verification Results* against the *Card Issuer Action Code—Online*.

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code—Online* **and** its corresponding bit in the *Card Verification Results* [4-6] are both set	Computes an ARQC.
The bits do not match	• Approves the transaction. • Computes a TC. • Updates *Cumulative Offline Transaction Amount* or the *Consecutive Offline Transactions Number* (depending on the transaction currency) with transaction amount.

2.5.1.2.2 Non-online Capable Terminals

There are two scenarios for non-online capable terminals.

The M/Chip 4 application does **not** check the *Card Issuer Action Code—Default* for non-online capable terminals where:

- The terminal is a CAT-level 3 terminal (terminal type of '26') **and**
- You personalized the M/Chip 4 application to skip the check on the *Card Issuer Action Code—Default* on CAT3.

In this case, the M/Chip 4 application:

- Approves the transaction
- Computes a TC
- Updates *Cumulative Offline Transaction Amount* (if it is in the counter currency or convertible) with the transaction amount, or the *Consecutive Offline Transactions Number*.

For non-online capable terminals where:

- The terminal is not a CAT-level 3 terminal **or**
- You do not want to skip the check on CAT3, checks the *Card Issuer Action Code*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 55

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code—Default* **and** its corresponding bit in the *Card Verification Results* [4-6] are both set	• Declines the transaction. • Computes an AAC.
The bits do not match	• Approves the transaction. • Computes a TC. • Updates *Cumulative Offline Transaction Amount* (if it is in the counter currency or convertible) with the transaction amount, or the *Consecutive Offline Transactions Number*.

2.5.1.3 Terminal Requests an ARQC at First GENERATE AC

By requesting an ARQC, the terminal indicates that the transaction should go online to the issuer. Typically, this occurs on an online-capable terminal if the transaction amount is above the terminal floor limit.

In such a case, the M/Chip 4 application Card Risk Management is limited to checking that no critical events have occurred by checking the *Card Verification Results* against the *Card Issuer Action Code—Decline*.

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code—Decline* **and** its corresponding bit in the *Card Verification Results* [4-6] are both set.	• Declines the transaction. • Computes an AAC.
The bits do not match	• Computes an ARQC

2.5.2 Second Occurrence of GENERATE AC

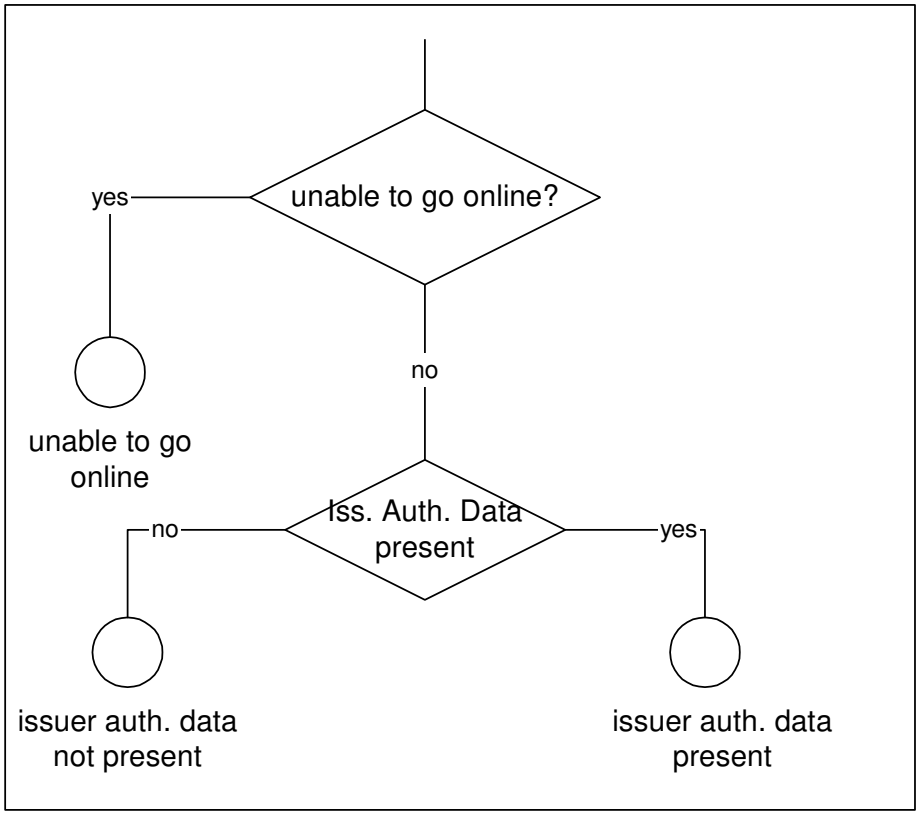
The second Card Risk Management takes place after a transaction is sent online to the issuer as a result of the first Card Risk Management.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 56

Figure 2.7 illustrates the Card Risk Management performed by the M/Chip 4 application at second **GENERATE AC**.

Figure 2.7—Second Card Risk Management at Second GENERATE AC



The M/Chip 4 application first checks if it was possible to send the transaction online to the issuer. If it was not possible to go online, the M/Chip 4 application considers the transaction as an offline transaction (i.e. unable to go online). The "Unable to Go Online." section describes the Card Risk Management for this scenario.

If the transaction goes online successfully to the issuer, the M/Chip 4 application expects you to provide a response. The response, the *Issuer Authentication Data*, contains your decision (*ARPC Response Code*) to accept or decline the transaction and the Message Authentication Code (*Authorization Response Cryptogram*) for this decision.

Two scenarios may then occur:

- Your response is complete.
- Your response is incomplete.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 57

In the first scenario, when your response is complete:

- You received the chip data in the authorization request.
- You computed the response (i.e. the *Issuer Authentication Data*).
- You sent the response to the terminal and it is complete.

The "Issuer Authentication Data Present" section describes the Card Risk Management for this scenario.

The second scenario occurs when you operate in the magstripe grade issuer mode (or you use the chip to magstripe conversion service) or if the acquirer is partial grade:

- It was possible to reach the issuer, and to get a response.
- The response does not contain the chip data (i.e. the *Issuer Authentication Data*).

The "Issuer Authentication Data Not Present" section describes the Card Risk Management for this scenario.

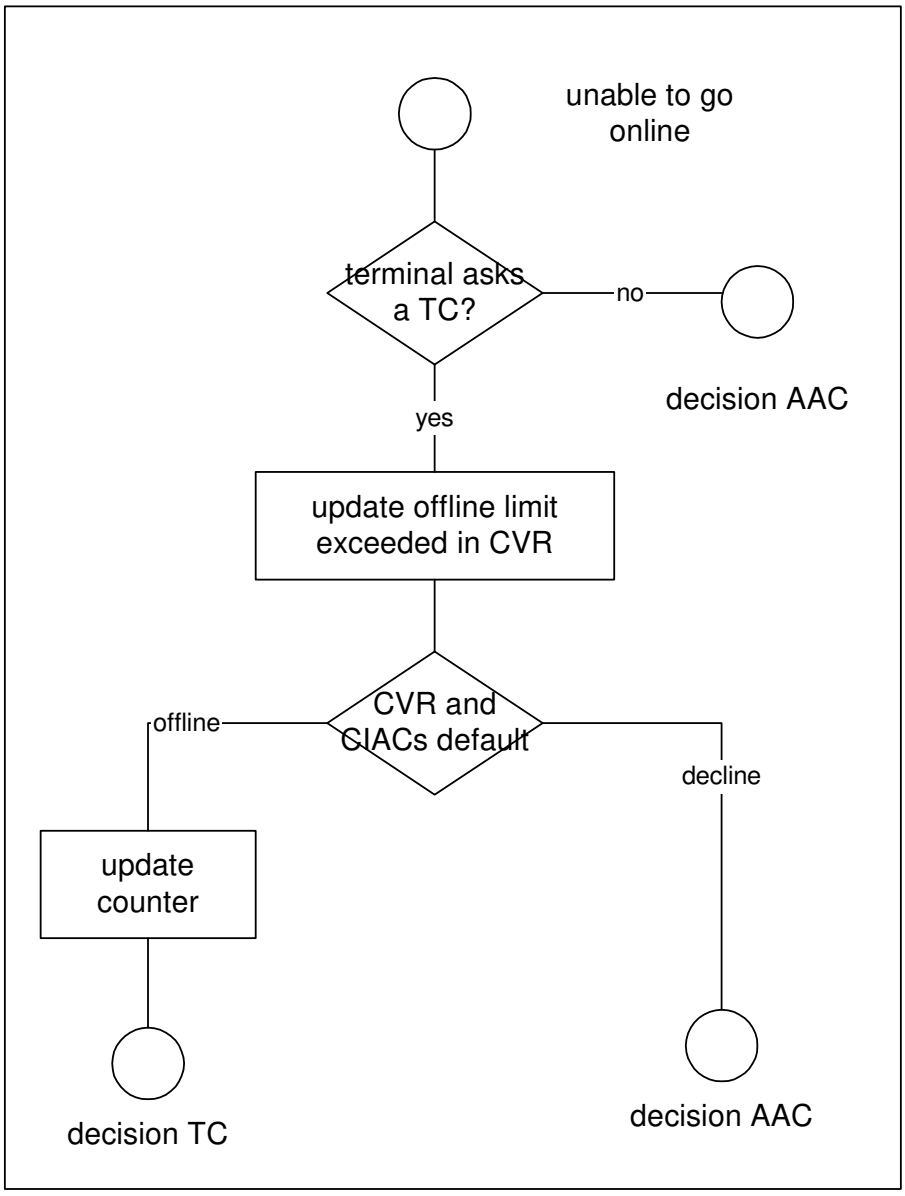
© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 58

2.5.2.1 Unable to Go Online.

Figure 2.8 illustrates the Card Risk Management performed by the M/Chip 4 application when the transaction was unable to go online to the issuer and therefore the transaction must be performed offline.

Figure 2.8—Card Risk Management When Unable to Go Online



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 59

In this situation, the terminal will either decline the transaction or request an approval.

If the terminal requests a transaction decline, the M/Chip 4 application computes an AAC. Such a declined transaction has no impact on the M/Chip 4 application status, is not counted in the offline counters and therefore does not impact the Card Risk Management of subsequent transactions.

If the terminal requests a transaction approval, the M/Chip 4 application checks whether it can accept the transaction by reflecting the transaction value in either the *Cumulative Offline Transaction Amount* or the *Consecutive Offline Transactions Number* (depending on the transaction currency) and comparing these values with the offline limits.

If …	Then the M/Chip 4 application …
The offline counters exceed the limits.	Updates the *Card Verification Results*: • *Lower Consecutive Offline Limit Exceeded* • *Upper Consecutive Offline Limit Exceeded* • *Lower Cumulative Offline Limit Exceeded* • *Upper Cumulative Offline Limit Exceeded*.

The M/Chip 4 application then checks the *Card Issuer Action Code—Default*.

If …	Then the M/Chip 4 application …
A bit in the *Card Issuer Action Code – Default* **and** its corresponding bit in the *Card Verification Results* [4-6] are both set	• Declines the transaction. • Computes an AAC.
The bits do not match	• Approves the transaction. • Computes a TC. • Updates *Cumulative Offline Transaction Amount* with the transaction amount (depending on the transaction currency) or the *Consecutive Offline Transactions Number*.

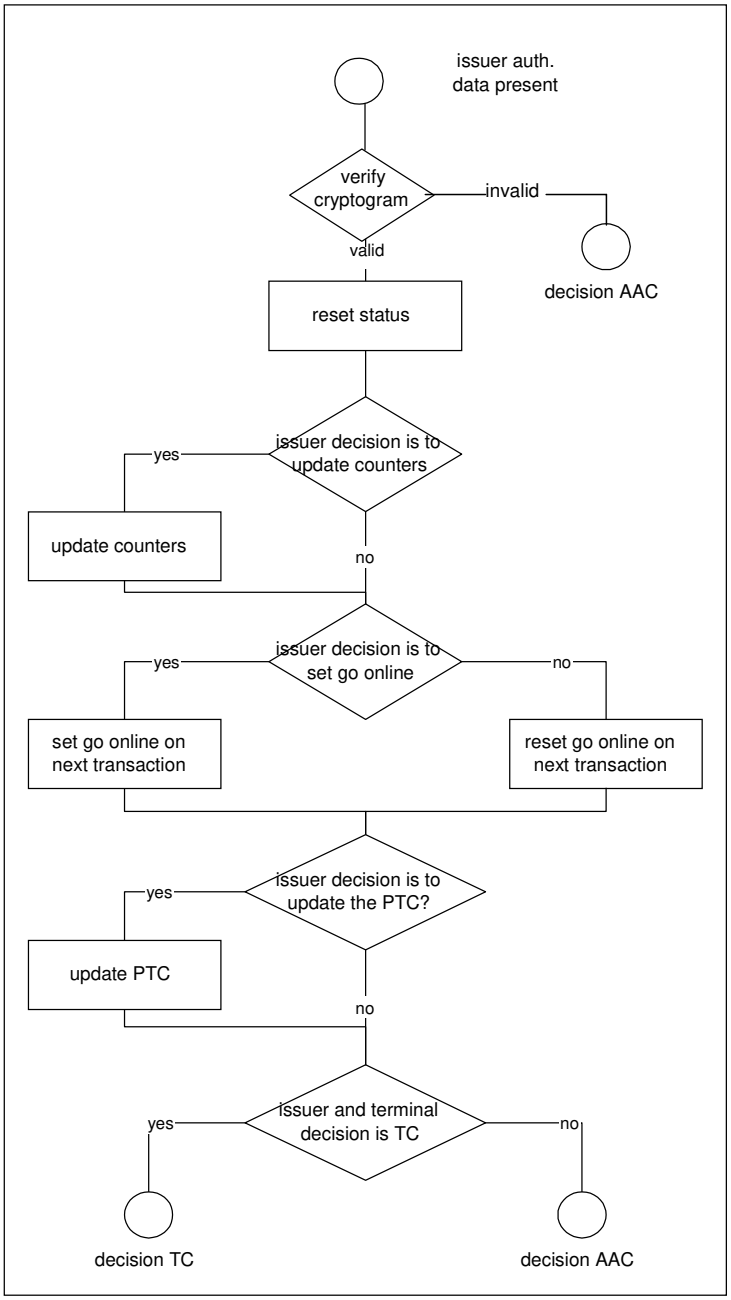
© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 60

2.5.2.2 Issuer Authentication Data Present

Figure 2.9 illustrates Card Risk Management when *Issuer Authentication Data* is present.

Figure 2.9—Card Risk Management when Issuer Authentication Data Present



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 61

When the *Issuer Authentication Data* is present, the M/Chip 4 application first verifies the cryptogram that you computed. It then takes actions depending upon the outcome of this verification.

2.5.2.2.1 Issuer Authentication Data Verification Succeeds

If the Issuer Authentication Data verification succeeds, it indicates that you acknowledged the status of the M/Chip 4 application as part of the *Card Verification Results* received in the *Issuer Application Data*. The M/Chip 4 application can therefore reset the following flags and counters:

- *Issuer Authentication Failed on Online Transaction Flag*
- *Script Received on Online Transaction Flag*
- *Script Failed on Online Transaction Flag* **and**
- *Number of Issuer Script Commands Received on Last Online Transaction*.

The M/Chip 4 application can then perform any of the following actions as :

- Update of the offline counters
- Set or reset of *Go Online on Next Transaction*
- Update of the *PIN Try Counter*
- Approval (TC) or decline (AAC) of the transaction.

2.5.2.2.2 Issuer Authentication Data Verification Fails

If the Issuer Authentication Data verification fails, it indicates that the issuer decision cannot be trusted. This should be an extremely rare occurrence. In such an event, the M/Chip 4 application performs the following:

Dec 2004

- Declines the transaction
- Computes an AAC
- Tracks the critical event and may modify the Card Risk Management of the next transactions (for instance, the M/Chip 4 application may go online on the next transaction so that you are informed of the verification failure).

2.5.2.3 Issuer Authentication Data Not Present

If the transaction goes online when there is no *Issuer Authentication Data* present, this can indicate that the issuer is a magstripe grade issuer (or uses the chip to magstripe conversion service) or that the acquirer is partial grade.

The M/Chip 4 application does not require specific settings for partial grade acquirers. Even following a rejection of the transaction by the card, the terminal will eventually override the card decision with your decision.

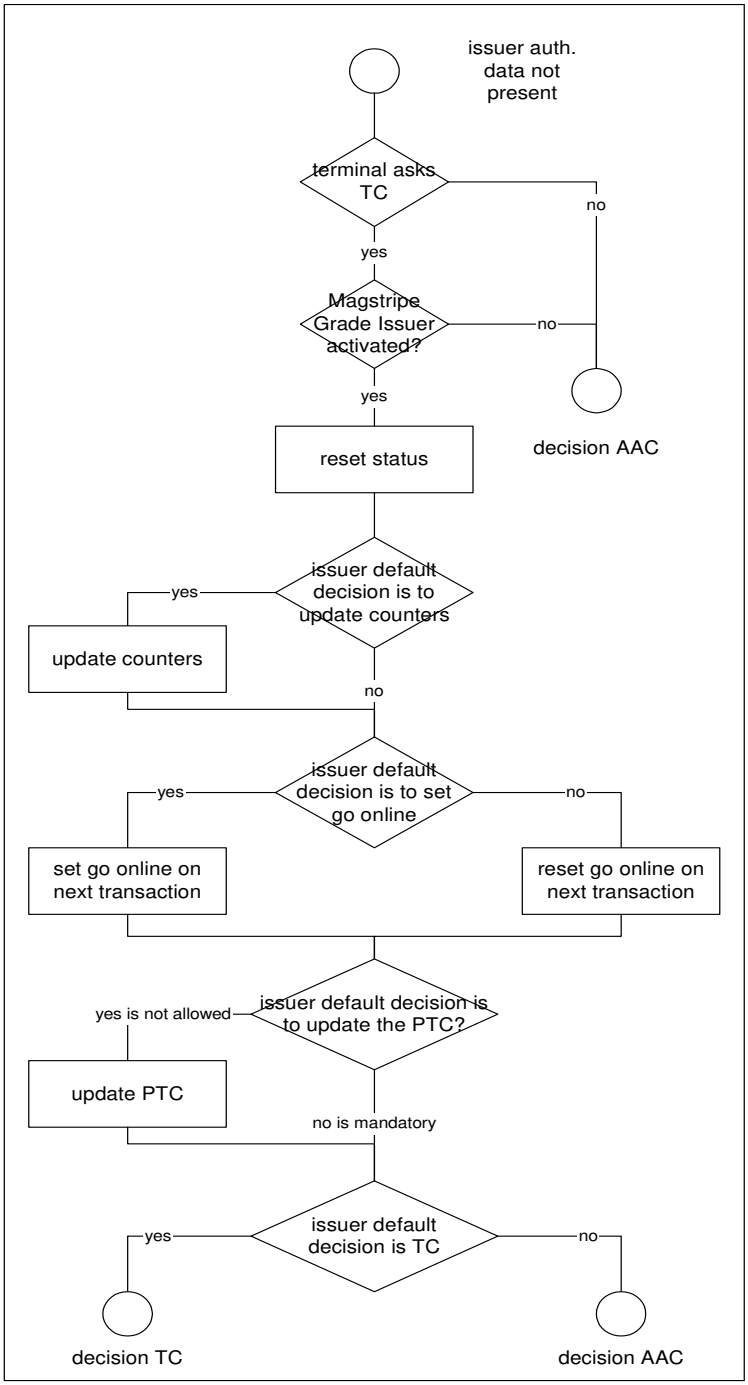
If the acquirer is full grade but there is no *Issuer Authentication Data* present, the transaction can still be performed in the magstripe grade issuer mode.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 62

Figure 2.10 illustrates the Card Risk Management.

Figure 2.10—Card Risk Management when Issuer Authentication Data Not Present



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 63

When there is no *Issuer Authentication Data*, the M/Chip 4 application first verifies that the terminal wishes the transaction to be accepted and that you support the magstripe grade issuer mode. The magstripe grade issuer mode allows the card to accept transaction when the *Issuer Authentication Data* is not present. You select this at personalization.

If …	Then the M/Chip 4 application …
The M/Chip 4 application does not support the magstripe grade issuer mode.	• Declines the transaction. • Computes an AAC.
The terminal requests an AAC.	• Declines the transaction. • Computes an AAC.
The terminal requests a TC **and** the M/Chip 4 application supports the magstripe grade issuer mode	Resets flags and counter: • *Issuer Authentication Failed on Online Transaction Flag* • *Script Received on Online Transaction Flag* • *Script Failed on Online Transaction Flag* **and** • *Number Of Issuer Script Commands Received on Last Online Transaction* Performs default actions as defined at personalization: • Update of the offline counters • Set/reset of the *Go Online on Next Transaction Flag* • Approval (TC) of transaction or decline (AAC) of transaction



Note **If the acquirer is partial grade but the issuer is full grade, the transaction would be rejected by the card. However, the partial grade terminal will override the issuer decision. Such a transaction has no impact on the M/Chip 4 application status and therefore no impact on the Card Risk Management of the transactions that follow.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 64

3 Configuring the M/Chip 4 Application

This chapter describes the features of the M/Chip 4 application that you configure to define the application behavior.

3.1 Overview 3-1

3.2 Configuring the Application Control Data Element 3-1
3.2.1 Application Control Coding 3-1
3.2.2 Application Control Usage 3-4
3.2.2.1 Magstripe Grade Issuer Activated 3-4
3.2.2.2 Skip CIAC – Default on CAT3 3-4
3.2.2.3 Key for Offline Encrypted PIN Verification 3-4
3.2.2.4 Offline Encrypted PIN Verification 3-5
3.2.2.5 Offline Plaintext PIN Verification 3-5
3.2.2.6 Session Key Derivation 3-6
3.2.2.7 Encrypt Offline Counters 3-6
3.2.2.8 Activate Additional Check Table 3-7
3.2.2.9 Allow Balance Retrieval 3-7
3.2.2.10 Include Counters in AC 3-7

3.3 Configuring Card Risk Management Data Elements 3-8
3.3.1 Card Issuer Action Codes 3-8
3.3.2 CRM Country Code 3-8
3.3.3 CRM Currency Code 3-9
3.3.4 Lower Cumulative Offline Transaction Amount 3-9
3.3.5 Upper Cumulative Offline Transaction Amount 3-9
3.3.6 Lower Consecutive Offline Limit 3-10
3.3.7 Upper Consecutive Offline Limit 3-10
3.3.8 Currency Conversion Table and Currency Conversion Parameters 3-10
3.3.9 Default ARPC Response Code 3-11
3.3.10 Additional Check Table 3-12
3.3.11 CDOL 1 and CDOL 2 Related Data 3-12
3.3.12 Offline PIN, PIN Try Counter and PIN Try Limit 3-13
3.3.13 Previous Transaction History 3-13
3.3.14 Application Control 3-13

3.4 Selecting Cryptographic Features 3-14

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 65

3.4.1 Session Key Derivation 3-14
3.4.1.1 Additional Personalization for EMV 2000 Session Key Derivation 3-15
3.4.1.2 Switching between Session Key Derivation Methods 3-15
3.4.2 Key for Offline Encrypted PIN 3-15
3.4.2.1 RSA Key = DDA Key 3-16
3.4.2.2 RSA Key = Dedicated PIN Encryption Key 3-16
3.4.3 Offline Counters Encryption 3-17
3.4.4 Offline Counters inclusion in AC 3-17
3.4.5 Cryptogram Version Number 3-18

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 66

3.1 Overview

You can customize your M/Chip 4 application in the following ways:

- By defining the settings of the Application Control data element
- By defining the settings of the Card Risk Management data elements
- By selecting specific cryptographic features

The following sections describe each of the selections available to you.

3.2 Configuring the Application Control Data Element

The *Application Control* is an internal data element that activates or deactivates several features of the M/Chip 4 applications. You activate the required features at personalization or change the features using script command during the card life.

The following sections describe the coding and usage of each byte of the *Application Control* data element.

3.2.1 Application Control Coding

The following tables describe the coding of each byte of the *Application Control* data element.

Table 3.1 describes the coding of byte 1 of the *Application Control* for the M/Chip Select 4 application.

Table 3.1—Application Control for M/Chip Select 4, Byte 1

b8	b7	b6	B5	b4	b3	b2	b1	Meaning
x								**Magstripe grade issuer activated**
0								Magstripe grade issuer not activated
1								Magstripe grade issuer activated
	x							**Skip CIAC-default on CAT3**
	0							Do not skip CIAC-default on CAT3
	1							Skip CIAC-default on CAT3
		x						**Reserved**
		0						Other value RFU

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 67

b8	b7	b6	B5	b4	b3	b2	b1	Meaning
			x					**Key for offline encrypted PIN verification**
			0					DDA key
			1					Dedicated key
				x				**Offline encrypted PIN verification**
				0				Not supported
				1				Supported
					x			**Offline plaintext PIN verification**
					0			Not supported
					1			Supported
						x		**Session key derivation**
						0		EPI/MCI
						1		EMV 2000
							x	**Encrypt offline counters**
							0	Do not encrypt offline counters
							1	Encrypt offline counters

Table 3.2 describes the coding for byte 1 of the *Application Control* for the M/Chip Lite 4 application.

Table 3.2—Application Control for M/Chip Lite 4, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								**Magstripe grade issuer activated**
0								Magstripe grade issuer not activated
1								Magstripe grade issuer activated
	x							**Skip CIAC-default on CAT3**
	0							Do not skip CIAC-default on CAT3
	1							Skip CIAC-default on CAT3
		x						**Reserved**
		0						Other value RFU
			x					**Reserved**
			0					Other value RFU

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 68

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
				x				**Reserved**
				0				Other value RFU
					x			**Offline plaintext PIN verification**
					0			Not supported
					1			Supported
						x		**Session key derivation**
						0		EPI/MCI
						1		EMV 2000
							x	**Encrypt offline counters**
							0	Do not encrypt offline counters
							1	Encrypt offline counters

Table 3.3 describes the coding for byte 2 of the *Application Control* for both the M/Chip 4 applications.

Table 3.3—Application Control for M/Chip 4 Applications, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x				**Reserved**
0	0	0	0	0				Other value RFU
					x			**Activate additional check table**
					0			Do not activate additional check table
					1			Activate additional check table
						x		**Allow retrieval of balance**
						0		Do not allow retrieval of balance
						1		Allow retrieval of balance
							x	**Include counters in AC**
							0	Do not include counters in AC
							1	Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 69

3.2.2 Application Control Usage

The following sections describe the usage of the *Application Control* data element.

3.2.2.1 Magstripe Grade Issuer Activated

The M/Chip 4 applications check the Magstripe Grade Issuer Activated bit during the second **GENERATE AC** when the *Issuer Authentication Data* is not present.

If the Magstripe Grade Issuer Activated bit set to '1', it allows the card to accept the transaction when the *Issuer Authentication Data* is not present.

The Magstripe Grade Issuer Activated must be set:

- When the chip to magstripe service is used
- When the authorization system does not use cryptography (Magstripe grade issuer mode)

3.2.2.2 Skip CIAC – Default on CAT3

The application checks the Skip CIAC – Default on CAT3 bit in the first **GENERATE AC**, when the terminal is a CAT level 3 terminal.

If …	Then the M/Chip 4 application….
Skip CIAC – Default on CAT3 bit = '1b'	Skips the check on the *Card Issuer Action Code – Default* in the first **GENERATE AC** on a CAT level 3 terminal. This allows the M/Chip 4 applications to approve low-value transactions when offline limits are exceeded.
Skip CIAC – Default on CAT3 bit = '0b'	Check the *Card Issuer Action Code – Default* in the first **GENERATE AC** on a CAT level 3 terminal. The M/Chip 4 applications treat CAT level 3 terminals in the same way as other offline-only terminals.

Note **This only applies to MasterCard credit transactions.**

3.2.2.3 Key for Offline Encrypted PIN Verification

The M/Chip Select 4 application checks the Key for Offline Encrypted PIN Verification bit during the **VERIFY**, when offline encrypted PIN verification is performed.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 70

If …	Then the M/Chip 4 Select application….
Key for Offline Encrypted PIN Verification bit = ‘1b’	Uses a dedicated PIN Encryption key for offline encrypted PIN decryption.
Key for Offline Encrypted PIN Verification bit = ‘0b’	Uses the DDA key for offline encrypted PIN decryption. The advantage of using the DDA key for encrypted PIN is that personalization can be simplified and transaction time is shorter.

Note **The M/Chip Lite 4 application does not use this bit. In an M/Chip Lite 4 implementation, the Key for Offline Encrypted PIN Verification bit must therefore be set to '0b'.**

3.2.2.4 Offline Encrypted PIN Verification

The M/Chip Select 4 application checks the Offline Encrypted PIN Verification bit during the **`VERIFY`**, when offline encrypted PIN verification is performed. By selecting to check this bit, you enjoy the advantage of greater protection against attack but also the disadvantage of a longer transaction time.

If …	Then the M/Chip 4 Select application….
Offline Encrypted PIN Verification bit = ‘1b’	Supports the offline encrypted PIN.
Offline Encrypted PIN Verification bit = ‘0b’	Does not support the offline encrypted PIN.

Note **The M/Chip Lite 4 application does not use this bit. In an M/Chip Lite 4 implementation, the Offline Encrypted PIN Verification bit must therefore be set to '0b'.**

3.2.2.5 Offline Plaintext PIN Verification

The M/Chip application checks the Offline Plaintext PIN Verification bit during the **`VERIFY`**, when offline plaintext PIN verification is performed.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 71

If …	Then the M/Chip 4 application….
Offline Plaintext PIN Verification bit = '1b'	Supports offline plaintext PIN.
Offline Plaintext PIN Verification bit = '0b'	Does not support offline plaintext PIN.

3.2.2.6 Session Key Derivation

The M/Chip 4 application checks the Session Key Derivation bit whenever a session key is derived. The M/Chip 4 application also checks the Session Key Derivation bit during the first and second **GENERATE AC** to construct the value of the *Cryptogram Version Number* in the *Issuer Application Data*.

If …	Then the M/Chip 4 application….
Session Key Derivation bit = '1b'	Uses the session key derivation method as specified in EMV 2000.
Session Key Derivation bit = '0b'	Uses the EPI/MCI session key derivation method. **This is the method already used by the M/Chip Select 2 and M/Chip Lite 2.1 applications.**

3.2.2.7 Encrypt Offline Counters

The M/Chip 4 application uses the Encrypt Offline Counters bit to decide whether the offline counters are sent in clear or encrypted in the *Issuer Application Data*.

By selecting to encrypt the offline counters, you enjoy the advantage of protecting data deemed private. The disadvantage of encryption is that your authorization system has to decrypt the counters before using them. However, your authorization system can perform verification of the ARQC without decrypting the offline counters.

If …	Then the M/Chip 4 application….
Encrypt Offline Counters bit = '1b'	Sends the offline counters encrypted in the *Issuer Application Data*.
Encrypt Offline Counters bit = '0b'	Sends the offline counters in clear in the *Issuer Application Data*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 72

3.2.2.8 Activate Additional Check Table

The M/Chip 4 application checks the Activate Additional Check Table bit during the processing of the first **GENERATE AC** to control the activation of the optional Card Risk Management check on the *Additional Check Table*.

If …	Then the M/Chip 4 application….
Activate Additional Check Table bit = '1b'	Checks the *Additional Check Table* and performs the additional test as defined.
Activate Additional Check Table bit = '0b'	Does not check the *Additional Check Table*.

3.2.2.9 Allow Balance Retrieval

The M/Chip 4 application checks the Allow Balance Retrieval bit during the **GET DATA** processing to control retrieval of the *Offline Balance*.

If …	Then the M/Chip 4 application….
Allow Balance Retrieval bit = '1b'	Can access the *Offline Balance* with the **GET DATA** command.
Allow Balance Retrieval bit = '0b'	Cannot access the *Offline Balance* with the **GET DATA** command.

3.2.2.10 Include Counters in AC

The M/Chip 4 application checks the Include Counters in AC bit during the first and second **GENERATE AC** to construct:

- The input to the AC computation
- The value of the *Cryptogram Version Number* in the *Issuer Application Data*

If …	Then the M/Chip 4 application….
Include Counters in AC bit = '1b'	Includes the offline counters as part of the input to the AC.
Include Counters in AC bit = '0b'	Does not include the offline counters as part of the input to the AC.

If you choose to include the offline counters in the AC computation, the counters cannot be altered.

If you are migrating from M/Chip Select 2 and M/Chip Lite 2.1, MasterCard recommends that you exclude the counters.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 73

Note **If the offline counters are sent encrypted in the *Issuer Application Data*, the counters input to the AC computation are also encrypted.**

3.3 Configuring Card Risk Management Data Elements

There are three types of data elements that impact Card Risk Management for a transaction:

- Data elements set at personalization
- Data elements linked to the current transaction
- Data elements linked to the previous transactions

This section briefly describes the impact of each data element on Card Risk Management.

3.3.1 Card Issuer Action Codes

The *Card Issuer Action Codes* are data elements that allow you to specify the conditions that determine:

- Whether the M/Chip 4 application declines or approves a transaction offline
- Whether the M/Chip 4 application sends the transaction online when the transaction is performed at an online-capable terminal (e.g. when the offline limits are exceeded).

Refer to the "Card Issuer Actions Codes" section in chapter 2 for further details.

3.3.2 CRM Country Code

The *CRM Country Code* contains the country specified by the issuer. The M/Chip 4 applications use the *CRM Country Code* internal data element to differentiate between domestic and international transactions as follows:

- If the *CRM Country Code* matches the *Terminal Country Code*, the transaction is domestic.
- If the *CRM Country Code* does not match the *Terminal Country Code*, the transaction is international.

An action (decline or go online) can be triggered based on the *Card Issuer Action Code* settings for the 'International transaction' or 'Domestic transaction' bits.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 74

3.3.3 CRM Currency Code

The *CRM Currency Code* is an internal data element containing the currency of the *Cumulative Offline Transaction Amount.* The M/Chip 4 application uses the *CRM Currency Code* and the *Currency Conversion Table* to determine which of the two offline counters, the *Cumulative Offline Transaction Amount* and the *Cumulative Offline Transaction Number*, to increment.

An action (decline or go online) can be triggered based on the *Card Issuer Action Code* settings if the offline counters (*Cumulative Offline Transaction Amount* and *Cumulative Offline Transaction Number*) exceed the limits.

3.3.4 Lower Cumulative Offline Transaction Amount

The *Lower Cumulative Offline Transaction Amount* is an internal data element that specifies the lower value used to check against the *Cumulative Offline Transaction Amount* in either of the following situations:

- The transaction is in the counter currency.
- The M/Chip 4 application can convert the transaction into the counter currency.

An action (decline or go online) can be triggered based on the *Card Issuer Action Code* settings of the 'Lower Cumulative Offline Limit exceeded' bit.

3.3.5 Upper Cumulative Offline Transaction Amount

The *Upper Cumulative Offline Transaction Amount* is an internal data element that specifies the upper value used to check against the *Cumulative Offline Transaction Amount* in either of the following situations:

- The transaction is in the counter currency.
- The M/Chip 4 application can convert the transaction into the counter currency.

An action (decline or go online) can be triggered based on the *Card Issuer Action Code* settings of the 'Upper Cumulative Offline Limit exceeded'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 75

3.3.6 Lower Consecutive Offline Limit

The *Lower Consecutive Offline Limit* is an internal data element that specifies the lower limit that is used to check against the *Consecutive Offline Transactions Number* in either of the following situations:

- The transaction is not in the counter currency.
- The M/Chip 4 application cannot convert the transaction into the counter currency.

An action (decline or go online) can be triggered based on the Card Issuer Action Code settings of the 'Lower Consecutive Offline Limit exceeded'.

3.3.7 Upper Consecutive Offline Limit

The *Upper Consecutive Offline Limit* is an internal data element that specifies the upper limit that is used to check against the *Consecutive Offline Transactions Number* in either of the following situations:

- The transaction is not in the counter currency.
- The M/Chip 4 application cannot convert the transaction into the counter currency.

An action (decline or go online) can be triggered based on the Card Issuer Action Code settings of the 'Upper Consecutive Offline Limit exceeded'.

3.3.8 Currency Conversion Table and Currency Conversion Parameters

The *Currency Conversion Table* is an internal data element that you define.

If the *Currency Conversion Table* contains the transaction currency, the M/Chip 4 application converts the transaction amount, using the *Currency Conversion Parameters*, and adds the transaction value to the *Cumulative Offline Transaction Amount*.

If the *Currency Conversion Table* does not contain the transaction currency and the transaction currency is not the currency of the *Cumulative Offline Transaction Amount* (i.e. the currency of the *CRM Currency Code*), the M/Chip 4 application does not convert the transaction value. Instead, it counts the transaction by incrementing the *Cumulative Offline Transaction Number*.

To ensure the accuracy of the *Cumulative Offline Transaction Amount*, you should avoid currencies with a highly volatile conversion rate against the *Counter Currency*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 76

3.3.9 Default ARPC Response Code

The *Default ARPC Response Code* is an internal data element that you define during personalization. It allows you to customize the application behavior when there is no *Issuer Authentication Data* for an online transaction.

The setting of the *Default ARPC Response Code* is only active if the magstripe grade issuer mode is supported (in the *Application Control*). The *Default ARPC Response Code* replaces the *ARPC Response Code* when **all** of the following conditions are met:

- The *Issuer Authentication Data* is not present in an online transaction.
- The magstripe grade issuer mode is activated (i.e. *Application Control* [1][8] is set to '1b').
- The transaction is approved by the terminal and issuer which means:
  - The Authorization Response Code is neither 'Y3' ("Unable to go online—Offline approved" response code generated by the terminal at second **`GENERATE AC`**) nor 'Z3' ("Unable to go online—Offline declined" response code generated) and
  - The terminal requests a TC.

Table 3.4 provides the values that you must use for the personalization of the *Default ARPC Response Code*.

Table 3.4—Mandatory Values for Default ARPC Response Code

Bit	Meaning	Value
Byte 1		
8-5	Reserved	'0000b' mandatory
4-1	PIN Try Counter	'0000b' mandatory
Byte 2		
8-6	Reserved	'000b' mandatory
5	Approve online transaction	'1b' mandatory
4	Update PIN Try Counter	'0b' mandatory
3	Set go online on next transaction	'0b' recommended
2-1	Update counters – reset counters to zero	'10b' mandatory

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 77

3.3.10 Additional Check Table

The *Additional Check Table* is an internal data element that you define during personalization.

The M/Chip 4 application compares the values in the *Additional Check Table* with the values given by the terminal in *CDOL 1 Related Data*. The M/Chip 4 application reflects the result of this comparison in the decision-making information part of the *Card Verification Results*.

The M/Chip 4 application only checks the *Additional Check Table* when the *Application Control* [2][3] is set to '1b'.

3.3.11 CDOL 1 and CDOL 2 Related Data

Transaction-related data is communicated to the application via the *CDOL 1 Related Data* and *CDOL 2 Related Data* data elements. Table 3.5 identifies this data and briefly describes the role it plays in Card Risk Management.

Table 3.5—Role of CDOL-Related Data in Card Risk Management

Data element	Role in Card Risk Management
Amount, Authorised and *Transaction Currency Code*	Used to determine if the offline counters would exceed the limits.
Terminal Country Code	Used to determine if the transaction is domestic or international.
Terminal Type	Used to determine if the terminal is offline only and if it is CAT level 3.
CVM Results	Used to check that the terminal is not misled about the offline PIN verification.
Issuer Authentication Data	Used to determine the actions that you decided upon in an online transaction.
Authorization Response Code	Used to determine the action decided by the terminal in an online transaction or if the terminal cannot go online.

If the M/Chip 4 application also uses the *Additional Check Table*, other information from *CDOL 1 Related Data* may also influence the Card Risk Management.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 78

3.3.12 Offline PIN, PIN Try Counter and PIN Try Limit

The *PIN Try Counter* is an internal counter that counts the number of offline PIN tries remaining. Whenever the correct PIN is entered, the *PIN Try Counter* is reset to the *PIN Try Limit*.

You can customize the M/Chip 4 applications as follows:

- To support offline PIN
- To set the PIN Try Limit
- To trigger an action (decline or go online) in the following situations:
  - When offline PIN verification is not performed
  - When the offline PIN verification performed is incorrect
  - When there are no PIN tries remaining

3.3.13 Previous Transaction History

The *Previous Transaction History* data element keeps track of events that occurred in previous transactions. You reset the *Previous Transaction History* in an online transaction.

The following events related to a previous online transaction are kept in the *Previous Transaction History*:

- You decided that the next transaction should go online.
- The issuer authentication failed.
- A script command was processed.
- A script command failed.

You can customize the M/Chip 4 application to trigger a specific action (e.g. go online) if one of the above events took place.

3.3.14 Application Control

The *Application Control* enables you to:

- Activate or inactivate the magstripe grade issuer mode.
- Allow the application to skip or not to skip the CIAC – Default check on the CAT level 3 terminals.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 79

3.4 Selecting Cryptographic Features

The M/Chip 4 applications support the following:

- EPI/MCI session key derivation or EMV 2000 session key derivation
- Encrypted or "in clear" offline counters in the *Issuer Application Data*
- Optional inclusion of offline counters in the input to the AC generation

In addition, the M/Chip Select 4 application offers the following options:

- Selection of the length of the RSA keys
- DDA key or a dedicated PIN encryption key as key for offline encrypted PIN

The following sections describe each of these options.

3.4.1 Session Key Derivation

The M/Chip 4 applications support two different session key derivation methods:

- EPI/MCI session key derivation used in the M/Chip Select 2 or M/Chip Lite 2.1
- Session key derivation as defined in EMV 2000

Only one session key method can be active at any one time. The active session key method is specified in the *Application Control* [1][2].

If Application Control …	Then the M/Chip 4 application….
Session Key Derivation bit = '1b'	Uses the session key derivation method as specified in EMV 2000.
Session Key Derivation bit = '0b'	Uses the EPI/MCI session key derivation method. **This is the method already used by the M/Chip Select 2 and M/Chip Lite 2.1 applications.**

Independently of the profile and session key derivation method, you must also personalize the symmetric master keys in Table 3.6 in the card application.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 80

Table 3.6—3-DES Master Keys for Session Key Derivation

Data Element	Length
SM for Integrity Master Key (MK_{SMI})	16
SM for Confidentiality Master Key (MK_{SMC})	16
AC Master Key (MK_{AC})	16

3.4.1.1 Additional Personalization for EMV 2000 Session Key Derivation

If you select the EMV 2000 session key derivation method, you must personalize data elements as described in Table 3.7 in addition to those data elements described in Table 3.6.

Table 3.7—Additional Personalization Data for EMV 2000 Session Key Derivation

Data Element	Length	Value
CFDC_limit for Integrity Session Key	1	Refer to related publications. [a] [b]
CFDC_limit for Confidentiality Session Key	1	Refer to related publications. [a] [b]
CFDC_limit for AC Session Key	1	Refer to related publications. [a] [b]

[a] *M/Chip 4 Card Application Specifications for Debit and Credit.*

[b] *M/Chip 4 Security and Key Management.*

3.4.1.2 Switching between Session Key Derivation Methods

It is possible to switch from EPI/MCI to EMV 2000 session key derivation, or less likely from the EMV 2000 to the EPI/MCI session key derivation, by changing the value of the *Application Control* data element. In order to allow for switching from EPI/MCI to EMV 2000 session key derivation, you must also personalize the data elements in Table 3.7.

3.4.2 Key for Offline Encrypted PIN

You configure the M/Chip Select 4 application to support offline encrypted PIN verification by setting the *Application Control* [1][4] to '1b'.

EMV specifies two different ways to protect the offline PIN during transport between the terminal and the ICC:

- By encrypting the PIN block with the DDA key

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 81

- By encrypting the PIN block with a dedicated PIN encryption key.

The *Application Control* data element specifies the active encryption method.

3.4.2.1 RSA Key = DDA Key

When the RSA Key is implemented as the DDA Key:

- The *CVM List* must specify that offline encrypted PIN verification is supported
- The *Application Control* [1][5] must be set to '0b'
- You must personalize the *ICC Private Key*
- The data in Table 3.8 must be contained in the records referred to in the *Application File Locator*.

Table 3.8—Records Content for Offline Encrypted PIN with the DDA Key

Tag	Data Element
'8F'	*Certification Authority Public Key Index*
'9F32'	*Issuer Public Key Exponent*
'92'	*Issuer Public Key Remainder*
'90'	*Issuer Public Key Certificate*
'9F47'	*ICC Public Key Exponent*
'9F48'	*ICC Public Key Remainder*
'9F46'	*ICC Public Key Certificate*

3.4.2.2 RSA Key = Dedicated PIN Encryption Key

When the RSA key is a dedicated PIN encryption key:

- The *CVM List* must specify that offline encrypted PIN verification is supported.
- The *Application Control* [1][5] must be set to '1b'.
- You must personalize the *ICC PIN Encipherment Private Key*.
- The records referred to in the *Application File Locator* must contain the data in Table 3.9.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 82

Table 3.9—Records Content for Offline Encrypted PIN with a Dedicated Key

Tag	Data Element
'8F'	*Certification Authority Public Key Index*
'9F32'	*Issuer Public Key Exponent*
'92'	*Issuer Public Key Remainder*
'90'	*Issuer Public Key Certificate*
'9F2F'	*ICC PIN Encipherment Public Key Exponent*
'9F2E'	*ICC PIN Encipherment Public Key Remainder*
'9F2D'	*ICC PIN Encipherment Public Key Certificate*

3.4.3 Offline Counters Encryption

You configure the M/Chip 4 application to support the encryption of offline counters encryption by setting the *Application Control* [1][1] to '1b'.



Note **It is possible to switch from the encrypted counters to plaintext counters, or from plaintext counters to encrypted counters, by changing the value of the *Application Control*.**

3.4.4 Offline Counters inclusion in AC

You configure the M/Chip 4 application to include the offline counters in the input to the Application Cryptogram by setting the *Application Control* [2][1] to '1b'.

When counters are also encrypted, it is the encrypted form that is included in the Application Cryptogram. This allows the verification of the AC without first having to decrypt the counters.



Note **It is possible to switch from an input to the cryptogram including the counters to an input without counters or from an input without counters to an input with counters, by changing the value of the *Application Control*.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 83

3.4.5 Cryptogram Version Number

The *Cryptogram Version Number* reflects the choice of cryptographic features that you made. You can modify your selection of cryptographic features after personalization. The M/Chip 4 applications will automatically update the value of the *Cryptogram Version Number* to reflect the activated cryptographic features.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 84

4 Issuer Host Processing of Transactions

This chapter describes the processing performed by your host as part of online authorization and clearing. It also describes the conditions when the application status is updated.

4.1 Online Authorization 4-1
4.1.1 Verifying the ARQC 4-1
4.1.2 Interpreting the Issuer Application Data 4-1
4.1.2.1 Key Derivation Index 4-2
4.1.2.2 Cryptogram Version Number 4-2
4.1.2.3 Card Verification Results 4-3
4.1.2.4 DAC/ICC Dynamic Number 2 Bytes 4-4
4.1.2.5 Encrypted Counters 4-4
4.1.3 Making The Decision 4-5
4.1.4 Building The Issuer Authentication Data 4-5
4.1.4.1 Authorization Response Cryptogram 4-6
4.1.4.2 ARPC Response Code 4-7
4.1.4.2.1 Approve Online Transaction 4-8
4.1.4.2.2 Update PIN Try Counter 4-8
4.1.4.2.3 Set Go Online on Next Transaction 4-8
4.1.4.2.4 Update Counters 4-9
4.1.5 Script Processing 4-9
4.1.6 Issuer Referral 4-10

4.2 Clearing 4-11
4.2.1 Check that Transactions Were Approved Online 4-11
4.2.2 Potential De-synchronization between AC and Terminal Verification Results 4-11

4.3 Update of Application Status 4-13
4.3.1 Reset of Script Counter 4-13
4.3.2 Setting of "Go Online on Next Transaction" Bit 4-13
4.3.3 Setting of "Issuer Authentication Failed," "Script Received", "Script Failed" Bits 4-14
4.3.4 Update of Offline Counters 4-14

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 85

4.1 Online Authorization

When an online authorization is requested during a transaction, the M/Chip 4 application generates an Authorization Request Cryptogram (ARQC). Full grade acquirers (i.e. the acquirer supports the transfer of the ICC System Related Data (DE 55) data element) send you the ARQC in the authorization request message along with the transaction data.

4.1.1 Verifying the ARQC

Full grade issuers can authenticate the M/Chip 4 application dynamically through the ARQC. Refer to the *M/Chip 4 Security and Key Management* manual for details of cryptogram validation.

You may use the following steps to perform ARQC verification:

1. Verify that the card computed an ARQC in the *Card Verification Results* [1][8-5] = '1010b'.
2. Determine the session key derivation from the *Cryptogram Version Number*.
3. Determine the issuer master key to use from the *Key Derivation Index*.
4. Determine the input to the cryptogram from the *Cryptogram Version Number*.
5. Build the input to the cryptogram using the chip data. Verify the cryptogram.

Magstripe grade issuers do not verify the ARQC on the issuer authorization host.

4.1.2 Interpreting the Issuer Application Data

The *Issuer Application Data* informs you about:

- The Application Cryptogram calculation (including key derivation index, type of cryptogram and the algorithm used)
- Whether offline PIN verification was performed for the transaction, and if so, whether it was successful
- The PIN Try counter
- The number of scripts sent in the previous transaction
- In the event that a script was sent in the previous transaction, whether the script was correctly transmitted to the application and successfully executed

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 86

- The number of offline chip transactions performed and the cumulated offline amount since the previous online chip transaction
- The reason the transaction was sent online for authorization
- Whether the terminal performed the offline Card Authentication Method

Table 4.1 identifies M/Chip 4 application data elements concatenated (without TLV coding) in the *Issuer Application Data*. The following sections provide a brief description of each of these data elements.

Table 4.1—Issuer Application Data for the M/Chip 4 Application

Data Element	Length
Key Derivation Index	1
Cryptogram Version Number	1
Card Verification Results	6
DAC/ICC Dynamic Number 2 Bytes	2
Plaintext/Encrypted Counters	8

The following five sections describe the contents of the *Issuer Application Data* in more detail.

4.1.2.1 Key Derivation Index

The *Key Derivation Index* is issuer-specific. It may identify the key you use to derive the session key.

4.1.2.2 Cryptogram Version Number

The M/Chip 4 application manages the *Cryptogram Version Number*. This data element informs you about the algorithm and data used for the *Application Cryptogram* computation. The value depends on the activated session key derivation method (EMV 2000 OR EPI/MCI) and on the data included in the MAC (whether or not offline counters are included).

Table 4.2 describes the values the M/Chip 4 application uses for the *Cryptogram Version Number*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 87

Table 4.2—Cryptogram Version Number

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					**Cryptogram version**
0	0	0	1					**4, other values RFU**
				x	x			**Reserved**
				0	0			**Other value RFU**
						x		**Session key used for AC computation**
						0		EPI/MCI session key
						1		EMV2000 session key
							x	**Counters included in AC computation**
							0	Counters not included in AC data
							1	Counters included in AC data

4.1.2.3 Card Verification Results

During online authorization, the *Card Verification Results* informs you about the "context" of an online transaction as follows:

- if 'AC was not requested' in second **GENERATE AC**
- if an ARQC was returned in the first **GENERATE AC**
- if offline PIN verification or Offline Encrypted PIN verification was performed
- if offline PIN verification was performed successfully
- if DDA was returned (only for M/Chip Select 4)
- if combined DDA/AC was returned in the first **GENERATE AC** (only for M/Chip Select 4)
- if combined DDA/AC was not returned in the second **GENERATE AC** (only for M/Chip Select 4)
- information about the script counter and the PIN Try Counter
- if the PIN Try Limit was exceeded
- the transaction type (international or domestic)
- if the terminal erroneously considers offline PIN was OK
- if the lower, upper consecutive or cumulative offline limits were exceeded
- if 'Go online on next transaction' was set

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 88

- if an issuer script was received and whether it passed or failed in the previous transaction
- if issuer authentication failed in the previous online transaction
- if a match was found in the additional check table

4.1.2.4 DAC/ICC Dynamic Number 2 Bytes

For each of the M/Chip Select 4 and M/Chip Lite 4 applications, this data element contains:

If	DAC/ICC Dynamic Number 2 Bytes contains...	
	M/Chip Select 4	**M/Chip Lite 4**
The terminal performed the DDA or CDA successfully.	Two left-most bytes of the *ICC Dynamic Number*	N/A
The terminal performed the SDA successfully.	DAC	DAC
The terminal did not perform SDA, DDA, or CDA successfully.	'0000'	0000'

4.1.2.5 Encrypted Counters

This data element contains the offline counters, in clear or encrypted:

- *Cumulative Offline Transaction Amount*
- *Consecutive Offline Transactions Number*

If the counters are sent in clear (*Application Control* [1][1] is set to '0b' [Do not encrypt offline counters]), this data element is the concatenation of the *Cumulative Offline Transaction Amount*, the *Consecutive Offline Transactions Number* and 'FF'.

If the counters are sent encrypted (*Application Control* [1][1] is set to '1b' [Encrypt offline counters]), this data element contains the encrypted counters (eight bytes). Refer to the *M/Chip 4 Security and Key Management* manual for details.

The *Cryptogram Version Number* [1] value of '1b' indicates that the counters are included in the *Application Cryptogram* data.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 89

4.1.3 Making The Decision

You make the decision whether to approve or decline a transaction based on the *Issuer Application Data* received. You may use any of the following information to make your decision:

- The ARQC verification result
- The offline PIN verification result or whether the PTL was exceeded
- The online PIN verification result or whether the PTL was exceeded
- Offline spending (offline counters)
- Transaction value and money available in the account
- Transaction type (international or domestic)
- If the terminal approved the offline PIN in error
- When the Additional Check Table feature is used, whether a match was found

Full grade issuers may decide to change the M/Chip 4 application behavior by using the *ARPC Response Code* to instruct the application to:

- respond with TC or AAC
- reset the Card Risk Management counters
- go online at the next transaction
- update the PIN Try Counter to synchronize the PIN Try Counter on the card and on your online host

Magstripe grade issuers, where the magstripe grade issuer mode is activated, handle online transaction without *Issuer Authentication Data* differently and use the *Default ARPC Response Code* to instruct the application to determine the next actions. Refer to section "Supporting the Magstripe Grade Issuer" in chapter 5 for more detail.

4.1.4 Building The Issuer Authentication Data

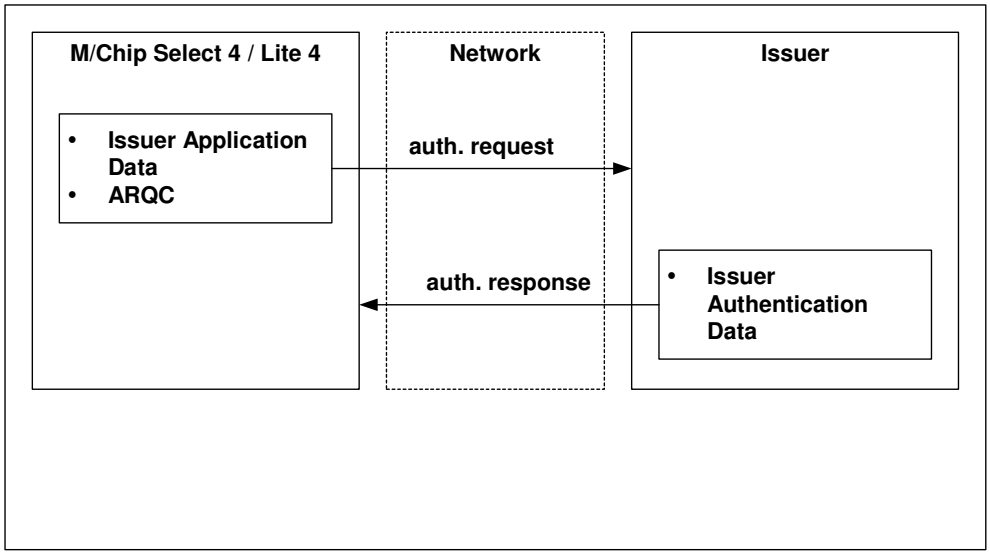
Once you have taken your decision, your host generates the *Issuer Authentication Data*. The full grade chip issuer generates the *Issuer Authentication Data* for the authorization response to the terminal. The terminal transfers the *Issuer Authentication Data* to the M/Chip 4 application, which uses it to authenticate the issuer.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 90

Figure 4.1 illustrates your transfer of the *Issuer Authentication Data* information to the M/Chip 4 application in the Authorization Response message.

Figure 4.1—Issuer Authentication Data Transaction



The *Issuer Authentication Data* contains two data elements:

- *Authorization Response Cryptogram (ARPC)*
- *ARPC Response Code*

The following sections describe each of these data elements.

4.1.4.1 Authorization Response Cryptogram

You compute the *Authorization Response Cryptogram*. Refer to the *M/Chip 4 Security and Key Management* manual for a detailed specification of this computation.

If the M/Chip 4 application verifies the *Authorization Response Cryptogram* successfully, it resets the following flags and counters:

- *Issuer Authentication Failed on Online Transaction Flag*
- *Script Received on Online Transaction Flag*
- *Script Failed on Online Transaction Flag*
- *Number of Issuer Script Commands Received on Last Online Transaction*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 91

4.1.4.2 ARPC Response Code

The M/Chip 4 application only interprets the *ARPC Response Code* following successful verification of the *Authorization Response Cryptogram*.

Table 4.3 describes the content of byte 1 of the *ARPC Response Code*.

Table 4.3—ARPC Response Code, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Reserved
0	0	0	0					Other value RFU
				x	x	x	x	*PIN Try Counter*

Table 4.4 describes the content of byte 2 of the *ARPC Response Code*.

Table 4.4—ARPC Response Code, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x						Reserved
0	0	0						Other value RFU
			x					Approve online transaction
			0					Do not approve online transaction
			1					Approve online transaction
				x				Update *PIN Try Counter*
				0				Do not update *PIN Try Counter*
				1				Update *PIN Try Counter*
					x			Set go online on next transaction
					0			Reset go online on next transaction
					1			Set go online on next transaction
						x	x	Update counters
						0	0	Do not update offline counters
						1	0	Reset counters to zero
						0	1	Set counters to upper offline limits
						1	1	Add transaction to counter

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 92

The following tables describe how the M/Chip 4 application interprets each of the bits in the *ARPC Response Code* data element.

4.1.4.2.1 Approve Online Transaction

If …	Then the M/Chip 4 application …
Approve Online Transaction is set (i.e. *ARPC Response Code* [2][5] = '1b') **and** the terminal requests a TC.	• Approves the transaction. • Computes a TC.
Approve Online Transaction is not set (i.e. *ARPC Response Code* [2][5] = '0b').	• Declines the transaction. • Computes an AAC.

4.1.4.2.2 Update PIN Try Counter

If …	Then the M/Chip 4 application …
Update PIN Try Counter is set (i.e. *ARPC Response Code* [2][4] = '1b').	Updates the *PIN Try Counter* with the value contained in the *ARPC Response Code* [1][4-1].
Update PIN Try Counter is not set (i.e. *ARPC Response Code* [2][4] = '0b').	Does not interpret the *ARPC Response Code* [1][4-1].

4.1.4.2.3 Set Go Online on Next Transaction

If …	Then the M/Chip 4 application …
Set Go Online on Next Transaction is set (i.e. *ARPC Response Code* [2][3] = '1b').	Forces the next transaction on an online capable terminal to go online (i.e. give an ARQC). It will continue to try to go online on an online capable terminal until connection to the issuer is achieved.
Set Go Online on Next Transaction is not set (i.e. *ARPC Response Code* [2][3] = '0b').	Does not force the next transaction on an online capable terminal to go online (i.e. may accept the next transaction offline at the first **GENERATE AC**).

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 93

4.1.4.2.4 Update Counters

If …	Then the M/Chip 4 application …
Reset Counters to Zero is set (i.e. *ARPC Response Code* [2][2-1] = '10b').	Resets the two offline counters so that it can accept transactions offline, up to the offline limits.
Do Not Update Offline Counters is set (i.e. *ARPC Response Code* [2][2-1] = '00b').	Does not modify the two offline counters.
Set Counters To Upper Offline Limits is set (i.e. *ARPC Response Code* [2][2-1] = '01b')	Sets the two offline counters to the *Upper Consecutive Offline Limit* and the *Upper Cumulative Offline Transaction Amount.*
Add Transaction to Counter is set (i.e. *ARPC Response Code* [2][2-1] = '11b').	Accumulates the transaction: • In the *Cumulative Offline Transaction Amount* if the transaction is in the *Counter Currency* or in a currency the M/Chip 4 application can convert • In the *Consecutive Offline Transactions Number* if the transaction is in a currency that the application does not recognize

4.1.5 Script Processing

The M/Chip 4 application supports non-critical scripts (Tag 72).

You include the script in its online reply and the terminal sends each of the commands listed in the script to the M/Chip 4 application. The M/Chip 4 application processes all these commands after TC generation, with the exception of the **`APPLICATION UNBLOCK`**, which is issued after an AAC generation.

The international network supports scripts up to a maximum length of 128 bytes. In a domestic environment, you may implement scripts up to the length supported by your domestic network.

If the script length exceeds the limit, it may be truncated or dropped. If a script fails, the M/Chip 4 application communicates the result of the script in the *Issuer Application Data* in the online transaction that follows the script message.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 94

You can issue the following script commands during online authorization:

- **APPLICATION BLOCK** to block the application because of Credit Losses, Lost or Stolen cards or cards that were never received
- **APPLICATION UNBLOCK** to unblock a blocked application
- **PIN UNBLOCK** or **PIN CHANGE**
- **PUT DATA** to update the Card Risk Management data elements
- **UPDATE RECORD** to update a record read by the terminal.

The transmission of scripts requires the use of secure messaging.

You may use the **UPDATE RECORD** command during script processing when the command length does not exceed the supported network length, and when you know the file and record structure of the card (you do not receive this information during an online transaction). In other cases, the **UPDATE RECORD** command should be performed in a specific environment. Refer to the "Post Issuance Maintenance" section in chapter 5 for further information. Magstripe grade issuers do not support script processing. However, they can use post issuance maintenance to maintain their cards.

4.1.6 Issuer Referral

The M/Chip 4 application does not support issuer referrals initiated by the card because MasterCard, Maestro and Cirrus terminals do not allow this. However, you may request a referral before approving a transaction by setting the Response Code (DE 39) in the Authorization Response message to '01' (Refer to card issuer). In this case, MasterCard recommends that you provide the ICC System Related Data (DE 55) data element, with the following settings in the ARPC Response Code:

- Approve online transaction
- Do not update PIN Try Counter
- Do not update offline counters.

You can decide to approve or decline the transaction after the referral.

MasterCard takes this approach because some terminals may reject transactions approved by the issuer after a referral if the card does not return a TC.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 95

4.2 Clearing

The following sections help you (or your representative) to interpret the data contained in the ICC System Related Data (DE 55) data element during the clearing process.

4.2.1 Check that Transactions Were Approved Online

You can identify that a transaction was approved online, without needing to consult the transaction history log by checking for the following information in the clearing message:

- The cryptogram is a TC, all the data involved in the cryptogram computation provided by the terminal (amount authorised, amount other, etc), the data provided by the card (ATC, AIP, CVR), the Cryptogram Version Number and the Key Derivation Index.
- The TC verification is successful.
- The *Card Verification Results* [2][5] indicates that issuer authentication has been performed (i.e. *Card Verification Results* [2][5] = '1b').

If an M/Chip 4 application receives *Issuer Authentication Data*, it can only compute a TC when the following are true:

- Issuer authentication was performed.
- You explicitly requested the approval in the *Issuer Authentication Data* (i.e. *ARPC Response Code* [2][5] = '1b' [Approve online transaction]).

4.2.2 Potential De-synchronization between AC and Terminal Verification Results

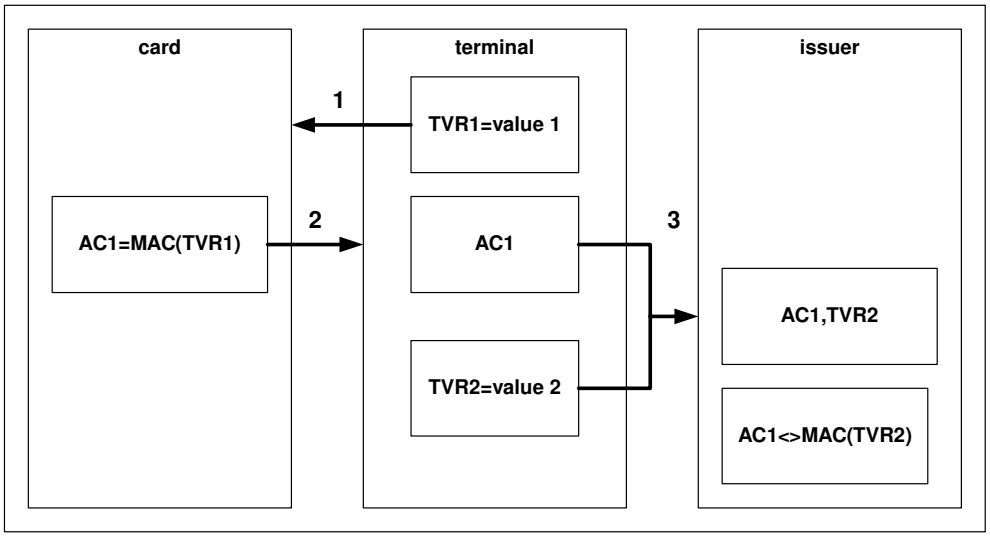
The *Terminal Verification Results* used as input to the AC and the *Terminal Verification Results* present in your clearing message may become desynchronized. This can occur, following EMV 2000, as the terminal can modify the *Terminal Verification Results* after presentation to the card.

If the terminal modifies the *Terminal Verification Results* after presenting them to the M/Chip 4 application, the M/Chip 4 application computes a cryptogram in the **GENERATE AC** with *Terminal Verification Results* that are different from the results you received in the ICC System Related Data (DE 55) data element. In this case, the issuer cryptogram verification would fail, as illustrated by Figure 4.2.

© 2004 MasterCard International Incorporated

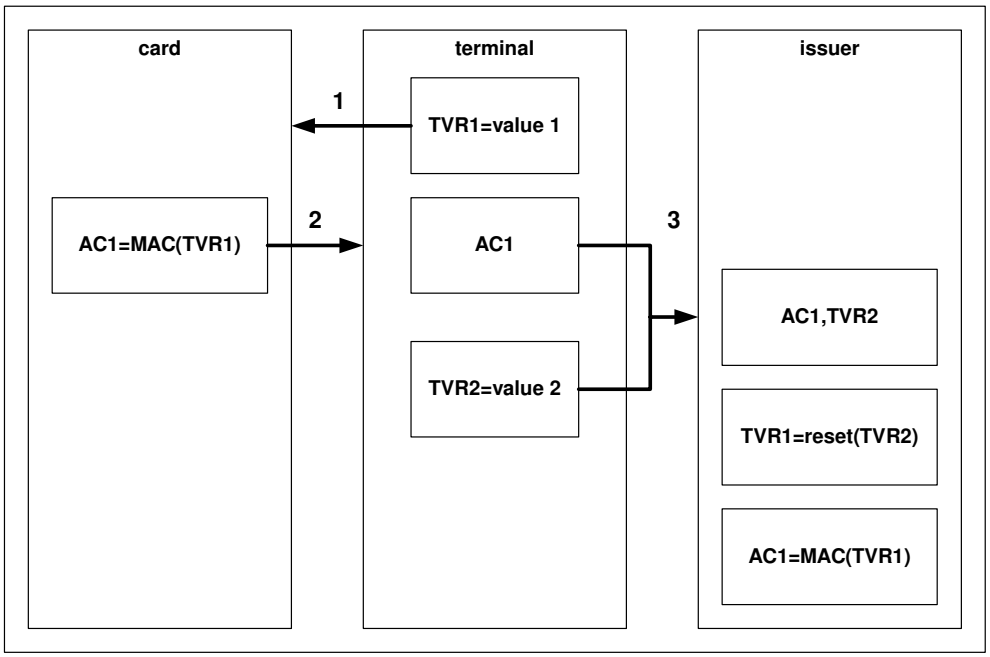
OV Loop Inc.
Ex. 2021 - Page 96

Figure 4.2—AC and Terminal Verification Results



To resolve this problem, you can reset the bits in the *Terminal Verification Results* that may have been modified by the terminal after presentation to the card, prior to *Application Cryptogram* verification, as illustrated by Figure 4.3.

Figure 4.3—Solution to the AC and Terminal Verification Results Inconsistency in EMV



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 97

In the M/Chip 4 application, the only bit in the *Terminal Verification Results* that can be modified by the terminal after presentation to the card but before inclusion in the ICC System Related Data (DE 55) data element is the *Terminal Verification Results* [5][5] (*Script Processing Failed After Final GENERATE AC*).

4.3 Update of Application Status

This section describes the update of the application status in non-volatile memory during an online transaction.

4.3.1 Reset of Script Counter

The M/Chip 4 application resets the issuer *Script Counter*:

- **If** the transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3'):
  - **and** *Issuer Authentication Data* is present
  - **and** the *Authorization Response Cryptogram* verification is successful
- Or **if** the transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3')
  - **and** *Issuer Authentication Data* is not present
  - **and** the terminal requests a TC
  - **and** the magstripe grade issuer mode is supported (i.e. *Application Control* [1][8] is '1b').

4.3.2 Setting of "Go Online on Next Transaction" Bit

The "Go Online on Next Transaction" bit in the Card Verification Results (Card Verification Results [5][4]) is set in an online transaction (*Authorization Response Code* is neither equal to 'Y3' nor 'Z3'):

- **If** *Issuer Authentication Data* is present:
  - **if** the *Authorization Response Cryptogram* verification is successful, it is set to the value you requested in the *ARPC Response Code*
  - **if** the *Authorization Response Cryptogram* verification is not successful, it keeps the value it had in the previous transaction

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 98

- **If** *Issuer Authentication Data* is not present
  - **if** the terminal requests a TC **and** the magstripe grade issuer mode is supported, it is set to the value you requested in the *Default ARPC Response Code*
  - **otherwise** it keeps the value it had in the previous transaction.

4.3.3 Setting of "Issuer Authentication Failed," "Script Received", "Script Failed" Bits

The M/Chip 4 application resets the "Issuer Authentication Failed," "Script Received," "Script Failed" Bits in the *Previous Transaction History* (*Previous Transaction History* [3-1]):

- **If** a transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3')
  - **and** *Issuer Authentication Data* is present
  - **and** the *Authorization Response Cryptogram* verification is successful
- Or **if** the transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3')
  - **and** *Issuer Authentication Data* is not present
  - **and** the terminal requests a TC
  - **and** the magstripe grade issuer mode is supported.

4.3.4 Update of Offline Counters

The M/Chip 4 application updates the *Cumulative Offline Transaction Amount* and *Consecutive Offline Transactions Number* when:

- The transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3')
  - **and** *Issuer Authentication Data* is present
  - **and** the *Authorization Response Cryptogram* verification is successful
  - **and** *Update Counters* is set in the *ARPC Response Code*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 99

- Or the transaction goes online (i.e. if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3')
  - **and** *Issuer Authentication Data* is not present
  - **and** the terminal requests a TC
  - **and** the magstripe grade issuer mode is supported
  - **and** *Update Counters* is set in the *Default ARPC Response Code*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 100

5 Advanced Features

This chapter describes advanced features of the M/Chip 4 application.

5.1 Synchronization between Online and Offline PIN Try Counters 5-1

5.2 Support of Magstripe Grade Issuer Mode 5-2
5.2.1 Magstripe Grade Issuer Mode Not Activated 5-2
5.2.2 Magstripe Grade Issuer Mode Activated 5-3
5.2.2.1 Approve Online Transaction 5-3
5.2.2.2 Update PIN Try Counter 5-4
5.2.2.3 Set Go Online on Next Transaction 5-4
5.2.2.4 Update Counters 5-5

5.3 Behavior on CAT Level 3 Terminals 5-6

5.4 Swapping Application File Locator Configurations 5-7
5.4.1 AFL Swap Mechanism 5-7
5.4.2 PIN De-synchronization on New Cards and Offline PIN Post-activation 5-8
5.4.2.1 How PIN Value De-synchronization Occurs 5-9
5.4.2.2 How the M/Chip 4 Application Resolves PIN Value De-synchronization 5-9
5.4.2.2.1 Temporary Configuration 5-10
5.4.2.2.2 Regular Configuration 5-10

5.5 Consulting the Log of Transactions 5-11

5.6 Retrieving the Offline Balance 5-12

5.7 Post-Issuance Maintenance 5-13
5.7.1 PUT DATA to Modify Data Elements 5-13
5.7.2 UPDATE RECORD to Modify Records 5-14
5.7.3 GET DATA to Retrieve Data 5-14
5.7.4 GET PROCESSING OPTIONS to Retrieve Data 5-15
5.7.5 Retrieving Records In The Transaction Log 5-16
5.7.6 Sending Script Commands to the Card 5-16
5.7.6.1 MAC in Script Counter Limit 5-16

5.8 Additional Check Table 5-17

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 101

5.8.1 How the M/Chip Application Checks the Additional Check Table 5-17
5.8.2 Additional Check Table Content 5-19
5.8.3 Example of Additional Check Table Value 5-21

© 2004 MasterCard International Incorporated

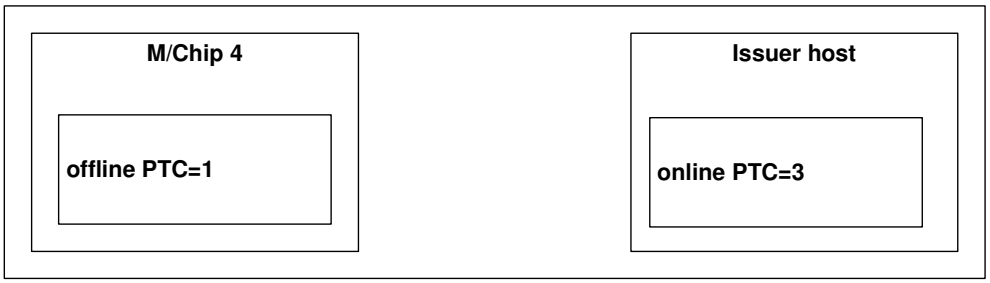
OV Loop Inc.
Ex. 2021 - Page 102

5.1 Synchronization between Online and Offline PIN Try Counters

The M/Chip 4 application allows you to update the offline *PIN Try Counter* during an online transaction without using a script command. The offline *PIN Try Counter* is the card's internal *PIN Try Counter*, representing the number of PIN tries remaining in offline mode. The online *PIN Try Counter* represents the number of PIN tries remaining in online mode. You maintain this data element in the same way as for magnetic stripe-based transactions.

Figure 5.1 illustrates the two *PIN Try Counter*s.

Figure 5.1—Offline and Online PIN Try Counters



During an online transaction, you can synchronize both counters by sending the offline *PIN Try Counter* (in the *Card Verification Results* [3][4-1]) in the authorization request.

If you want to change the offline *PIN Try Counter*, you can send the new value in the authorization response in the *ARPC Response Code*. The *ARPC Response Code* [2][4] is set to '1b' to indicate that the offline *PIN Try Counter* must be updated. The new counter value is contained in the *ARPC Response Code* [1][4-1].

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 103

5.2 Support of Magstripe Grade Issuer Mode

To take into account issuer's migration to chip, the M/Chip 4 application supports the magstripe grade issuer mode. If you support the magstripe grade issuer mode, you can perform online transactions without cryptography. This feature is useful in the following situations:

- The issuer uses the 'chip to magstripe' conversion service.
- The issuer does not use a security module for online transactions (except for the online PIN verification module).

You may also find the magstripe grade issuer mode useful when the card is used mainly on a partial grade network (partial grade acquirer) where the offline counters would otherwise not be reset. For issuers using the magstripe grade issuer mode on a partial grade network, when the counter lower limits are reached, the card will always attempt to go online when used at an online capable terminal. When it is not possible to go online to the issuer, the M/Chip 4 application will approve the transaction. When the counter reaches the upper limit, the card must always go online to the issuer.

If the card is used regularly on full grade terminals, you do not need to support the magstripe grade issuer mode. On a partial grade terminal, after online authorization by the issuer, the terminal accepts the transaction, even if the card rejects the transaction because *Issuer Authentication Data* is missing.

The M/Chip 4 application optionally supports the magstripe grade issuer mode, indicated by the following settings:

- If the *Application Control* [1][8] = '1b', the magstripe grade issuer mode is activated.
- If the *Application Control* [1][8] = '0b', the magstripe grade issuer mode is not activated.

5.2.1 Magstripe Grade Issuer Mode Not Activated

When the magstripe grade issuer mode is not activated, the M/Chip 4 application declines all online transactions without *Issuer Authentication Data* (i.e. the application always provides an AAC in the response to the second **`GENERATE AC`**).

Therefore, the M/Chip 4 application does **not** reset values for the following data elements:

- *Number of Issuer Script Commands Received*
- *Go Online on Next Transaction*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 104

- *Issuer Authentication Failed*
- *Script Received Flag*
- *Script Failed Flag*
- *Cumulative Offline Transaction Amount*
- *Consecutive Offline Transactions Number*

This can prevent the acceptance of future offline transactions, for example when the *Consecutive Offline Transactions Number* equals the *Upper Consecutive Offline Limit*.

5.2.2 Magstripe Grade Issuer Mode Activated

When the magstripe grade issuer mode is activated, the M/Chip 4 application handles online transactions without *Issuer Authentication Data* as follows:

- If the issuer declines the transaction, the terminal requests an AAC in the second **`GENERATE AC`**, and the M/Chip 4 application declines the transaction.
- If the issuer accepts the transaction, the terminal requests a TC in the second **`GENERATE AC`**, and the M/Chip 4 application resets the:
  - *Issuer Authentication Failed*
  - *Script Received Flag*
  - *Script Failed Flag*
  - *Number of Issuer Script Commands Received*

The following tables describe how the M/Chip 4 application interprets each of the bits in the *Default ARPC Response Code* data element to determine which actions to perform.

5.2.2.1 Approve Online Transaction

If …	Then the M/Chip 4 application …
Approve Online Transaction is set (i.e. *Default ARPC Response Code* [2][5] = '1b')	• Approves the transaction. • Computes a TC.
Approve Online Transaction is not set (i.e. *Default ARPC Response Code* [2][5] = '0b')	• Declines the transaction. • Computes an AAC.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 105

5.2.2.2 Update PIN Try Counter

To avoid updates of the *PIN Try Counter* by other parties, you **must not set** the *Default ARPC Response Code* [2][4] to '1b' (Update PIN Try Counter).



Warning **You must set the *Default ARPC Response Code* [2][4] to '0b' (Do not update *PIN Try Counter*).**

Dec 2004

5.2.2.3 Set Go Online on Next Transaction

If …	Then the M/Chip 4 application …
Set Go Online on Next Transaction is set (i.e. *Default ARPC Response Code* [2][3] = '1b').	Forces the next transaction on an online capable terminal to go online (i.e. give an ARQC). It will continue to try to go online on an online capable terminal until it succeeds in connecting to the issuer.
Set Go Online on Next Transaction is not set (i.e. *Default ARPC Response Code* [2][3] = '0b').	Does not force the next transaction on an online capable terminal to go online (i.e. may accept the next transaction offline at the first **`GENERATE AC`**).

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 106

5.2.2.4 Update Counters

If …	Then the M/Chip 4 application …
Reset Counters to Zero is set (i.e. *Default ARPC Response Code* [2][2-1] = '10b').	Resets the two offline counters so that it can accept transactions offline, up to the offline limits.
Do Not Update Offline Counters is set (i.e. *Default ARPC Response Code* [2][2-1] = '00b').	Does not modify the two offline counters.
Set Counters To Upper Offline Limits is set (i.e. *Default ARPC Response Code* [2][2-1] = '01b')	Sets the two offline counters to the *Upper Consecutive Offline Limit* and the *Upper Cumulative Offline Transaction Amount*.
Add Transaction to Counter is set (i.e. *Default ARPC Response Code* [2][2-1] = '11b').	Accumulates the transaction: • in the *Cumulative Offline Transaction Amount* if the transaction is in the *Counter Currency* or in a currency the M/Chip 4 application can convert • in the *Consecutive Offline Transactions Number* if the transaction is in a currency that the application does not recognize.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 107

5.3 Behavior on CAT Level 3 Terminals

At personalization, you can configure the M/Chip 4 application to favor service availability on CAT level 3 terminals by defining that the M/Chip 4 application does not check the *Card Issuer Action Code – Default* on such terminals. This configuration allows the M/Chip 4 application to accept offline transactions on CAT level 3 terminals when the upper offline limits are exceeded.



Definition **A CAT level 3 terminal has a Terminal Type of '26' (Merchant-controlled, unattended and offline only).**

The "Offline Counters and Offline Limits" section in chapter 2 explains how the typical behavior of the application is to accept offline transactions until the *Upper Consecutive Offline Limit* or the *Upper Cumulative Offline Transaction Amount* is reached. Once an upper limit is reached, offline transactions are declined.

If you set the *Application Control* [1][7] to '1b' at personalization, the M/Chip 4 application skips the CIAC – Default check on CAT level 3 terminals. As a result, the M/Chip 4 application can approve a transaction even when the offline limits are exceeded. The M/Chip 4 application counts such approved transactions in the offline counters, in the same way as any other offline transaction.

If you set the *Application Control* [1][7] to '0b' at personalization, the M/Chip 4 application does not skip the CIAC – Default check on the CAT level 3 terminals. It treats CAT level 3 terminals in the same way as any other "offline only" terminal.

Enabling the "unlimited" acceptance of transactions on CAT level 3 terminals has an impact on offline risk management as the upper offline limits can be exceeded on CAT level 3 terminals. The issuer must decide between:

- Giving priority to the service availability by allowing offline transactions to go over the limits on CAT level 3 terminals
- Giving priority to the offline risk management by forbidding offline transactions over the limits on CAT level 3 terminals



Note **When this feature is used at the terminal, you are informed that part of Card Risk Management was skipped when the terminal simulated a CAT level 3 terminal after fraudulent tampering, by the** *Card Verification Results* **[2][4] (set to '1b') contained in the** *Issuer Application Data***.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 108

5.4 Swapping Application File Locator Configurations

5.4.1 AFL Swap Mechanism

The M/Chip 4 application supports the issuance of cards with a temporary configuration activated, which you can deactivate after the card issuance and replace with a regular configuration.

You achieve this by personalizing the M/Chip 4 application with values covering both the temporary and regular configurations. When you are ready to activate the regular configuration, you trigger the swap from the temporary configuration to the regular configuration by changing the value of the *Application File Locator*.

The situation is as follows:

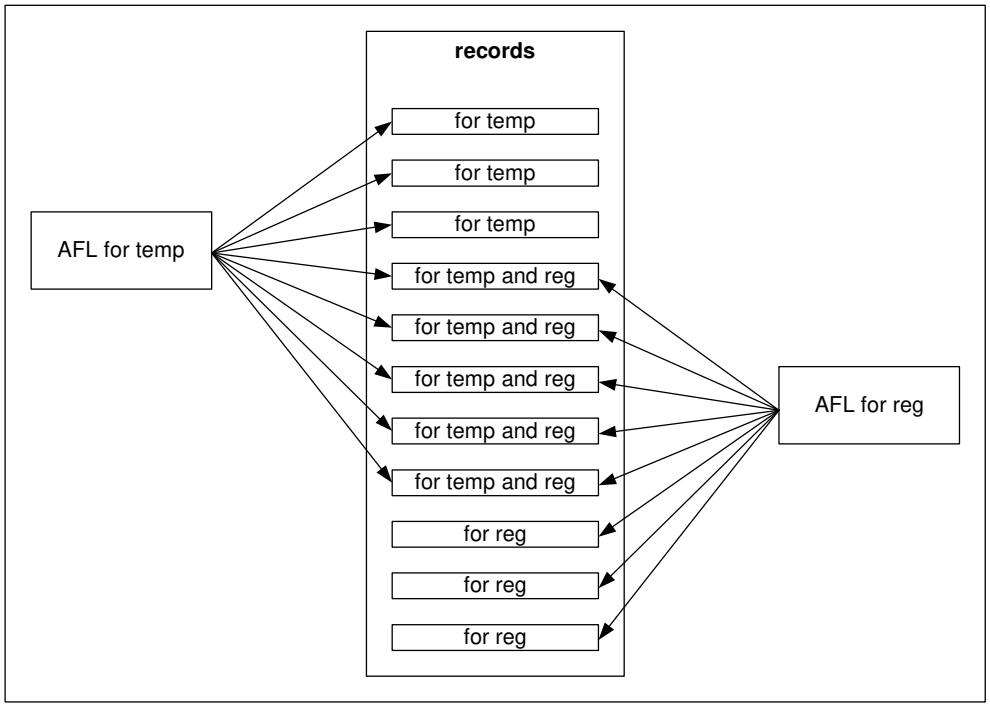
- At card issuance, the M/Chip 4 application already contains the records needed for both configurations, but only the records corresponding to the temporary configuration are referenced in the *Application File Locator*.
- When the card goes online and you wish to activate a new function, you modify the value of the *Application File Locator* using the **PUT DATA** script command to swap from the temporary configuration to the regular configuration. Following the swap, the temporary records cannot be retrieved as they are no longer referenced by the *Application File Locator*. However, the records containing the regular configuration can be retrieved using the **READ RECORD** command as they are now referenced by the *Application File Locator*.

Figure 5.2 illustrates the swap between the temporary and regular *Application File Locator* configurations.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 109

Figure 5.2—AFL for Temporary and Regular Configurations



This mechanism is useful because it provides the issuer with a solution to the problem of PIN de-synchronization on new cards and offline PIN post-activation. There are alternative solutions that you may use.

5.4.2 PIN De-synchronization on New Cards and Offline PIN Post-activation

There are two PIN values as follows:

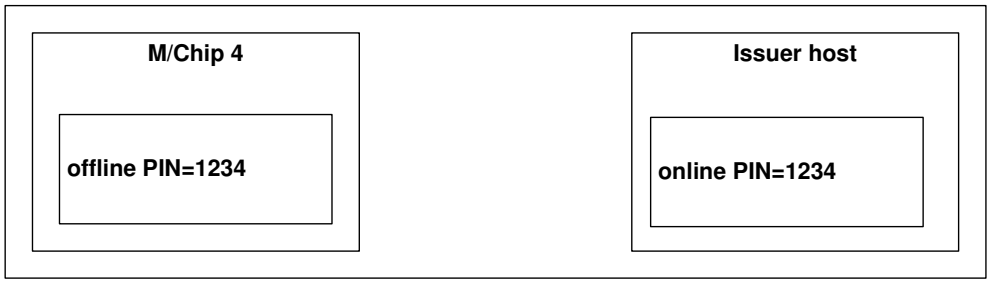
- The offline *Reference PIN* - the card internal PIN that the M/Chip 4 application uses for offline PIN verification.
- The online *Reference PIN* - that you maintain the issuer for online PIN verification.

The values of the offline and online *Reference PIN* must always be identical, as the cardholder cannot distinguish between them, as illustrated in Figure 5.3.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 110

Figure 5.3—Offline and Online PIN



This section describes the situation you may encounter with PIN de-synchronization on new cards after issuance, and the solution to correct the problem.

5.4.2.1 How PIN Value De-synchronization Occurs

The following steps describe how PIN value de-synchronization occurs:

1. At the time of card renewal, you personalize the new card with the *Reference PIN* value.
2. The cardholder changes the *Reference PIN* value using the old card. The online *Reference PIN* value is updated to reflect the change, but you can no longer change the offline *Reference PIN* value on the new card, for example because it is already on its way to the cardholder.
3. The new card is issued. The offline *Reference PIN* value does not reflect the change made by the cardholder in step 2. When the cardholder uses the new PIN value, the offline PIN verification fails.

A similar situation exists for offline PIN post-activation. In this case, the card is issued without offline PIN support but you plan to migrate to offline PIN when the card is already in use.

5.4.2.2 How the M/Chip 4 Application Resolves PIN Value De-synchronization

The M/Chip 4 application can resolve PIN value de-synchronization problems using the AFL swap mechanism as follows. When you personalize the new card, two configurations are considered for the *CVM List*:

- A temporary configuration
- The regular configuration

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 111

5.4.2.2.1 Temporary Configuration

You activate the temporary configuration when the card is issued. It has the following characteristics:

- Offline PIN verification is not supported. Signature verification is supported for "offline only" terminals.
- Online PIN verification is used for online terminals.

At issuance, the card will behave as follows:

- On "offline only" terminals, signature verification is used.
- On online capable terminals, the transaction goes online and Online PIN verification is used.

As a result, when the offline *Reference PIN* is not synchronized with the online *Reference PIN*:

- There is no confusion for the cardholder as the offline *Reference PIN* is not used.
- As soon as the card goes to an online capable terminal, the issuer will synchronize the offline *Reference PIN* value with the online *Reference PIN* value using a script command.

5.4.2.2.2 Regular Configuration

You activate the regular configuration in one of the following situations:

- The values of the offline and online PIN value are synchronized.
- You wish to migrate to offline PIN.

In the regular configuration, the offline PIN verification can replace signature verification depending on the brand carried by the application. Therefore, the value of the *CVM List* for the regular configuration differs from that used in the temporary configuration.

The different values for the temporary and regular *CVM Lists* lead to different values in the associated records referred to in the *Application File Locator*:

- The regular *CVM List* is stored in another record referenced by the new *AFL*.
- Modifying the *CVM List* implies modification to other records, essentially the records for SDA, as the *CVM List* is one of the data elements signed by the issuer.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 112

5.5 Consulting the Log of Transactions

The M/Chip 4 application makes use of a single payment system-specific file: the *Log of Transactions*. The *Short File Identifier (SFI)* for the *Log of Transactions* is fixed at 11.

The *Log of Transactions* contains the logs for **at least** the ten most recent transactions completed with a TC or an AAC. The number of logs can be extended for a specific implementation.

The terminal can retrieve these logs using the EMV **READ RECORD** C-APDU.

The content of each *Transaction Log* is the concatenation of the data elements (without TLV coding) listed in Table 5.1.

Table 5.1—The Transaction Log

Tag	Data Element	Length
'9F27'	*Cryptogram Information Data*	1
'9F02'	*Amount, Authorised*	6
'5F2A'	*Transaction Currency Code*	2
'9A'	*Transaction Date*	3
'9F36'	*Application Transaction Counter*	2
'9F52'	*Card Verification Results*	6

If the M/Chip 4 application has not completed at least ten transactions in its lifetime, some of the entries do not represent transactions, but are empty. These empty entries are not retrievable with the **READ RECORD** (SW1 SW2 = '6A83'). The actual implementation is left to the card application developer.

To allow for future flexibility in the content of the *Transaction Log*, the M/Chip 4 application uses the new data element, *Log Format* (Tag '9F51'). The *Log Format* identifies the content of records in the *Log of Transactions*. The *Log Format* is coded in the same way as a Data Object List and its value is fixed for the M/Chip 4 application as defined in the "Log Format" section of appendix A.

The terminal can access the *Log Format* with a **GET DATA**, immediately after application selection.

The terminal reads the content of the *Log of Transactions* with the following steps:

1. Select the M/Chip 4 application.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 113

2. Receive the *Log Format*, as the response to a **GET DATA**, using Tag '9F51'. The *Log Format* specifies how to interpret the *Transaction Logs*.
3. Receive the *Transaction Logs*, as the response to successive **READ RECORD** C-APDUs, using SFI 11. Record number 1 provides the log for the most recent transaction. Record number 2 provides the log for the most recent transaction –1, record number 3 provides the log for the most recent transaction –2, etc up to ten records (unless the number of records has been extended for the specific implementation). When all records have been retrieved, the card responds with the SW1 SW2 '6A83' – Record not found.



Note **When the card is new, all Transaction Log records are empty. The terminal can read the Transaction Log without initiating a payment transaction.**

5.6 Retrieving the Offline Balance

The terminal retrieves the offline balance and the *CRM Currency Code* from the M/Chip 4 application after a successful selection of the application.

The *Counter Currency* defining the currency of the *Cumulative Offline Transaction Amount* is stored in data element with Tag 'C9' (*CRM Currency Code*) and is always retrievable from the application with a **GET DATA**.

The offline balance is assigned Tag '9F50'. You can allow access to the offline balance by setting the *Application Control* [2][2] to '1b' at personalization. If you allow access, it is retrievable from the application using a **GET DATA** command. If you do not allow access to the offline balance, the application rejects the **GET DATA**.

The M/Chip 4 application computes the offline balance as follows:

Offline Balance = Upper Cumulative Offline Transaction Amount - Cumulative Offline Transaction Amount.

When the cumulative offline transaction amount is greater than the upper cumulative offline limit, the M/Chip 4 application returns a zero balance.



Note **The feature is useful for pre-authorized debit cards.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 114

5.7 Post-Issuance Maintenance

Post-issuance maintenance allows you to modify the personalization settings of cards that are already in circulation.

You can use script commands to update M/Chip 4 application parameters. You can perform these script commands on domestic bank branch terminals, where they are able to verify the cardholder identity. In this environment, you can implement scripts up to the length supported by their domestic networks. The domestic networks may implement a proprietary protocol with a confirmation message informing the issuer of the result of the script processing.

The M/Chip 4 application supports the following script commands:

- **PUT DATA**
- **UPDATE RECORD**
- **PIN CHANGE/UNBLOCK**
- **APPLICATION BLOCK**
- **APPLICATION UNBLOCK**

The following sections describe the use of these commands.

5.7.1 PUT DATA to Modify Data Elements

Table 5.2 lists the data elements that the M/Chip 4 application can modify using the **PUT DATA** command.

Table 5.2—Data Elements that can be Updated Using PUT DATA

Tag	Data Element	Length
'94'	*Application File Locator*	var.
'82'	*Application Interchange Profile*	2
'9F14'	*Lower Consecutive Offline Limit*	1
'9F23'	*Upper Consecutive Offline Limit*	1
'CA'	*Lower Cumulative Offline Transaction Amount*	6
'CB'	*Upper Cumulative Offline Transaction Amount*	6
'C3'	*Card Issuer Action Code – Decline*	3
'C4'	*Card Issuer Action Code – Default*	3

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 115

Tag	Data Element	Length
'C5'	*Card Issuer Action Code – Online*	3
'C7'	*CDOL1 Related Data Length*	1
'C8'	*CRM Country Code*	2
'C9'	*CRM Currency Code*	2
'D1'	*Currency Conversion Table*	25
'D3'	*Additional Check Data*	18
'D5'	*Application Control*	2
'D6'	*Default ARPC Response Code*	2

5.7.2 UPDATE RECORD to Modify Records

The M/Chip 4 application can modify any of the records located in *SFI 1 to 10* using the **UPDATE RECORD** command. The M/Chip 4 application cannot update these records using the **PUT DATA** command.

The terminal can retrieve these records using the **READ RECORD**. The **GET DATA** command cannot be used to retrieve records.

As the records located in SFI 1 to 10 may exceed the international network message size limitation, you must not send **UPDATE RECORD** commands via the international network. Instead, you should send the **UPDATE RECORD** command at the bank branch or via your domestic network.

Records for the *Log of Transactions (SFI 11)* are not updateable with the **UPDATE RECORD**.

5.7.3 GET DATA to Retrieve Data

Table 5.3 lists the data elements that the M/Chip 4 application can access using the **GET DATA** command.

Table 5.3—Data Elements Accessible Using GET DATA

Tag	Data Element	Length
'9F14'	*Lower Consecutive Offline Limit*	1
'9F17'	*PIN Try Counter*	1

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 116

Tag	Data Element	Length	
'9F23'	*Upper Consecutive Offline Limit*	1	
'9F4F'	*Log Format*	17	Dec 2004
'9F50'	*Offline Balance*	6	
'9F7E'	*Application Life Cycle Data*	48	
'CB'	*Upper Cumulative Offline Transaction Amount*	6	
'C3'	*Card Issuer Action Code – Decline*	3	
'C4'	*Card Issuer Action Code – Default*	3	
'C5'	*Card Issuer Action Code – Online*	3	
'C6'	*Counters*	10	Dec 2004
'C7'	*CDOL1 Related Data Length*	1	
'C8'	*CRM Country Code*	2	
'C9'	*CRM Currency Code*	2	
'CA'	*Lower Cumulative Offline Transaction Amount*	6	
'CB'	*Upper Cumulative Offline Transaction Amount*	6	Dec 2004
'D1'	*Currency Conversion Table*	25	
'D3'	*Additional Check Data*	18	
'D5'	*Application Control*	2	
'D6'	*Default ARPC Response Code*	2	

5.7.4 GET PROCESSING OPTIONS to Retrieve Data

Table 5.4 lists the data elements that the M/Chip 4 application can retrieve using the **GET PROCESSING OPTIONS** command. These data elements are not retrievable using the **GET DATA** command.

Table 5.4—Data Elements Returned in GET PROCESSING OPTIONS Response

Tag	Data Element	Length
'94'	Application File Locator	var.
'82'	Application Interchange Profile	2

The M/Chip 4 application can update the data elements listed in Table 5.4 using the **PUT DATA** command.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 117

5.7.5 Retrieving Records In The Transaction Log

The transaction logs are located in *SFI* 11. The terminal can retrieve these logs using the **READ RECORD** command. Refer to the "5.5 Consulting the Log of Transactions" section for more information about the transaction log.

5.7.6 Sending Script Commands to the Card

The M/Chip 4 application accepts script commands after a (first or second) **GENERATE AC** with TC or AAC. The easiest way to send script commands on a bank branch terminal is to request an AAC at first **GENERATE AC**.

Refer to the *M/Chip 4 Security and Key Management* manual for the cryptographic computations required for script commands.

5.7.6.1 MAC in Script Counter Limit

At personalization, you define a value for the MAC in Script Counter Limit. This limit defines the number of MAC verifications in script commands performed by the M/Chip 4 application for a given value of the *Application Transaction Counter* (i.e. per transaction).

If you wish to send a number of script commands in excess of the MAC in Script Counter Limit, you can split the script commands into several sets. You then send each set of scripts for a different value of the *Application Transaction Counter*. The M/Chip 4 application updates the *Application Transaction Counter* each time it performs the **GET PROCESSING OPTIONS** command.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 118

5.8 Additional Check Table

The *Additional Check Table* allows you to add a check to the basic Card Risk Management. The M/Chip 4 application only performs this additional check when you have personalized the *Application Control* [2][3] setting to '1b' (Activate additional check table).

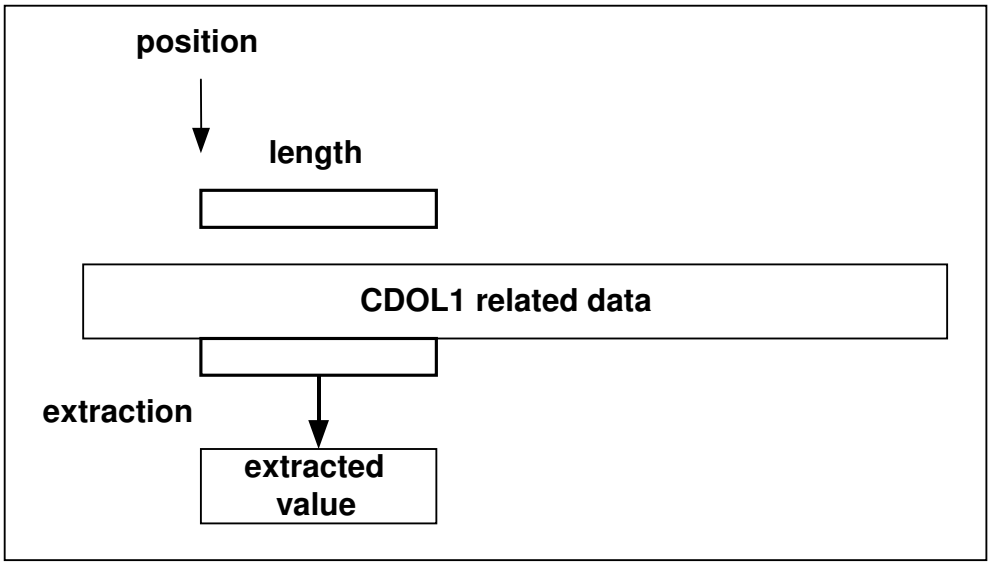
This section explains how the M/Chip 4 application checks the *Additional Check Table*. It also describes and illustrates the detailed content, and provides an example of how it is used.

5.8.1 How the M/Chip Application Checks the Additional Check Table

The M/Chip 4 application checks the *Additional Check Table* by performing the following steps illustrated in Figure 5.5.

1. Extracts a value from the *CDOL 1 Related Data*. This value can be up to seven consecutive bytes. You define the part that is extracted from *CDOL 1 Related Data* at personalization, by setting the following parameters:
   - position in *CDOL 1 Related Data*
   - length in *CDOL 1 Related Data*.

Figure 5.4—CDOL1 Related Data



© 2004 MasterCard International Incorporated

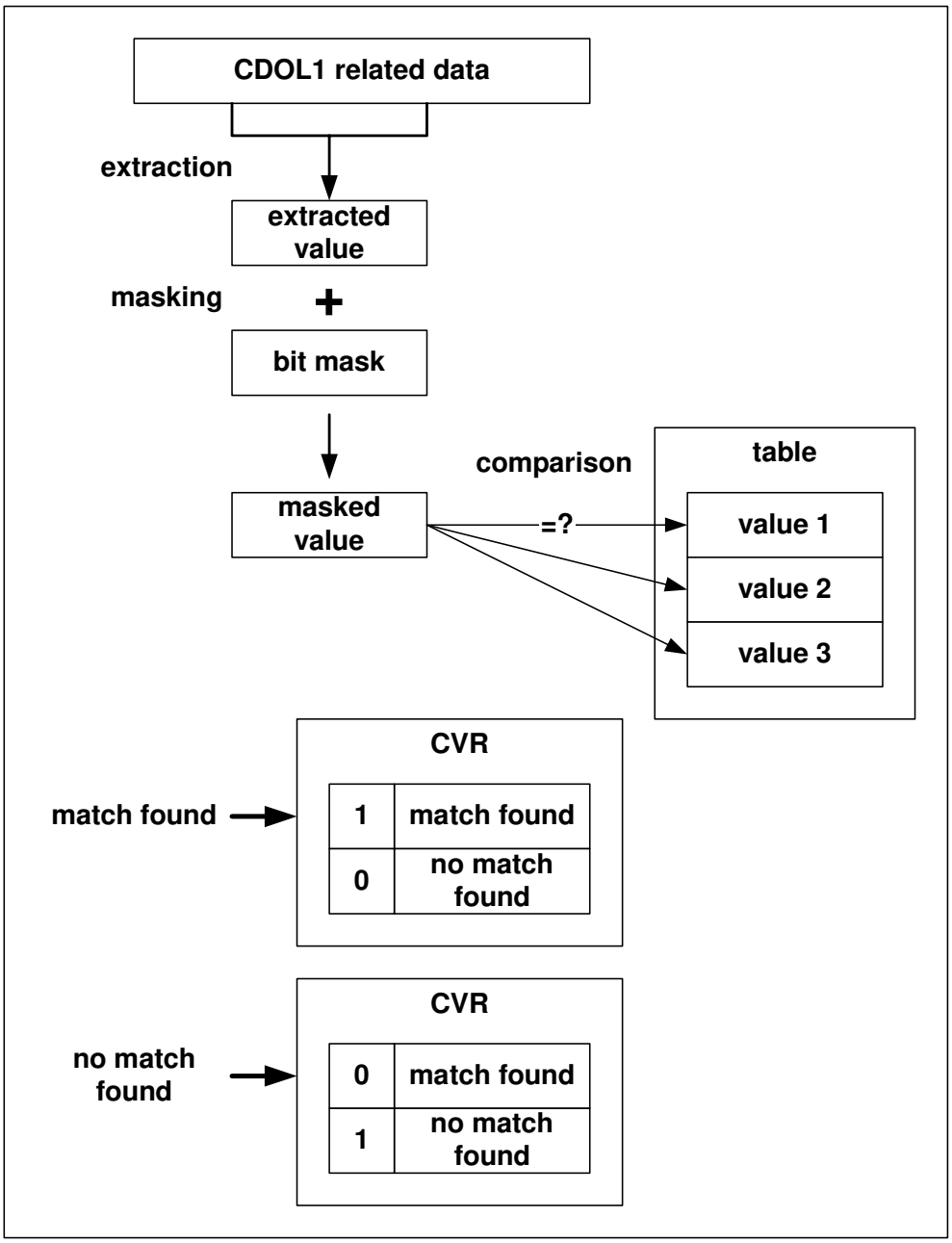
OV Loop Inc.
Ex. 2021 - Page 119

2. Masks the extracted value to a *Bit Mask* to force some of the bits to '0b'.
3. Compares the masked value with values stored in the *Additional Check Table*.
4. **If** the requested value matches a value in the table, sets the *Card Verification Results* [6][2] (Match found in additional check table) bit to '1b' **otherwise** sets the *Card Verification Results* [6][1] bit to '1b' (No match found in additional check table.)
5. Takes an action depending whether a match is found or not, as defined in the settings of the *Card Issuer Action Codes*. Refer to the "Card Issuer Action Codes" section in chapter 2 for further information.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 120

Figure 5.5—Additional Check Table Usage



5.8.2 Additional Check Table Content

The *Additional Check Table* is the concatenation (without TLV coding) of the data elements identified in Table 5.5

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 121

Table 5.5—Additional Check Table

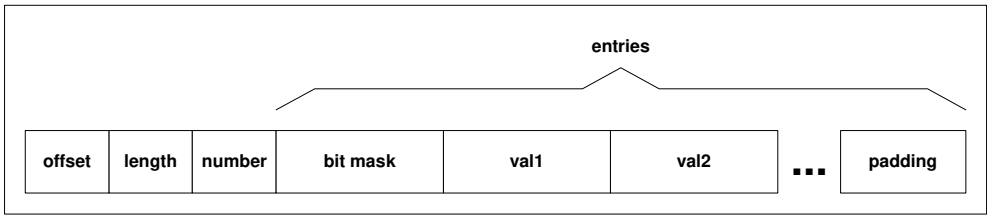
Data Element	Length	Format	Description
Position in CDOL 1 Related Data	1	Binary	Contains the position of the portion of *CDOL 1 Related Data* that is compared to the table entries. If the first byte in *CDOL 1 Related Data* is checked against the entries in the table, the value of *Position in CDOL 1 Related Data* is '01'.
Length in CDOL 1 Related Data	1	Binary	Contains the length of the portion of *CDOL 1 Related Data* that is compared to the table entries.
Number Of Entries	1	Binary	Contains the number of values (including the *Bit Mask*) in the Table Content that are used for the comparison.
Entries	15	Binary	Contains the concatenation of the values used for the comparison, optionally padded with 'FF' to make up 15 bytes. The first value is used as a *Bit Mask*.
Bit Mask	Length in CDOL 1 Related Data	Binary	
Value 1	Length in CDOL 1 Related Data	Binary	
…		…	
Value Number Of Entries – 1	Length in CDOL 1 Related Data	Binary	
Padding	15 – number of entries * Length in CDOL 1 Related Data	'FF...FF'	

Figure 5.6 illustrates the content of the *Additional Check Table*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 122

Figure 5.6—Additional Check Table



Note **The M/Chip 4 application accepts extensions to the *CDOL 1*. It is therefore possible to apply the check on any value that can be requested from the terminal.**

5.8.3 Example of Additional Check Table Value

You can personalize the M/Chip 4 application to take a decision when the value of the *Terminal Country Code* indicates that the transaction did not take place in the following countries:

- Belgium ('0056')
- France ('0250').

To do so, you define the value of the *Additional Check Table* as '0D0203FFFF00560250FFFFFFFFFFFFFFFF. Table 5.6 describes each of the sub-components of this value.

Table 5.6—Explanation of Example Addition Check Table Value

Data Element	Value	Description
Position in CDOL 1 Related Data	0D	*Terminal Country Code* is located in the thirteenth byte of the *CDOL 1 Related Data*, i.e. '0D' in hexadecimal.
Length in CDOL 1 Related Data	02	The length of the *Terminal Country Code* is two bytes.
Number Of Entries	03	The two values in the table used for the comparison are the *Terminal Country Code* for Belgium and France.
Entries		
Bit Mask	FFFF	The comparison is performed on the complete value of the *Terminal Country Code*. The *Bit Mask* is therefore equal to 'FFFF'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 123

Data Element	Value	Description
Value 1	0056	The value of the country code for Belgium.
Value 2	0250	The value of the country code for France.
Padding	FFFFFFFFFFFFFFFFFF	

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 124

6 Personalizing the M/Chip 4 Application

This chapter describes the different types of personalization. It then identifies the data elements that require personalization and the different M/Chip 4 application profiles.

6.1 Personalization Commands and Values 6-1

6.2 Data Element Personalization Values 6-2
6.2.1 Persistent Data Elements for Application Selection 6-2
6.2.2 Persistent Data Elements Referenced in the AFL 6-2
6.2.3 Persistent Data Elements For Card Risk Management 6-4
6.2.4 Secret Keys—Triple DES Keys 6-5
6.2.5 Miscellaneous 6-7
6.2.6 Get Processing Options Response 6-7
6.2.7 Counters and Previous Transaction 6-8
6.2.8 PIN Information 6-8
6.2.9 Data Elements With a Fixed Initial Value 6-9
6.2.10 Additional Data Elements 6-10

6.3 Common Profiles 6-10
6.3.1 Profile Assumptions 6-10
6.3.1.1 Cirrus 6-10
6.3.1.2 MasterCard, MasterCard Electronic, and Maestro 6-10
6.3.1.3 Settings for Offline PIN Verification 6-11
6.3.1.3.1 Modifications to the CVM List 6-11
6.3.1.3.2 Modifications to the Application Control 6-12
6.3.1.4 Application Interchange Profile 6-14
6.3.1.5 Previous Transaction History 6-15
6.3.2 Full Grade Profiles 6-16
6.3.2.1 Default ARPC Response Code 6-16
6.3.2.2 Full Chip—MasterCard—CVM List (Signature + Online PIN + No CVM) 6-17
6.3.2.3 Full Chip—MasterCard—CVM List (Offline Plaintext PIN + Signature + Online PIN + No CVM) 6-21
6.3.2.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Full Grade) 6-25
6.3.2.4 Full Chip—Maestro—CVM List (Online PIN + Signature) 6-27
6.3.2.5 Full Chip Maestro CVM List (Offline Plaintext PIN + Online PIN + Signature) 6-30

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 125

6.3.2.6 Full Chip—Cirrus—CVM List (Online PIN)....6-35
6.3.2.7 Full Chip—MasterCard–Electronic—CVM List (Online PIN + Offline PIN + Signature)....6-38
6.3.2.8 Full Chip—MasterCard Electronic—CVM List (Online PIN + Signature)....6-43
6.3.2.9 Full Chip—MasterCard Electronic—CVM List (Offline PIN + Signature)....6-47
6.3.2.10 Full Chip—MasterCard Electronic—CVM List (Signature)....6-51
6.3.3 Magstripe Grade Profiles....6-55
6.3.3.1 Default ARPC Response Code....6-55
6.3.3.2 Magstripe Grade—MasterCard–CVM List (Signature + Online PIN + No CVM)....6-55
6.3.3.3 Magstripe Grade—MasterCard—CVM List (Offline Plaintext PIN + Signature + Online PIN + No CVM)....6-60
6.3.3.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Magstripe Grade)....6-64
6.3.3.4 Magstripe Grade—Maestro—CVM List (Online PIN + Signature)....6-65
6.3.3.5 Magstripe Grade—Maestro—CVM List (Offline Plaintext PIN + Online PIN + Signature)....6-70
6.3.3.6 Magstripe Grade—Cirrus—CVM List (Online PIN)....6-74
6.3.3.7 Magstripe Grade—MasterCard Electronic—CVM List (Online PIN + Offline PIN + Signature)....6-78
6.3.3.8 Magstripe Grade—MasterCard Electronic—CVM List (Online PIN + Signature)....6-82
6.3.3.9 Magstripe Grade—MasterCard Electronic–CVM List (Offline PIN + Signature)....6-86
6.3.3.10 Magstripe Grade—MasterCard Electronic—CVM List (Signature)....6-90

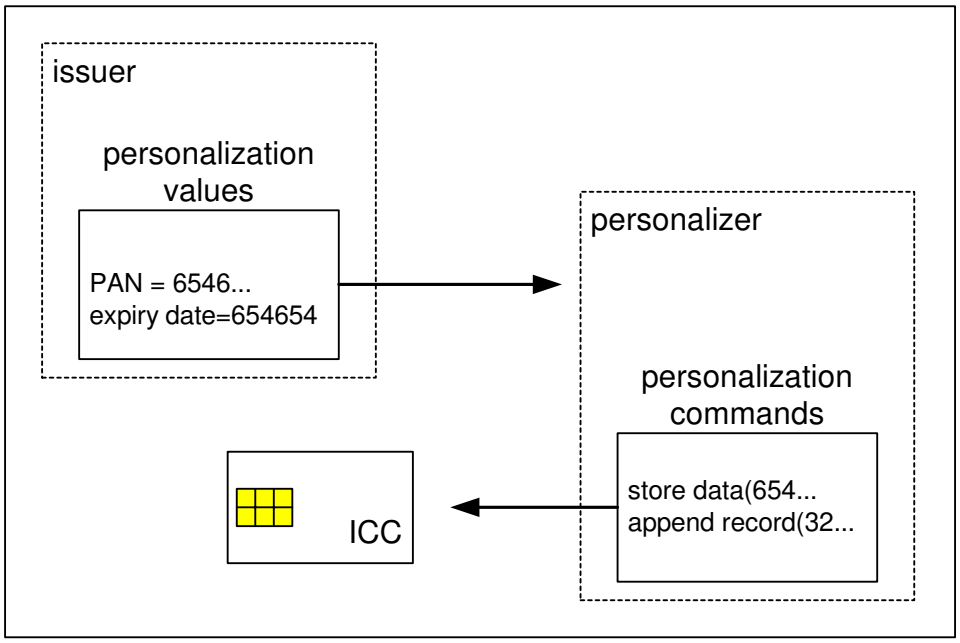
© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 126

6.1 Personalization Commands and Values

It is usually the card personalizer, a third party, who makes the personalization commands creating the link between the card issuer and the card manufacturer. The card personalizer builds personalization commands (i.e. C-APDUs) corresponding to the personalized card using the personalization values it receives from the card issuer. Figure 6.1 illustrates this process.

Figure 6.1—Personalization Process



The card personalizer can hide the implementation details of the card personalization completely from the issuer. In such a case, the personalization role of the issuer is limited to:

- The preparation of the personalization values for the application data elements
- The transmission of these values to the card personalizer

The scope of this document is limited to describing the preparation of personalization values for the M/Chip 4 application data elements.

Note **This does not apply to card platforms like MULTOS, where the application load unit is personalized.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 127

6.2 Data Element Personalization Values

The section identifies the data elements that require personalization. Unless stated otherwise, all data elements are mandatory.

6.2.1 Persistent Data Elements for Application Selection

Table 6.1 lists the persistent data elements for application selection.

Table 6.1—Persistent Data Elements for Application Selection

Tag	Data Element	Length	Application	Value
'4F'	*Application Identifier (AID)*	var.	Lite and Select	The value must be the same as the value for the DF Name in the *FCI*.
'A5'	*File Control Information (FCI)*	var.	Lite and Select	Refer to the *M/Chip Functional Architecture for Debit and Credit*. The M/Chip 4 application does not use the *PDOL* to receive data from the terminal in the **GET PROCESSING OPTIONS**. A PDOL, Tag '9F38', in the *FCI* is not allowed.

6.2.2 Persistent Data Elements Referenced in the AFL

Table 6.2—Persistent Data Elements for Application Selection

Tag	Data Element	Length	Application	Format/Value Supported
'9F42'	*Application Currency Code*	2	Lite and Select	3 numeric [a]
'5F25'	*Application Effective Date*	3	Lite and Select	6 numeric [a]
'5F24'	*Application Expiration Date*	3	Lite and Select	6 numeric [a]
'9F07'	*Application Usage Control*	2	Lite and Select	Binary [a]
'5A'	*Application Primary Account Number*	var. up to 10	Lite and Select	Binary [a]
'5F34'	*Application PAN Sequence Number*	1	Lite and Select	2 numeric [a]

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 128

Tag	Data Element	Length	Application	Format/Value Supported
'9F0D'	*Issuer Action Code – default*	5	Lite and Select	Binary [a] [b]
'9F0E'	*Issuer Action Code – denial*	5	Lite and Select	Binary [a] [b]
'9F0F'	*Issuer Action Code – online*	5	Lite and Select	Binary [a] [b]
'9F08'	*Application Version Number*	2	Lite and Select	Binary [a]
'8C'	*CDOL 1*	var.	Lite and Select	Binary. Default values: • M/Chip Lite 4 = '9F02069F03069F1A0295055F2A029A039C019F37049F35019F45029F3403' • M/Chip Select 4 = '9F02069F03069F1A0295055F2A029A039C019F37049F35019F45029F4C089F3403'. For extensions, refer to the "Additional Check Table Usage" section in chapter 4.
'8D'	*CDOL 2*	var.	Lite and Select	Binary. Values are: • M/Chip Lite 4 = '910A8A029505' • M/Chip Select 4 = '910A8A0295059F37049F4C08'.
'5F20'	*Cardholder Name* [c]	2 – 26	Lite and Select	Alphanumeric and special characters [a]
'8E'	*Cardholder Verification Method (CVM) List*	var. up to 252	Lite and Select	Binary [a] [b]
'5F28'	*Issuer Country Code*	2	Lite and Select	3 numeric [a]
'9F4A'	*SDA tag list*	0 or 1	Lite and Select	Binary [d] If used, only value allowed = '82'.
'57'	*Track-2 Equivalent Data*	var. up to 19	Lite and Select	Binary [a]
'9F49'	*DDOL*	3	Select	Binary. Mandatory value = '9F3704'.
'8F'	*Certification Authority Public Key Index*	1	Lite and Select	Binary [d]
'9F32'	*Issuer Public Key Exponent*	var.	Lite and Select	Binary [d]
'92'	*Issuer Public Key Remainder*	var. (N_I – N_{CA} + 36)	Lite and Select	Binary [d]
'93'	*Signed Application Data*	N_I	Lite and Select	Binary [a] [d]

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 129

Tag	Data Element	Length	Application	Format/Value Supported
'90'	*Issuer Public Key Certificate*	N_{CA}	Lite and Select	Binary [d]
'9F47'	*ICC Public Key Exponent*	var.	Select	Binary [d]
'9F48'	*ICC Public Key Remainder*	var.($N_{IC} - N_I$ + 42)	Select	Binary [d]
'9F46'	*ICC Public Key Certificate*	var. (N_I)	Select	Binary [d]

[a] Refer to the *M/Chip Functional Architecture for Debit and Credit.*

[b] Refer to "6.3 Common Profiles".

[c] The cardholder name as encoded in track-1 of the magnetic stripe, if there is a Track-1 on the magstripe.

[d] Refer to the *M/Chip 4 Security and Key Management* manual.

If offline encrypted *PIN* is supported and if the RSA key for PIN decryption is not the RSA key for signature generation, the data elements listed in Table 6.3 are also referenced in the *Application File Locator*.

Table 6.3—Additional Persistent Data Elements Referenced in the AFL, For Offline Encrypted PIN With a Dedicated Key

Tag	Data Element	Length	Application	Format/Value supported
'9F2E'	*ICC PIN Encipherment Public Key Exponent*	var.	Select	Binary [a]
'9F2F'	*ICC PIN Encipherment Public Key Remainder*	var. ($N_{PE} - N_I$ + 42)	Select	Binary [a]
'9F2D'	*ICC PIN Encipherment Public Key Certificate*	var. (N_I)	Select	Binary [a]

[a] Refer to the *M/Chip 4 Security and Key Management* manual.

Note **The *Lower Consecutive Offline Limit*, Tag '9F14', and the *Upper Consecutive Offline Limit*, Tag '9F23', must not appear in a record covered by the *AFL*. The M/Chip 4 application does not support EMV terminal velocity checking using the LCOL or UCOL.**

6.2.3 Persistent Data Elements For Card Risk Management

Table 6.4 lists the persistent data elements for Card Risk Management.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 130

Table 6.4—Persistent Data Elements for Card Risk Management

Tag	Data Element	Length	Application	Format/Value Supported
'9F14'	*Lower Consecutive Offline Limit*	1	Lite and Select	Binary [a]
'9F23'	*Upper Consecutive Offline Limit*	1	Lite and Select	Binary [a]
'CA'	*Lower Cumulative Offline Transaction Amount*	6	Lite and Select	12 numeric [a]
'CB'	*Upper Cumulative Offline Transaction Amount*	6	Lite and Select	12 numeric [a]
'C3'	*Card Issuer Action Code – Decline*	3	Lite and Select	Binary [b]
'C4'	*Card Issuer Action Code – Default*	3	Lite and Select	Binary [b]
'C5'	*Card Issuer Action Code – Online*	3	Lite and Select	Binary [b]
'C7'	*CDOL1 Related Data Length*	1	Lite and Select	Default values: • M/Chip Lite 4 = '23' • M/Chip Select 4 = '2B'. For extensions, refer to the "Additional Check Table Usage" section in chapter 4. The value must be consistent with the value of CDOL 1.
'C8'	*CRM Country Code*	2	Lite and Select	Binary [a]
'C9'	*CRM Currency Code*	2	Lite and Select	Binary [a]
'D1'	*Currency Conversion Table*	25	Lite and Select	Binary [a]. Refer to appendix B.
'D3'	*Additional Check Data*	18	Lite and Select	Binary. Refer to chapter 5.
'D5'	*Application Control*	2	Lite and Select	Binary [a]
'D6'	*Default ARPC Response Code*	2	Lite and Select	Binary [a]

[a] Refer to appendix A, "Data Dictionary."

[b] Refer to the "6.3 Common Profiles" section.

6.2.4 Secret Keys—Triple DES Keys

Table 6.5—Triple DES key for ICC Dynamic Number Generation

Data Element	Length	Application	Format/Value Supported
ICC Dynamic Number Master Key (MK_{IDN})	16	Select	Binary [a]

[a] Refer to the *M/Chip 4 Security and Key Management* manual.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 131

Table 6.6—Triple DES Master Keys for EPI/MCI and EMV 2000 Session Key Derivation

Data Element	Length	Application	Format/Value Supported
SM for Integrity Master Key (MK_{SMI})	16	Lite and Select	Binary [a]
SM for Confidentiality Master Key (MK_{SMC})	16	Lite and Select	Binary [a]
AC Master Key (MK_{AC})	16	Lite and Select	Binary [a]

[a] Refer to the *M/Chip 4 Security and Key Management* manual.

Table 6.7—Personalization Data for EMV'2000 Session Key Derivation

Data Element	Length	Application	Format/Value Supported
CFDC_limit for Integrity Session Key	1	Lite and Select	Binary [a]
CFDC_limit for Confidentiality Session Key	1	Lite and Select	Binary [a]
CFDC_limit for AC Session Key	1	Lite and Select	Binary [a]

[a] Refer to the *M/Chip 4 Security and Key Management* manual.

Table 6.8—RSA keys (for M/Chip Select 4 only)

Data Element	Length	Application	Format/Value Supported
Length of ICC Public Key Modulus (N_{IC})	1	Select	IS [a]
ICC Private Key	IS [b]	Select	IS [a]
Length of ICC PIN Encipherment Public Key Modulus (N_{PE})	1	Select	IS [a]
ICC PIN Encipherment Private Key	IS [b]	Select	IS [a]

[a] Refer to the *M/Chip 4 Security and Key Management* manual.

[b] Implementation-specific.

The personalization of the *Length of ICC PIN Encipherment Public Key Modulus (N_{PE})* and the *ICC PIN Encipherment Private Key* may be optional on some implementation but must be consistent with the value set for the *Application Control* at personalization.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 132

Note **The M/Chip Select 4 application accepts any RSA key with modulus in the range [80;128], for both DDA and PIN verification. The storage format of the RSA keys is implementation-specific (RSA computations may choose whether to use the Chinese Remainder Theorem). The card application developer must provide storage format details for the RSA keys.**

6.2.5 Miscellaneous

Table 6.9—Miscellaneous Persistent Data Elements

Tag	Data Element	Length	Application	Format/Value Supported
-	*Key Derivation Index*	1	Lite and Select	Binary. Refer to the *M/Chip 4 Security and Key Management* manual.
'9F7E'	*Application Life Cycle Data*	48	Lite and Select	Binary, refer to appendix A. Depending on the possible separation between the loading of the application code and the personalization data on the hardware, only part of the *Application Life Cycle Data* may be personalized.

6.2.6 Get Processing Options Response

Table 6.10—Persistent Data Elements for the Get Processing Options Response

Tag	Data Element	Length	Application	Format/Value Supported
'94'	*Application File Locator*	Var. The length of the *Application File Locator* depends on the organization of data elements in records. The record capacity, and therefore the memory needed for the *Application File Locator*, is specific to each implementation.	Lite and Select	Binary. The value must be consistent with the organization of data into records in files with SFI 1 to 30.
'82'	*Application Interchange Profile*	2	Lite and Select	Binary [a] [b]

[a] Refer to the *M/Chip Functional Architecture for Debit and Credit*.

[b] Refer to the "6.3 Common Profiles" section.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 133

6.2.7 Counters and Previous Transaction

Table 6.11 lists persistent data elements that are linked to the counters and keep track of previous transaction history.

Table 6.11—Persistent Data Elements for Counters and Previous Transactions

Data Element	Length	Application	Format/Value Supported
Application Transaction Counter Limit	2	Lite and Select	Binary, 'FFFF' recommended
Previous Transaction History	1	Lite and Select	Binary. Refer to appendix A.
MAC In Script Counter Limit	1	Lite and Select	Binary, '0F' recommended
Global MAC in Script Counter Limit	3	Lite and Select	Binary, 'FFFFFF' recommended
Bad Cryptogram Counter Limit	2	Select	Binary, 'FFFF' recommended

6.2.8 PIN Information

Table 6.12—Persistent Data Elements for PIN information

Tag	Data Element	Length	Application	Format/Value Supported
'9F17'	*PIN Try Counter*	1	Lite and Select	Binary '0x' Issuer-specific, generally the initial value is the *PIN Try Limit*
-	*PIN Try Limit* [a]	1	Lite and Select	Binary '0x' Issuer-specific
-	*Reference PIN*	8	Lite and Select	Binary, see below

[a] The value of this *PIN Try Limit* is used to (re)initialize the value of the *PIN Try Counter* after each successful offline PIN entry or at the reception of a **`PIN CHANGE/UNBLOCK`** command.

The reference PIN is stored in a PIN block. Figure 6.2 illustrates the format of the PIN block where:

- C = Control field, with a value of binary 2 ('0010b')
- N = PIN length, a 4-bit binary number with permissible values of '0100b' to '1100b'
- P = PIN digit, a 4-bit field with permissible values of '0000b' to '1001b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 134

- P/F = PIN/filler, determined by PIN length
- F = Filler, a 4-bit binary number with value of '1111b'.

Figure 6.2—Format of PIN Block

C	N	P	P	P	P	P/F	P/F	P/F	P/F	P/F	P/F	P/F	P/F	F	F

6.2.9 Data Elements With a Fixed Initial Value

The following data elements have a fixed initial value. The decision about whether to include these data elements as data to be personalized is implementation-specific. If these data elements cannot be personalized, their initial values must be as specified in Table 6.13.

Table 6.13—Data Elements with a Fixed Initial Value

Tag	Data Element	Length	Format	Application	Initial Value
-	*Cumulative Offline Transaction Amount*	6	12, numeric	Lite and Select	'000000000000'
-	*Consecutive Offline Transactions Number*	1	b	Lite and Select	'00b'
'9F5F'	*Script Counter*	1	b	Lite and Select	'00b'
-	*Log of The Current Transaction x (x=1…10 or more)*	20	b	Lite and Select	'00…00b'
-	*ATC for Integrity Session Key ($ATC_{SK,i}$)*	2	b	Lite and Select	'0000b'
-	*CFDC for Integrity Session Key ($CFDC_{SK,i}$)*	1	b	Lite and Select	'00b'
-	*ATC for Confidentiality Session Key ($ATC_{SK,C}$)*	2	b	Lite and Select	'0000b'
-	*CFDC for Confidentiality Session Key ($CFDC_{SK,c}$)*	1	b	Lite and Select	'00b'
-	*ATC for AC Session Key ($ATC_{SK,AC}$)*	2	b	Lite and Select	'0000b'
-	*CFDC for AC Session Key ($CFDC_{SK,AC}$)*	1	b	Lite and Select	'00b'
'9F36'	*Application Transaction Counter*	2	b	Lite and Select	'0000b'
-	*Global MAC in Script Counter*	3	b	Lite and Select	'000000b'
-	*Bad Cryptogram Counter (M/Chip Select 4 only)*	2	b	Lite and Select	'0000b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 135

6.2.10 Additional Data Elements

Some implementations may require the personalization of additional data elements. Contact your application provider for implementation specific data elements.

6.3 Common Profiles

6.3.1 Profile Assumptions

This section describes assumptions made for each profile.

6.3.1.1 Cirrus

This document makes the following assumptions for the profile of Cirrus cards:

- The application is M/Chip Lite 4.
- The M/Chip Lite 4 application does not support offline CAM:
  - No SDA
  - No DDA
  - No CDA
- The M/Chip Lite 4 application does not support offline PIN:
  - No offline plaintext PIN verification
  - No offline encrypted PIN verification

6.3.1.2 MasterCard, MasterCard Electronic, and Maestro

Dec 2004

This document makes the following assumptions for the profile of MasterCard, MasterCard Electronic, and Maestro cards:

- When the application is M/Chip Select 4, it supports:
  - SDA
  - DDA
  - CDA
- When the application is M/Chip Select 4 and it supports offline PIN, the offline PIN verification must be:
  - Either offline plaintext PIN verification only

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 136

  - Either offline plaintext and offline encrypted PIN verification.
- When the application is M/Chip Select 4 and it supports offline encrypted PIN, it may use for PIN encipherment:
  - A DDA public key or
  - A dedicated public key
- MasterCard issuers support Voice Authorization. For issuers who support Voice Authorization, the *Issuer Action Codes* [4][8] (Transaction exceeds floor limit) is set to ('0b', '1b', '1b').
- MasterCard Electronic and Maestro issuers do not support Voice Authorization. For issuers who do not support Voice Authorization, the *Issuer Action Codes* [4][8] (Transaction exceeds floor limit) is set to ('0b', '1b', '0b'). Dec 2004
- MasterCard Electronic has the following value sets:
  - Lower Consecutive Offline Limit ('9F14') is '00'
  - Upper Consecutive Offline Limit ('9F23') is '00'
  - Lower Cumulative Offline Transaction Amount ('CA') is '000000000000'
  - Upper Cumulative Offline Transaction Amount ('CB') is '000000000000'

6.3.1.3 Settings for Offline PIN Verification

In the profiles defined in the following sections, the support for offline PIN verification is limited to offline plaintext.

The support of offline encrypted PIN verification in addition to offline plaintext requires the following modifications to the profiles:

6.3.1.3.1 Modifications to the CVM List

Offline encrypted PIN verification is inserted in the CVM List before offline plaintext PIN verification:

In this example, offline encrypted PIN is added to CVM List (offline plaintext PIN + online PIN + signature + no CVM) to have CVM List (offline encrypted PIN + offline plaintext PIN + online PIN + signature + no CVM).

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 137

Table 6.14—CVM List (Offline Plaintext PIN + Online PIN + Signature + No CVM)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

Table 6.15—CVM List (Offline Encrypted PIN + Offline Plaintext PIN + Online PIN + Signature + No CVM)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Offline encrypted PIN	Apply next	'44'	'03'	If supported.
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

6.3.1.3.2 Modifications to the Application Control

When offline encrypted PIN verification is activated, Application Control [1][4] = '1b'.

- If the RSA key used for PIN decipherment is the CDA/DDA key, Application Control [1][5] = '0b'
- If the RSA key used for PIN decipherment is a dedicated key, *Application Control* [1][5] = '1b'.

Example

Add offline encrypted PIN with dedicated ICC PIN Encipherment public key to the profile with the *Application Control* as defined in Table 6.16.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 138

Table 6.16—Example Application Control (1)

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	'1b'
	1	Encrypt offline counters	'1b'
2	8-4	Reserved	'00000b'
	3	Activate additional check table	'0b'
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	'1b'

The *Application Control* then becomes as defined in Table 6.17.

Table 6.17—Example Application Control (2)

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'1b'
	4	Offline encrypted PIN verification	'1b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	'1b'
	1	Encrypt offline counters	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 139

Byte	Bit	Meaning	Setting
2	8-4	Reserved	'00000b'
	3	Activate additional check table	'0b'
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	'1b'

6.3.1.4 Application Interchange Profile

Based on the assumptions above, Table 6.18 illustrates the values for the *Application Interchange Profile*.

Table 6.18—AIP for M/Chip Select 4

Byte	Bit	Meaning	Setting
1	8	Initiate	'0b'
	7	Offline static data authentication is supported	'1b'
	6	Offline dynamic data authentication is supported	'1b'
	5	Cardholder verification is supported	'1b'
	4	Terminal risk management is to be performed	'1b'
	3	Issuer authentication is supported	'0b'
	2	RFU	'0b'
	1	Combined DDA-GENERATE AC supported	'1b'
2	8-1	RFU	'00'

Table 6.19—AIP for M/Chip Lite 4

Byte	Bit	Meaning	Setting
1	8	Initiate	'0b'
	7	Offline static data authentication is supported	'1b' = MasterCard and Maestro. '0b' = Cirrus.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 140

Byte	Bit	Meaning	Setting
	6	Offline dynamic data authentication is supported	'0b'
	5	Cardholder verification is supported	'1b'
	4	Terminal risk management is to be performed	'1b'
	3	Issuer authentication is supported	'0b'
	2	RFU	'0b'
	1	Combined DDA-GENERATE AC supported	'0b'
2	8-1	RFU	'00'

6.3.1.5 Previous Transaction History

In the profiles below, the "new card" feature is supported. When the M/Chip 4 application on the card supports this feature, a new card will always try to go online to the issuer. If the terminal cannot go online, the card will accept the transaction, but it will continue to try to go online for the following transactions until it is successful.

Table 6.20 defines the value for the *Previous Transaction History* when the "new card" feature is supported.

Table 6.20—Previous Transaction History when "New Card" Supported

Byte	Bit	Meaning	Setting
1	8-7	Reserved	'00b'
	6	Application disabled	'0b'
	5	Application blocked	'0b'
	4	Go Online On Next Transaction	'1b'
	3	Issuer Authentication Failed	'0b'
	2	Script Received	'0b'
	1	Script Failed	'0b'

Table 6.21 describes the modifications to the *Previous Transaction History* that are required when the "new card" feature is not supported.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 141

Table 6.21—Previous Transaction History when "New Card" Not Supported

Byte	Bit	Meaning	Setting
1	8-7	Reserved	'00b'
	6	Application disabled	'0b'
	5	Application blocked	'0b'
	4	Go Online On Next Transaction	'0b'
	3	Issuer Authentication Failed	'0b'
	2	Script Received	'0b'
	1	Script Failed	'0b'

6.3.2 Full Grade Profiles

6.3.2.1 Default ARPC Response Code

Full grade issuers must personalize the *Default ARPC Response Code* with the value defined in Table 6.22.

Table 6.22—Personalization Value for Default ARPC Response Code

Byte	Bit	Meaning	Setting
1	8-5	Reserved	'000'
	4-1	PIN Try Counter	'0000'
2	8-6	RFU	'000b'
	5	Approve online transaction	'0b'
	4	Update PIN Try Counter	'0b'
	3	Set go online on next transaction	'0b'
	2-1	Update counters	'00b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 142

6.3.2.2 Full Chip—MasterCard—CVM List (Signature + Online PIN + No CVM)

Table 6.23—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Signature	Apply next	'5E'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

Dec 2004

Alternatively, Online PIN and Signature can be reversed to give the following table:

Table 6.24—CVM List (Alternative)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

Table 6.25—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 143

Byte	Bit	Meaning	Setting
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.26—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 144

Byte	Bit	Meaning	Decline	Online	Default
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'0b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 145

Byte	Bit	Meaning	Decline	Online	Default
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Table 6.27—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 146

Byte	Bit	Meaning	Decline	Online	Default
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

6.3.2.3 Full Chip—MasterCard—CVM List (Offline Plaintext PIN + Signature + Online PIN + No CVM)

Table 6.28—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash.
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

Dec 2004

Alternatively, Online PIN and Signature can be reversed to give the following table:

Dec 2004

Table 6.29—CVM List (Alternative)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash.
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 147

Table 6.30—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.31—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 148

Byte	Bit	Meaning	Decline	Online	Default
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded [a]	'0b'/'1b'	'0b'/'1b'	'0b'/'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered [a]	'1b'/'0b'	'1b'/'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 149

Byte	Bit	Meaning	Decline	Online	Default
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

[a] Refer to the "6.3.2.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Full Grade)" section for an explanation of the settings.

Table 6.32—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 150

Byte	Bit	Meaning	Decline	Online	Default
	5	Offline PIN Verification Failed [a]	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	4	PTL Exceeded [a]	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'1b'	'1b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

[a] Refer to the "6.3.2.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Full Grade)" section for an explanation of the settings.

6.3.2.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Full Grade)

The settings for the *Issuer Action Code* [3] [6] and *Card Issuer Action Code* [1][4] (PIN Try Limit Exceeded) are as follows:

Setting	If issuers ....
'0b', '0b', '0b'	Accept offline magstripe signature-based transaction even when the Online PIN Try Limit is exceeded on the issuer authorization host and want the same card behavior for both chip and magstripe.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 151

Setting	If issuers ....
'1b', '0b', '0b'	Decline any transaction when the Online PIN Try Limit is exceeded on the issuer authorization host and want the same card behavior for both chip and magstripe.
'0b', '1b', '0b'	Require chip transactions to go online when the terminal detects that offline PIN Try Limit is exceeded but will accept transactions with signature, even if the terminal does not receive a valid online issuer authorization, or if the terminal was offline only.
'0b', '1b', '1b'	Require chip transactions to go online when the terminal detects that offline PIN Try Limit is exceeded and will only accept signature-based transactions if the terminal first obtains a valid online issuer approval.

The settings for the *Issuer Action Codes* [3][4] (PIN entry required, PIN pad present but PIN not entered) and *Card Issuer Action Codes* [1] [5] (offline PIN verification failed) are as follows:

Setting	If issuers ....
'1b', '0b', '0b'	Do not accept PIN entry bypass.
'0b', '0b', '0b'	Accept offline signature-based transactions when PIN entry is bypassed.
0b', '1b', '0b'	Accept signature-based transactions when PIN entry is bypassed, even if the terminal did not get a valid online issuer authorization, or if the terminal was offline only.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 152

6.3.2.4 Full Chip—Maestro—CVM List (Online PIN + Signature)

Dec 2004

These settings are not allowed for new Maestro cards. Those cards must support both Online PIN and Offline PIN, but are not permitted to support Signature.

Table 6.33—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'00'	Always.
Signature	Fail	'1E'	'03'	If supported.

Table 6.34—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 153

Table 6.35—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'1b'	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 154

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	‘0b’	‘1b’	‘1b’
	3	Online PIN entered	‘0b’	‘1b’	‘1b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
4	8	Transaction exceeds floor limit	‘0b’	‘1b’	‘1b’
	7	Lower consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	6	Upper consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	5	Transaction selected randomly for online processing	‘0b’	‘1b’	‘0b’
	4	Merchant forced transaction online	‘0b’	‘1b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
5	8	Default TDOL used	‘0b’	‘0b’	‘0b’
	7	Issuer Authentication was unsuccessful	‘0b’	‘0b’	‘0b’
	6	Script processing failed before final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	5	Script processing failed after final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	4	RFU	‘0b’	‘0b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 155

Table 6.36—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

6.3.2.5 Full Chip Maestro CVM List (Offline Plaintext PIN + Online PIN + Signature)

Dec 2004

New cards must support only Online PIN and Offline PIN. The following settings, except for Signature-related settings, are valid for new cards.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 156

Table 6.37—CVM

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash.
Online PIN	fail	'02'	'04'	If manual cash.
Offline Encrypted PIN	Apply next	'44'	'03'	If supported.
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Online PIN	Apply next	'42'	'00'	Always.
Signature	fail	'1E'	'03'	If supported.

Dec 2004

Note that Offline Encrypted PIN should be included only if the card supports it. In addition, Signature is not permitted for new cards.

Table 6.38—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table. • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 157

Byte	Bit	Meaning	Setting
	1	Include counters in AC	• '0b' Do not include counters in AC • '1b' Include counters in AC

Table 6.39—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 158

Byte	Bit	Meaning	Decline	Online	Default
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'1b'	'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'1b'	'1b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 159

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Table 6.40—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'1b'	'1b'
	5	Offline PIN Verification Failed	'0b'	'1b'	'1b'
	4	PTL Exceeded	'0b'	'1b'	'1b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'1b'	'1b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 160

6.3.2.6 Full Chip—Cirrus—CVM List (Online PIN)

Table 6.41—CVM

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	fail	'02'	'00'	Always

Table 6.42—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 161

Table 6.43—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'0b'	'0b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	'0b'	'0b'
	3	Combined DDA/AC generation failed	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 162

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
4	8	Transaction exceeds floor limit	‘0b’	‘1b’	‘1b’
	7	Lower consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	6	Upper consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	5	Transaction selected randomly for online processing	‘0b’	‘1b’	‘0b’
	4	Merchant forced transaction online	‘0b’	‘1b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
5	8	Default TDOL used	‘0b’	‘0b’	‘0b’
	7	Issuer Authentication was unsuccessful	‘0b’	‘0b’	‘0b’
	6	Script processing failed before final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	5	Script processing failed after final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	4	RFU	‘0b’	‘0b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’

Table 6.44—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	‘0b’	‘0b’	‘0b’
	7	Unable To Go Online Indicated	‘0b’	‘0b’	‘1b’
	6	Offline PIN Verification Not Performed	‘0b’	‘0b’	‘0b’

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 163

Byte	Bit	Meaning	Decline	Online	Default
	5	Offline PIN Verification Failed	‘0b’	‘0b’	‘0b’
	4	PTL Exceeded	‘0b’	‘0b’	‘0b’
	3	International Transaction	‘0b’	‘1b’	‘1b’
	2	Domestic Transaction	‘0b’	‘1b’	‘1b’
	1	Terminal Erroneously Considers Offline PIN OK	‘0b’	‘0b’	‘0b’
2	8	Lower Consecutive Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	7	Upper Consecutive Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	6	Lower Cumulative Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	5	Upper Cumulative Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	4	Go Online On Next Transaction Was Set	‘0b’	‘1b’	‘0b’
	3	Issuer Authentication Failed	‘0b’	‘0b’	‘0b’
	2	Script Received	‘0b’	‘0b’	‘0b’
	1	Script Failed	‘0b’	‘0b’	‘0b’
3	8-3	Reserved-No Meaning	‘000000b’	‘000000b’	‘000000b’
	2	Match Found In Additional Check Table	‘0b’	‘0b’	‘0b’
	1	No Match Found In Additional Check Table	‘0b’	‘0b’	‘0b’

6.3.2.7 Full Chip—MasterCard–Electronic—CVM List (Online PIN + Offline PIN + Signature)

Dec 2004

Table 6.45—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	‘42’	‘01’	If unattended cash.
Offline Encrypted PIN	Apply next	‘44’	‘03’	If supported.
Offline Clear PIN	Apply next	‘41’	‘03’	If supported.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 164

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'03'	If supported.
Signature	Fail	'1E'	'03'	If supported.

Dec 2004

The CVM entry for Online PIN where the Byte 2 setting is '01' should be included if the card is intended to be accepted at ATM. The entry for Offline Encrypted PIN should be included only if the card supports it.

Table 6.46—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	• '0b' = DDA key • '1b' = Dedicated key
	4	Offline encrypted PIN verification	• '0b' = DDA key • '1b' = Dedicated key
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 165

Dec 2004

Table 6.47—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'1b'	'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 166

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	‘0b’	‘1b’	‘1b’
	3	Online PIN entered	‘0b’	‘1b’	‘1b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
4	8	Transaction exceeds floor limit	‘0b’	‘1b’	‘1b’
	7	Lower consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	6	Upper consecutive offline limit exceeded	‘0b’	‘0b’	‘0b’
	5	Transaction selected randomly for online processing	‘0b’	‘1b’	‘0b’
	4	Merchant forced transaction online	‘0b’	‘1b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’
5	8	Default TDOL used	‘0b’	‘0b’	‘0b’
	7	Issuer Authentication was unsuccessful	‘0b’	‘0b’	‘0b’
	6	Script processing failed before final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	5	Script processing failed after final **GENERATE AC**	‘0b’	‘0b’	‘0b’
	4	RFU	‘0b’	‘0b’	‘0b’
	3	RFU	‘0b’	‘0b’	‘0b’
	2	RFU	‘0b’	‘0b’	‘0b’
	1	RFU	‘0b’	‘0b’	‘0b’

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 167

Dec 2004

Table 6.48—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'1b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'1b'	'1b'
	4	PTL Exceeded	'0b'	'1b'	'1b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'0000000b'	'0000000b'	'0000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 168

6.3.2.8 Full Chip—MasterCard Electronic—CVM List (Online PIN + Signature)

Dec 2004

Table 6.49—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'03'	If supported.
Signature	Fail	'1E'	'03'	If supported.

Table 6.50—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 169

Dec 2004

Table 6.51—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'/'1b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 170

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 171

Dec 2004

Table 6.52—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 172

Dec 2004

6.3.2.9 Full Chip—MasterCard Electronic—CVM List (Offline PIN + Signature)

Table 6.53—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Offline Encrypted PIN	Apply next	'44'	'03'	If supported.
Offline Clear PIN	Apply next	'41'	'03'	If supported.
Signature	Fail	'1E'	'03'	If supported.

The CVM entry for Online PIN should be included if the card is intended to be accepted at ATM. The entry for Offline Encrypted PIN should be included only if the card supports it.

Table 6.54—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	• '0b' = DDA key • '1b' = Dedicated Key
	4	Offline encrypted PIN verification	• '0b' = if not supported • '1b' = if supported
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	'0b' = EPI/MCI '1b' = EMV 2000.
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 173

Byte	Bit	Meaning	Setting
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Dec 2004

Table 6.55—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 174

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'1b'	'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 175

Byte	Bit	Meaning	Decline	Online	Default
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Dec 2004

Table 6.56—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'1b'	'1b'
	4	PTL Exceeded	'0b'	'1b'	'1b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 176

Byte	Bit	Meaning	Decline	Online	Default
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

Dec 2004

6.3.2.10 Full Chip—MasterCard Electronic—CVM List (Signature)

Table 6.57—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Signature	Fail	'1E'	'03'	If supported.

Table 6.58—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'0b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 177

Dec 2004

Table 6.59—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'0b'	'1b'	'1b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 178

Dec 2004

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 179

Table 6.60—Card Issuer Action Codes

Dec 2004

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 180

6.3.3 Magstripe Grade Profiles

6.3.3.1 Default ARPC Response Code

Table 6.61—Default ARPC Response Code

Byte	Bit	Meaning	Setting
1	8-5	Reserved	'0'
	4-1	PIN Try Counter	'0'
2	8-6	RFU	'000b'
	5	Approve online transaction	'1b'
	4	Update PIN Try Counter	'0b'
	3	Set go online on next transaction	'0b'
	2-1	Update counters	'10b'

6.3.3.2 Magstripe Grade—MasterCard–CVM List (Signature + Online PIN + No CVM)

Table 6.62—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Signature	Apply next	'5E'	'03'	If supported.
Online PIN	Apply next	'42'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 181

Alternatively, Online PIN and Signature can be reversed to give the following table.

Dec 2004

Table 6.63—CVM List (Alternative)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'03'	If supported.
Signature	Apply next	'5E'	'03'	If supported.
No CVM	fail	'1F'	'03'	If supported.

Table 6.64—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 182

Table 6.65—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 183

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	'1b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'0b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 184

Table 6.66—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	‘0b’	‘0b’	‘0b’
	7	Unable To Go Online Indicated	‘0b’	‘0b’	‘0b’
	6	Offline PIN Verification Not Performed	‘0b’	‘0b’	‘0b’
	5	Offline PIN Verification Failed	‘0b’	‘0b’	‘0b’
	4	PTL Exceeded	‘0b’	‘0b’	‘0b’
	3	International Transaction	‘0b’	‘0b’ or ‘1b’	‘0b’
	2	Domestic Transaction	‘0b’	‘0b’ or ‘1b’	‘0b’
	1	Terminal Erroneously Considers Offline PIN OK	‘0b’	‘0b’	‘0b’
2	8	Lower Consecutive Offline Limit Exceeded	‘0b’	‘1b’	‘0b’
	7	Upper Consecutive Offline Limit Exceeded	‘0b’	‘1b’	‘1b’
	6	Lower Cumulative Offline Limit Exceeded	‘0b’	‘1b’	‘0b’
	5	Upper Cumulative Offline Limit Exceeded	‘0b’	‘1b’	‘1b’
	4	Go Online On Next Transaction Was Set	‘0b’	‘1b’	‘0b’
	3	Issuer Authentication Failed	‘0b’	‘0b’	‘0b’
	2	Script Received	‘0b’	‘1b’	‘0b’
	1	Script Failed	‘0b’	‘1b’	‘0b’
3	8-3	Reserved-No Meaning	‘0000000b’	‘0000000b’	‘0000000b’
	2	Match Found In Additional Check Table	‘0b’ or ‘1b’	‘0b’ or ‘1b’	‘0b’ or ‘1b’
	1	No Match Found In Additional Check Table	‘0b’ or ‘1b’	‘0b’ or ‘1b’	‘0b’ or ‘1b’

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 185

6.3.3.3 Magstripe Grade—MasterCard—CVM List (Offline Plaintext PIN + Signature + Online PIN + No CVM)

Table 6.67—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Offline Clear PIN	Apply next	'41'	'03'	If supported
Signature	Apply next	'5E'	'03'	If supported
Online PIN	Apply next	'42'	'03'	If supported
No CVM	fail	'1F'	'03'	If supported

Dec 2004

Alternatively, Online PIN and Signature can be reversed to give the following table.

Table 6.68—CVM List (Alternative)

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Offline Clear PIN	Apply next	'41'	'03'	If supported
Online PIN	Apply next	'42'	'03'	If supported
Signature	Apply next	'5E'	'03'	If supported
No CVM	fail	'1F'	'03'	If supported

Dec 2004

Table 6.69—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'1b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 186

Byte	Bit	Meaning	Setting
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.70—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 187

Byte	Bit	Meaning	Decline	Online	Default
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded [a]	'0b'/'1b'	'0b'/'1b'	'0b'/'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered [a]	'1b'/'0b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'0b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 188

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

[a] Refer to the "6.3.3.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Magstripe Grade)" section for an explanation of the settings.

Table 6.71—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed [a]	'0b' or '1b'	'0b'	'0b'
	4	PTL Exceeded [a]	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'1b'	'1b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 189

Byte	Bit	Meaning	Decline	Online	Default
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

[a] Refer to the "6.3.3.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Magstripe Grade)" section for an explanation of the settings.

6.3.3.3.1 Explanation of Issuer Action Code and Card Issuer Action Code Settings (Magstripe Grade)

The settings for the *Issuer Action Code* [3] [6] and *Card Issuer Action Code* [1][4] (PIN Try Limit Exceeded) are as follows:

Setting	If issuers ....
'0b', '0b', '0b'	Accept offline magstripe signature-based transaction even when the Online PIN Try Limit is exceeded on the issuer authorization host and want the same card behavior for both chip and magstripe.
'1b', '0b', '0b'	Decline any transaction when the Online PIN Try Limit is exceeded on the issuer authorization host and want the same card behavior for both chip and magstripe.
'0b', '1b', '0b'	Require chip transactions to go online when the terminal detects that offline PIN Try Limit is exceeded but will accept transactions with signature, even if the terminal does not receive a valid online issuer authorization, or if the terminal was offline only.
'0b', '1b', '1b'	Require chip transactions to go online when the terminal detects that offline PIN Try Limit is exceeded and will only accept signature-based transactions if the terminal first obtains a valid online issuer approval.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 190

The settings for the *Issuer Action Codes* [3][4] (PIN entry required, PIN pad present but PIN not entered) and *Card Issuer Action Codes* [1] [5] (offline PIN verification failed) are as follows:

Setting	If issuers ....
'1b', '0b', '0b'	Do not accept PIN entry bypass.
'0b', '0b', '0b'	Accept offline signature-based transactions when PIN entry is bypassed.

6.3.3.4 Magstripe Grade—Maestro—CVM List (Online PIN + Signature)

Dec 2004

These settings are not allowed for new Maestro cards. Those cards must support both Online PIN and Offline PIN, but are not permitted to support Signature.

Table 6.72—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'00'	Always
Signature	Fail	'1E'	'03'	If supported

Table 6.73—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 191

Byte	Bit	Meaning	Setting
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 192

Table 6.74—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'1b'	'0b'	'0b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 193

Byte	Bit	Meaning	Decline	Online	Default
	5	PIN entry required but PIN pad not present/working	'0b'	'1b'	'1b'
	4	PIN entry required, PIN pad present but PIN not entered	'1b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 194

Table 6.75—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	‘0b’	‘0b’	‘0b’
	7	Unable To Go Online Indicated	‘0b’	‘0b’	‘0b’
	6	Offline PIN Verification Not Performed	‘0b’	‘0b’	‘0b’
	5	Offline PIN Verification Failed	‘0b’	‘0b’	‘0b’
	4	PTL Exceeded	‘0b’	‘0b’	‘0b’
	3	International Transaction	‘0b’	‘1b’	‘1b’
	2	Domestic Transaction	‘0b’	‘1b’	‘1b’
	1	Terminal Erroneously Considers Offline PIN OK	‘0b’	‘0b’	‘0b’
2	8	Lower Consecutive Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	7	Upper Consecutive Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	6	Lower Cumulative Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	5	Upper Cumulative Offline Limit Exceeded	‘0b’	‘0b’	‘0b’
	4	Go Online On Next Transaction Was Set	‘0b’	‘1b’	‘0b’
	3	Issuer Authentication Failed	‘0b’	‘0b’	‘0b’
	2	Script Received	‘0b’	‘0b’	‘0b’
	1	Script Failed	‘0b’	‘0b’	‘0b’
3	8-3	Reserved-No Meaning	‘000000b’	‘000000b’	‘000000b’
	2	Match Found In Additional Check Table	‘0b’	‘0b’	‘0b’
	1	No Match Found In Additional Check Table	‘0b’	‘0b’	‘0b’

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 195

6.3.3.5 Magstripe Grade—Maestro—CVM List (Offline Plaintext PIN + Online PIN + Signature)

New cards must support only Online PIN and Offline PIN. The following settings, except for Signature-related settings, are valid for new cards. Dec 2004

Table 6.76—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Online PIN	Fail	'02'	'04'	If manual cash
Offline Encrypted PIN	Apply next	'44'	'03'	If supported
Offline Clear PIN	Apply next	'41'	'03'	If supported
Online PIN	Apply next	'42'	'00'	Always
Signature	Fail	'1E'	'03'	If supported

Dec 2004

Note that Offline Encrypted PIN should be included only if the card supports it. In addition, Signature is not permitted for new cards. Dec 2004

Table 6.77—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 196

Byte	Bit	Meaning	Setting
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.78—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'1b'	'0b'	'0b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 197

Byte	Bit	Meaning	Decline	Online	Default
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'1b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'1b'	'1b'
	4	PIN entry required, PIN pad present but PIN not entered	'1b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **`GENERATE AC`**	'0b'	'0b'	'0b'
	5	Script processing failed after final **`GENERATE AC`**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 198

Byte	Bit	Meaning	Decline	Online	Default
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Table 6.79—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'1b'	'1b'
	5	Offline PIN Verification Failed	'1b'	'0b'	'0b'
	4	PTL Exceeded	'1b'	'0b'	'0b'
	3	International Transaction	'0b'	'0b' or '1b'	'0b'
	2	Domestic Transaction	'0b'	'0b' or '1b'	'0b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'1b'	'1b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'1b'	'0b'
	1	Script Failed	'0b'	'1b'	'0b'
3	8-3	Reserved-No Meaning	'0b'	'0b'	'0b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 199

Byte	Bit	Meaning	Decline	Online	Default
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b' or '1b'	'0b' or '1b'

6.3.3.6 Magstripe Grade—Cirrus—CVM List (Online PIN)

Table 6.80—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Fail	'02'	'00'	Always

Table 6.81—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 200

Table 6.82—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'0b'	'0b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	'0b'	'0b'
	3	Combined DDA/AC generation failed	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'1b'	'0b'	'0b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'1b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'1b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 201

Byte	Bit	Meaning	Decline	Online	Default
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Table 6.83—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'1b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 202

Byte	Bit	Meaning	Decline	Online	Default
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 203

6.3.3.7 Magstripe Grade—MasterCard Electronic—CVM List (Online PIN + Offline PIN + Signature)

Dec 2004

Table 6.84—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Offline Encrypted PIN	Apply next	'44'	'03'	If supported
Offline Clear PIN	Apply Next	'41'	'03'	If supported
Online PIN	Apply Next	'42'	'03'	If supported
Signature	Fail	'1E'	'03'	If supported.

The CVM entry for Online PIN where the Byte 2 setting is '01' should be included if the card is intended to be accepted at ATM. The entry for Offline Encrypted PIN should be included only if the card supports it.

Table 6.85—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	• '0b' = DDA key • '1b' = Dedicated Key
	4	Offline encrypted PIN verification	• '0b' = if not supported • '1b' = if supported
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 204

Byte	Bit	Meaning	Setting
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Dec 2004

Table 6.86—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 205

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'1b'	'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **`GENERATE AC`**	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 206

Dec 2004

Byte	Bit	Meaning	Decline	Online	Default
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Table 6.87—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'0b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'0b'	'0b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'0b'	'0b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 207

Byte	Bit	Meaning	Decline	Online	Default
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

Dec 2004

6.3.3.8 Magstripe Grade—MasterCard Electronic—CVM List (Online PIN + Signature)

Table 6.88—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'00'	If supported
Signature	Fail	'1E'	'03'	If supported

Table 6.89—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 208

Dec 2004

Byte	Bit	Meaning	Setting
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.90—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 209

Byte	Bit	Meaning	Decline	Online	Default
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'1b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 210

Byte	Bit	Meaning	Decline	Online	Default
	1	RFU	‘0b’	‘0b’	‘0b’

Dec 2004

Table 6.91—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	‘0b’	‘0b’	‘0b’
	7	Unable To Go Online Indicated	‘0b’	‘0b’	‘1b’
	6	Offline PIN Verification Not Performed	‘0b’	‘0b’	‘0b’
	5	Offline PIN Verification Failed	‘0b’	‘0b’	‘0b’
	4	PTL Exceeded	‘0b’	‘0b’	‘0b’
	3	International Transaction	‘0b’	‘1b’	‘1b’
	2	Domestic Transaction	‘0b’	‘1b’	‘1b’
	1	Terminal Erroneously Considers Offline PIN OK	‘0b’	‘0b’	‘0b’
2	8	Lower Consecutive Offline Limit Exceeded	‘0b’	‘1b’	‘0b’
	7	Upper Consecutive Offline Limit Exceeded	‘0b’	‘1b’	‘1b’
	6	Lower Cumulative Offline Limit Exceeded	‘0b’	‘1b’	‘0b’
	5	Upper Cumulative Offline Limit Exceeded	‘0b’	‘1b’	‘1b’
	4	Go Online On Next Transaction Was Set	‘0b’	‘1b’	‘0b’
	3	Issuer Authentication Failed	‘0b’	‘0b’	‘0b’
	2	Script Received	‘0b’	‘0b’	‘0b’
	1	Script Failed	‘0b’	‘0b’	‘0b’
3	8-3	Reserved-No Meaning	‘000000b’	‘000000b’	‘000000b’
	2	Match Found In Additional Check Table	‘0b’ or ‘1b’	‘0b’	‘0b’
	1	No Match Found In Additional Check Table	‘0b’ or ‘1b’	‘0b’	‘0b’

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 211

6.3.3.9 Magstripe Grade—MasterCard Electronic–CVM List (Offline PIN + Signature)

Dec 2004

Table 6.92—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Online PIN	Apply next	'42'	'01'	If unattended cash
Offline Encrypted PIN	Apply next	'44'	'03'	If supported
Offline Clear PIN	Apply Next	'41'	'03'	If supported
Signature	Fail	'1E'	'03'	If supported.

The CVM entry for Online PIN should be included if the card is intended to be accepted at ATM. The entry for Offline Encrypted PIN should be included only if the card supports it.

Table 6.93—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	• '0b' =DDA key • '1b' =Dedicated Key
	4	Offline encrypted PIN verification	• '0b' = if not supported • '1b' = supported
	3	Offline plaintext PIN verification	'1b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 212

Dec 2004

Byte	Bit	Meaning	Setting
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

Table 6.94—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 213

Byte	Bit	Meaning	Decline	Online	Default
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'1b'	'1b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'1b'	'0b'
	3	Online PIN entered	'0b'	'1b'	'1b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 214

Byte	Bit	Meaning	Decline	Online	Default
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Dec 2004

Table 6.95—Card Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'1b'
	6	Offline PIN Verification Not Performed	'0b'	'1b'	'1b'
	5	Offline PIN Verification Failed	'0b'	'1b'	'1b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 215

6.3.3.10 Magstripe Grade—MasterCard Electronic—CVM List (Signature)

Dec 2004

Table 6.96—CVM List

CVM	Bit 7 of Byte 1 if CVM Unsuccessful	Byte 1 Setting	Byte 2 Setting	Meaning of Byte 2
Signature	Fail	'1E'	'03'	If supported

Table 6.97—Application Control

Byte	Bit	Meaning	Setting
1	8	Magstripe grade issuer activated	'1b'
	7	Skip CIAC-default on CAT3	'0b'
	6	Reserved	'0b'
	5	Key for offline encrypted PIN verification	'0b'
	4	Offline encrypted PIN verification	'0b'
	3	Offline plaintext PIN verification	'0b'
	2	Session key derivation	• '0b' = EPI/MCI • '1b' = EMV 2000
	1	Encrypt offline counters	• '0b' = Do not encrypt offline counters • '1b' = Encrypt offline counters
2	8-4	Reserved	'00000b'
	3	Activate additional check table	• '0b' = Do not activate additional check table • '1b' = Activate additional check table
	2	Allow retrieval of balance	'0b'
	1	Include counters in AC	• '0b' = Do not include counters in AC • '1b' = Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 216

Table 6.98—Issuer Action Codes

Byte	Bit	Meaning	Decline	Online	Default
1	8	Data authentication was not performed	'0b'	'1b'	'1b'
	7	Offline static data authentication failed	'0b'	'1b'	'1b'
	6	ICC data missing	'0b'	'1b'	'1b'
	5	Card appears on terminal exception file	'0b'	'1b'	'1b'
	4	Offline dynamic data authentication failed	'0b'	• '1b' = Select • '0b' = Lite	• '1b' = Select • '0b' = Lite
	3	Combined DDA/AC generation failed	• '1b' = Select • '0b' = Lite	'0b'	• '1b' = Select • '0b' = Lite
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
2	8	Chip card and terminal have different application versions	'0b'	'0b'	'0b'
	7	Expired application	'0b'	'1b'	'1b'
	6	Application not yet effective	'0b'	'1b'	'0b'
	5	Requested service not allowed for card product	'0b'	'1b'	'1b'
	4	New card	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
3	8	Cardholder verification was not successful	'1b'	'0b'	'0b'
	7	Unrecognized Cardholder Verification Method (CVM)	'0b'	'0b'	'0b'
	6	PIN Try Limit exceeded	'0b'	'0b'	'0b'
	5	PIN entry required but PIN pad not present/working	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 217

Byte	Bit	Meaning	Decline	Online	Default
	4	PIN entry required, PIN pad present but PIN not entered	'0b'	'0b'	'0b'
	3	Online PIN entered	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
4	8	Transaction exceeds floor limit	'0b'	'1b'	'1b'
	7	Lower consecutive offline limit exceeded	'0b'	'0b'	'0b'
	6	Upper consecutive offline limit exceeded	'0b'	'0b'	'0b'
	5	Transaction selected randomly for online processing	'0b'	'1b'	'0b'
	4	Merchant forced transaction online	'0b'	'1b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'
5	8	Default TDOL used	'0b'	'0b'	'0b'
	7	Issuer Authentication was unsuccessful	'0b'	'0b'	'0b'
	6	Script processing failed before final **GENERATE AC**	'0b'	'0b'	'0b'
	5	Script processing failed after final **GENERATE AC**	'0b'	'0b'	'0b'
	4	RFU	'0b'	'0b'	'0b'
	3	RFU	'0b'	'0b'	'0b'
	2	RFU	'0b'	'0b'	'0b'
	1	RFU	'0b'	'0b'	'0b'

Dec 2004

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 218

Table 6.99—Card Issuer Action Codes

Dec 2004

Byte	Bit	Meaning	Decline	Online	Default
1	8	Reserved-No Meaning	'0b'	'0b'	'0b'
	7	Unable To Go Online Indicated	'0b'	'0b'	'1b'
	6	Offline PIN Verification Not Performed	'0b'	'0b'	'0b'
	5	Offline PIN Verification Failed	'0b'	'0b'	'0b'
	4	PTL Exceeded	'0b'	'0b'	'0b'
	3	International Transaction	'0b'	'1b'	'1b'
	2	Domestic Transaction	'0b'	'1b'	'1b'
	1	Terminal Erroneously Considers Offline PIN OK	'0b'	'0b'	'0b'
2	8	Lower Consecutive Offline Limit Exceeded	'0b'	'1b'	'0b'
	7	Upper Consecutive Offline Limit Exceeded	'0b'	'1b'	'1b'
	6	Lower Cumulative Offline Limit Exceeded	'0b'	'1b'	'0b'
	5	Upper Cumulative Offline Limit Exceeded	'0b'	'1b'	'1b'
	4	Go Online On Next Transaction Was Set	'0b'	'1b'	'0b'
	3	Issuer Authentication Failed	'0b'	'0b'	'0b'
	2	Script Received	'0b'	'0b'	'0b'
	1	Script Failed	'0b'	'0b'	'0b'
3	8-3	Reserved-No Meaning	'000000b'	'000000b'	'000000b'
	2	Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'
	1	No Match Found In Additional Check Table	'0b' or '1b'	'0b'	'0b'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 219

7 Migration from M/Chip Lite 2.1

This chapter describes the migration of your authorization and clearing system from M/Chip Lite 2.1 to M/Chip Select 4 or M/Chip Lite 4.

7.1 Overview 7-1

7.2 Authorization Request and Clearing Data Handling 7-1
- 7.2.1 Application Interchange Profile 7-2
  - 7.2.1.1 M/Chip Select 4 7-2
  - 7.2.2 M/Chip Lite 4 7-2
- 7.2.2 Application Cryptogram 7-2
  - 7.2.2.1 Step 1: Derive the Session Key 7-2
  - 7.2.2.2 Step 2 : Build the MAC Input 7-3
    - 7.2.2.2.1 Online Counters not Included in the MAC 7-3
    - 7.2.2.2.2 Online Counters Included in MAC 7-4
  - 7.2.2.3 Step 3: Compute the MAC 7-4
- 7.2.3 Cryptogram Information Data 7-4
- 7.2.4 Issuer Application Data 7-4
  - 7.2.4.1 Length of Issuer Application Data 7-4
  - 7.2.4.2 Key Derivation Index 7-5
  - 7.2.4.3 Cryptogram Version Number 7-5
  - 7.2.4.4 Card Verification Results 7-6
  - 7.2.4.5 DAC/ICC Dynamic Number 2 Bytes 7-6
    - 7.2.4.5.1 M/Chip Select 4 7-6
    - 7.2.4.5.2 M/Chip Lite 4 7-7
  - 7.2.4.6 Plaintext/Encrypted Counters 7-7
- 7.2.5 Terminal Verification Results 7-7
- 7.2.6 Unpredictable Number 7-7
- 7.2.7 Remaining Data Elements 7-7

7.3 Preparing the Authorization Response 7-8
- 7.3.1 Issuer Authentication Data 7-8
  - 7.3.1.1 Step 1: Build the ARPC Response Code 7-8
  - 7.3.1.2 Step 2: Build the Authorization Response Cryptogram 7-8
- 7.3.2 Issuer Script 7-9
  - 7.3.2.1 Step 1: Build the Cryptogram Input 7-9
  - 7.3.2.2 Step 2: Compute the Cryptogram 7-9
  - 7.3.2.3 Step 3: Build the C-APDUs 7-9

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 220

7.3.2.4 Step 4: Build the Script 7-9

7.4 Personalization 7-10
7.4.1 Overview 7-10
7.4.2 Step 1: Build the Personalization Values 7-10

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 221

7.1 Overview

This chapter describes the differences between M/Chip Lite 2.1 and M/Chip Select 4 or M/Chip Lite 4 applications for you to consider when preparing your migration.

The first sections describes differences that impact your authorization and clearing systems, covering the following tasks:

- Handling the authorization request and clearing data
- Preparing the authorization response

These sections only consider the sub-elements in the ICC System Related Data (DE 55) data element. The final section describes the impact of the migration on the application personalization values.

7.2 Authorization Request and Clearing Data Handling

Table 7.1 lists the minimum chip sub-elements in the ICC System Related Data (DE 55) data element. These are identical in the authorization request and clearing data. The following sections describe the impact of the migration on each of these sub-elements.

Table 7.1—Minimum Chip Data (DE 55) in Authorization Request and Clearing Data

Tag	Sub-element	Format	Different?
'82'	*Application Interchange Profile*	b2	Yes
'9F26'	*Application Cryptogram*	b8	Yes
'9F27'	*Cryptogram Information Data*	b1	Yes
'9F10'	*Issuer Application Data*	b…32 var	Yes
'95'	*Terminal Verification Results*	b5	Yes
'9F37'	*Unpredictable Number*	b4	No
'9F36'	*Application Transaction Counter*	b2	No
'9A'	*Transaction Date*	b3	No
'9C'	*Transaction Type*	b1	No
'9F02'	*Amount Authorized*	b6	No
'5F2A'	*Transaction Currency Code*	b2	No

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 222

Tag	Sub-element	Format	Different?
'9F1A'	*Terminal Country Code*	b2	No

7.2.1 Application Interchange Profile

7.2.1.1 M/Chip Select 4

M/Chip Select 4 introduces a new value for the *Application Interchange Profile* to support the DDA and CDA, which were not previously supported by M/Chip Lite 2.1. The CDA generation supported by the application uses the "Combined DDA - Generate AC Supported" bit in the *Application Interchange Profile*.

The new value for the *Application Interchange Profile* does not impact your authorization and clearing systems.

7.2.2 M/Chip Lite 4

The *Application Interchange Profile* is unchanged between M/Chip Lite 2.1 and the M/Chip Lite 4.

7.2.2 Application Cryptogram

The verification of the *Application Cryptogram* can be broken down into the following steps:

1. Derive the session key.
2. Build the MAC input.
3. Compute the MAC.

The following sections describe the impact of the migration on each of these steps.

7.2.2.1 Step 1: Derive the Session Key

The impact of the migration to M/Chip 4 on the session key derivation depends upon the session key derivation algorithm used:

- If the M/Chip 4 application is personalized to allow the use of the EPI/MCI session key derivation algorithm, session key derivation is unchanged from M/Chip Lite 2.1.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 223

- If the M/Chip 4 application is personalized to allow the use of the EMV 2000 session key derivation algorithm, session key derivation is different to M/Chip Lite 2.1. Refer to the *M/Chip 4 Security and Key Management* manual for details of this method.

7.2.2.2 Step 2 : Build the MAC Input

7.2.2.2.1 Online Counters not Included in the MAC

Table 7.2 compares the content of the input to the MAC for the M/Chip Lite 2.1 application and the M/Chip 4 applications when the offline counters are not included in the input to the MAC.

Table 7.2—Input to the AC for M/Chip Lite 2.1 and M/Chip 4 Applications

		Length	
Tag	**Sub-element**	**M/Chip Lite 2.1**	**M/Chip 4**
'9F02'	*Amount Authorised (Numeric)*	6	6
'9F03'	*Amount Other (Numeric)*	6	6
'9F1A'	*Terminal Country Code*	2	2
'95'	*Terminal Verification Results*	5	5
'5F2A'	*Transaction Currency Code*	2	2
'9A'	*Transaction Date*	3	3
'9C'	*Transaction Type*	1	1
'9F37'	*Unpredictable Number*	4	4
'82'	*Application Interchange Profile*	2	2
'9F36'	*ATC*	2	2
'9F52'	*Card Verification Results*	4	6

The impact of the migration is as follows:

- For clearing, the M/Chip 4 application *Terminal Verification Results* may require modification, as described in the "Clearing" section in chapter 4, "Issuer Host Processing of Transactions." There is no impact for authorization.
- The *Card Verification Results* length in the M/Chip 4 applications is longer than in the M/Chip Lite 2.1, as indicated in bold in Table 7.2.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 224

7.2.2.2.2 Online Counters Included in MAC

If the offline counters are included in the MAC input, the MAC input for the M/Chip 4 applications contains eight additional bytes as follows:

- The concatenation of the *Cumulative Offline Transaction Amount*, the *Consecutive Offline Transactions Number* and 'FF' if the counters are sent in clear (i.e. if the *Application Control* [1][1] = '0b')
- The encrypted counters (eight bytes), if the counters are sent encrypted (i.e. if the *Application Control* [1][1] = '1b'). Refer to the *M/Chip 4 Security and Key Management* manual for details.

7.2.2.3 Step 3: Compute the MAC

There is no difference for this step between the M/Chip Lite 2.1 and the M/Chip 4 applications.

7.2.3 Cryptogram Information Data

The M/Chip 4 applications use less values for the *Cryptogram Information Data* as the bits b4 to b1 are no longer used. The *Cryptogram Information Data* set of values for the M/Chip 4 applications is a subset of the set of values used for M/Chip Lite 2.1.

There is no impact on your authorization and clearing systems.

7.2.4 Issuer Application Data

7.2.4.1 Length of Issuer Application Data

Table 7.3 compares the content of *Issuer Application Data* for the M/Chip Lite 2.1 application and the M/Chip 4 applications.

Table 7.3—Issuer Application Data Content for M/Chip Lite 2.1 and M/Chip 4 Applications

Data Element	M/Chip Lite 2.1 Length	M/Chip 4 Length
Key Derivation Index	1	1
Cryptogram Version Number	1	1
Card Verification Results	4	6
DAC/ICC Dynamic Number 2 Bytes	2	2
Plaintext/Encrypted Counters	Not supported	8

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 225

7.2.4.2 Key Derivation Index

As the *Key Derivation Index* is a data element that you control, there is no impact on your authorization and clearing system.

7.2.4.3 Cryptogram Version Number

In M/Chip Lite 2.1, you control the *Cryptogram Version Number* data element. However, in the M/Chip 4, the *Cryptogram Version Number* is controlled by the application.

Table 7.4 provides the *Cryptogram Version Number* values for the M/Chip 4 applications.

Table 7.4—Cryptogram Version Number

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	**x**	**x**	**x**					**Version**
0	**0**	**0**	**1**					**4, other value RFU**
				x	**x**			**Reserved**
				0	**0**			**Other value RFU**
						x		**Session key used for AC computation**
						0		EPI/MCI Session Key
						1		EMV2000 Session Key
							x	**Counters included in AC computation**
							0	Counters not included in AC data
							1	Counters included in AC data

In M/Chip Lite 2.1, the recommended value for the *Cryptogram Version Number* is '01'. Therefore, the values of the *Cryptogram Version Number* differentiate between application versions as follows:

If	Indicates
Cryptogram Version Number [8-5] = '0000b'	M/Chip Lite 2.1 Application.
Cryptogram Version Number [8-5] = '0001b'	M/Chip Select 4 or M/Chip Lite 4 Application.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 226

For the M/Chip 4 applications, the values of the *Cryptogram Version Number* indicate the session key derivation type used and whether online counters are included in AC data as follows:

If *Cryptogram Version Number [8-5]* = '0001b' and …	Indicates
Cryptogram Version Number [2]= '0b'	EPI/MCI session key derivation.
Cryptogram Version Number [2]= '1b'	EMV2000 session key derivation.
Cryptogram Version Number [1]= '0b'	Counters are not included in AC data.
Cryptogram Version Number [1]= '1b'	Counters are included in AC data, as they appear in the *Issuer Application Data*, i.e. in plaintext or encrypted.



Note **The M/Chip 4 applications control the value of the *Cryptogram Version Number* and will adapt to any modification of the cryptographic features activated. A modification of the *Application Control* [1][2] or of the *Application Control* [2][1] via a script will be automatically reflected in the value of the *Cryptogram Version Number* provided by the application.**

7.2.4.4 Card Verification Results

In M/Chip 4, the *Card Verification Results* have been reorganized and enhanced to reflect new features. Therefore, the way in which your authorization and clearing systems interpret the *Card Verification Results* will be different between M/Chip Lite 2.1 and M/Chip 4.

Refer to Appendix D, "Interpreting the Card Verification Results" for detailed information.

7.2.4.5 DAC/ICC Dynamic Number 2 Bytes

7.2.4.5.1 M/Chip Select 4

In M/Chip Lite 2.1, the *DAC/ICC Dynamic Number 2 Bytes* can only contain the *DAC*. In M/Chip Select 4, it may contain two bytes from the *ICC Dynamic Number*, as M/Chip Select 4 supports DDA.

Verification of the *DAC* or the *ICC Dynamic Number* is only required when there is a dispute between the merchant/acquirer and the cardholder/issuer. As this value is therefore unlikely to be verified either during the online connection or during the verification of clearing data, this change should have no impact on your authorization and clearing system.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 227

7.2.4.5.2 M/Chip Lite 4

The *DAC/ICC Dynamic Number 2 Bytes* is unchanged between M/Chip Lite 2.1 and M/Chip Lite 4.

7.2.4.6 Plaintext/Encrypted Counters

The *Plaintext/Encrypted Counters* is not present in the M/Chip Lite 2.1 application. In the M/Chip 4 applications, it provides you with additional information. You can choose whether or not to interpret the *Plaintext/Encrypted Counters*. Therefore, if you choose not to interpret these counters, there is no impact on your authorization and clearing systems.

7.2.5 Terminal Verification Results

The new features supported by the M/Chip 4 applications mean that the *Terminal Verification Results* may contain new values, as compared to the values in M/Chip Lite 2.1. These new features are:

- The Combined DDA/AC generation for M/Chip Select 4
- The script '72' for M/Chip Lite 4

7.2.6 Unpredictable Number

The *Unpredictable Number* is controlled by the terminal. There is therefore no impact on your authorization and clearing systems.

7.2.7 Remaining Data Elements

There are no further differences between the M/Chip Lite 2.1 and the M/Chip 4 applications for the remaining data elements.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 228

7.3 Preparing the Authorization Response

Table 7.5 lists the minimum chip sub-elements in the authorization response. The following sections describe the impact of the migration on each of these sub-elements.

Table 7.5—Minimum Chip sub-elements in Authorization Response

Tag	Sub-element
91	*Issuer Authentication Data*
72	*Issuer Script*

7.3.1 Issuer Authentication Data

You build the *Issuer Authentication Data* with the following steps:

1. Build the *ARPC Response Code.*
2. Build the *Authorization Response Cryptogram.*

7.3.1.1 Step 1: Build the ARPC Response Code

There are differences in the *ARPC Response Code* values between the M/Chip Lite 2.1 and M/Chip 4 applications. Refer to chapter 4, "Issuer Host Processing of Transactions" for an explanation of how to build the *ARPC Response Code* for the M/Chip 4 applications.

7.3.1.2 Step 2: Build the Authorization Response Cryptogram

The impact of the migration to M/Chip 4 on the Authorization Response Cryptogram depends upon the session key derivation algorithm used:

- If the M/Chip 4 application is personalized to allow the use of the EPI/MCI session key derivation algorithm, the computation of the *Authorization Response Cryptogram* is unchanged from M/Chip Lite 2.1.
- If the M/Chip 4 application is personalized to allow the use of the EMV 2000 session key derivation algorithm, the computation of the Authorization Response Cryptogram is different from M/Chip Lite 2.1. This difference relates to session key derivation and not to the input to the cryptogram or the algorithm used to compute it.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 229

7.3.2 Issuer Script

If the M/Chip 4 application is personalized to use the EPI/MCI session key derivation algorithm, the approach for deriving the SMI and SMC session keys used for computing the Message Authentication Code is unchanged from M/Chip Lite 2.1.

You build the issuer script with the following steps:

1. Build the cryptogram input.
2. Compute the cryptogram.
3. Build the C-APDUs.
4. Build the script.

7.3.2.1 Step 1: Build the Cryptogram Input

The cryptogram input has the following differences between M/Chip Lite 2.1 and M/Chip 4:

- Different data elements are updated by the script.
- The **PUT DATA** command is used in place of the **UPDATE RECORD** command to update the Card Risk Management parameters.

7.3.2.2 Step 2: Compute the Cryptogram

If the M/Chip 4 application is personalized to use the EPI/MCI key derivation algorithm, this step is unchanged between M/Chip Lite 2.1 and M/Chip 4.

7.3.2.3 Step 3: Build the C-APDUs

Building the C-APDU is different between M/Chip Lite 2.1 and M/Chip 4. The M/Chip 4 application uses the **PUT DATA** command instead of the **UPDATE RECORD** command to update the Card Risk Management parameters. The M/Chip 4 application only uses the **UPDATE RECORD** command to update any data read by the terminal using the **READ RECORD** command.

7.3.2.4 Step 4: Build the Script

This step is different between M/Chip Lite 2.1 and M/Chip 4. The M/Chip Lite 2.1 application uses script '71'. The M/Chip 4 applications use script '72'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 230

7.4 Personalization

7.4.1 Overview

Neither the M/Chip Lite 2.1 application nor the M/Chip 4 applications specify personalization commands and therefore this section cannot describe potential differences in the execution of these commands. However, personalization can be broken down into two steps:

1. Build the personalization values.
2. Personalize the application with the personalization values.

The following section describes the impact of the migration on step 1 only.

7.4.2 Step 1: Build the Personalization Values

The migration impact between M/Chip Lite 2.1 and M/Chip Lite 4 is minimal for this step.

The migration impact between M/Chip Lite 2.1 and M/Chip Select 4 is mainly related to the management of the *ICC Private Key* or the *ICC PIN Encipherment Private Key* and all related information. These data elements do not exist in M/Chip Lite 2.1.

Table 7.6 describes the personalization data elements for the M/Chip Select 4 and M/Chip Lite 4 implementations and identifies potential differences with the M/Chip Lite 2.1 application.



Note **Depending on the actual implementation of each application, there may be other data elements requiring personalization. This section does not consider such data elements.**

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 231

Table 7.6—Personalization Data Elements

Data Element	Lite 2.1	Lite 4	Select 4	Migration Impact
AID	Y	Y	Y	No impact.
FCI	Y	Y	Y	No impact.
Application Currency Code (or CRM Currency Code)	Y	Y	Y	No impact.
Application Effective Date	Y	Y	Y	No impact.
Application Expiration Date	Y	Y	Y	No impact.
Application Usage Control	Y	Y	Y	No impact.
Application Primary Account Number	Y	Y	Y	No impact.
Application PAN Sequence Number	Y	Y	Y	No impact.
Issuer Action Code – Default	Y	Y	Y	New bit for CDA in M/Chip Select 4.
Issuer Action Code – Denial	Y	Y	Y	New bit for CDA in M/ Chip Select 4.
Issuer Action Code – Online	Y	Y	Y	New bit for CDA in M/ Chip Select 4.
Application Version Number	Y	Y	Y	No impact.
CDOL 1	Y	Y	Y	Values differ for the three applications.
CDOL 2	Y	Y	Y	Values differ for the three applications.
Cardholder Name	Y	Y	Y	No impact.
Cardholder Verification Method (CVM) List	Y	Y	Y	New CVM for Encrypted PIN for M/Chip Select 4.
Issuer Country Code	Y	Y	Y	No impact.
SDA Tag List	Y	Y	Y	No impact.
Track-2 Equivalent Data	Y	Y	Y	No impact.
DDOL	N	N	Y	New data element for M/ Chip Select 4.
Certification Authority Public Key Index	Y	Y	Y	No impact.
Issuer Public Key Certificate	Y	Y	Y	No impact.
Issuer Public Key Exponent	Y	Y	Y	No impact.
Issuer Public Key Remainder	Y	Y	Y	No impact.
Signed Application Data	Y	Y	Y	No impact.
ICC Public Key Certificate	N	N	Y	New data element for M/ Chip Select 4.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 232

Data Element	Lite 2.1	Lite 4	Select 4	Migration Impact
ICC Public Key Exponent	N	N	Y	New data element for M/ Chip Select 4.
ICC Public Key Remainder	N	N	Y	New data element for M/ Chip Select 4.
ICC PIN Encipherment Public Key Certificate	N	N	O	New data element for M/ Chip Select 4.
ICC PIN Encipherment Public Key Exponent	N	N	O	New data element for M/ Chip Select 4.
ICC PIN Encipherment Public Key Remainder	N	N	O	New data element for M/ Chip Select 4.
Application Control	Y	Y	Y	Values differ for the three applications.
Default ARPC Response Code	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
Lower Consecutive Offline Limit	Y	Y	Y	No impact.
Upper Consecutive Offline Limit	Y	Y	Y	No impact.
Lower Cumulative Offline Transaction Amount	Y	Y	Y	No impact.
Upper Cumulative Offline Transaction Amount	Y	Y	Y	No impact.
Card Issuer Action Code – Default	Y	Y	Y	Values differ for the three applications.
Card Issuer Action Code – Online	Y	Y	Y	Values differ for the three applications.
Card Issuer Action Code – Decline	Y	Y	Y	Values differ for the three applications.
Currency Conversion Table	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
ICC Dynamic Number Master Key (MK_{IDN})	N	N	Y	New data element for M/Chip Select 4.
SM for Integrity Master Key (MK_{SMI})	Y	Y	Y	No impact.
SM for Confidentiality Master Key (MK_{SMC})	Y	Y	Y	No impact.
AC Master Key (MK_{AC})	Y	Y	Y	No impact.
CFDC_limit for Integrity Session Key	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
CFDC_limit for Confidentiality Session Key	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 233

Data Element	Lite 2.1	Lite 4	Select 4	Migration Impact
CFDC_limit for AC Session Key	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
Length of ICC Public Key Modulus (N_{IC})	N	N	Y	New data element for M/Chip Select 4.
ICC Private Key	N	N	Y	New data element for M/Chip Select 4.
Length of ICC PIN Encipherment Public Key Modulus (N_{PE})	N	N	O	New data element for M/Chip Select 4.
ICC PIN Encipherment Private Key	N	N	O	New data element for M/Chip Select 4.
CRM Country Code	N	Y	Y	New data element for M/Chip Select 4.
Key Derivation Index	Y	Y	Y	No impact.
Application Life Cycle Data	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
Previous Transaction History	N	Y	Y	New data element for M/Chip Select 4 and M/Chip Lite 4.
Application File Locator	Y	Y	Y	The value of the *Application File Locator* depends on the organization of data in files, which is up to the issuer.
Application Interchange Profile	Y	Y	Y	No impact for M/Chip Lite 4; New value for M/Chip Select 4.
PIN Try Limit	Y	Y	Y	No impact.
PIN Try Counter	Y	Y	Y	No impact.
Reference PIN	Y	Y	Y	No impact.
Last Online Application Transaction Counter ('9F13')	Y	N	N	No longer used in M/Chip 4 implementations.
Card TVR Action Code	Y	N	N	No longer used in M/Chip 4 implementations.
Non-Domestic Control Factor	Y	N	N	No longer used in M/Chip 4 implementations.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 234

8 Migration from M/Chip Select 2

This chapter describes the migration of your authorization and clearing system from M/Chip Select 2 to M/Chip Select 4.

8.1 Overview 8-1

8.2 Authorization Request and Clearing Data Handling 8-1
- 8.2.1 Application Interchange Profile 8-2
- 8.2.2 Application Cryptogram 8-2
  - 8.2.2.1 Step 1: Derive the Session Key 8-2
  - 8.2.2.2 Step 2: Build the MAC Input 8-3
    - 8.2.2.2.1 Online Counters not Included in the MAC 8-3
    - 8.2.2.2.2 Online Counters Included in the MAC 8-4
  - 8.2.2.3 Step 3: Compute the MAC 8-4
- 8.2.3 Cryptogram Information Data 8-4
- 8.2.4 Issuer Application Data 8-4
  - 8.2.4.1 Length of Issuer Application Data 8-5
  - 8.2.4.2 Key Derivation Index 8-5
  - 8.2.4.3 Cryptogram Version Number 8-5
  - 8.2.4.4 Card Verification Results 8-6
  - 8.2.4.5 DAC/ICC Dynamic Number 2 Bytes 8-6
  - 8.2.4.6 Plaintext/Encrypted Counters 8-6
- 8.2.5 Terminal Verification Results 8-6
- 8.2.6 Unpredictable Number 8-6
- 8.2.7 Remaining Data Elements 8-7

8.3 Preparing the Authorization Response 8-7
- 8.3.1 Issuer Authentication Data 8-7
  - 8.3.1.1 Building the ARPC Response Code 8-7
  - 8.3.1.2 Building the Authorization Response Cryptogram 8-7
- 8.3.2 Issuer Script 8-8
  - 8.3.2.1 Step 1: Build the Cryptogram Input 8-8
  - 8.3.2.2 Step 2: Compute the Cryptogram 8-8
  - 8.3.2.3 Step 3: Build the C-APDUs 8-8
  - 8.3.2.4 Step 4: Build the Script 8-9

8.4 Personalization 8-9
- 8.4.1 Overview 8-9

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 235

8.4.2 Step 1: Build the Personalization Values 8-9

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 236

8.1 Overview

The following section is dedicated to the differences between M/Chip Select 2 and M/Chip Select 4 applications for consideration when preparing the migration.

The first sections describes differences that impact your authorization and clearing systems, covering the following tasks:

- Handling the authorization request and clearing data
- Preparing the authorization response.

These sections only consider the chip sub-elements in the ICC System Related Data (DE 55) data element. The final section describes the impact of the migration on the application personalization values.

8.2 Authorization Request and Clearing Data Handling

Table 8.1 lists the minimum chip sub-elements in the ICC System Related Data (DE 55) data element. These are identical in the authorization request and clearing data. The following sections describe the impact of the migration on each of these sub-elements.

Table 8.1—Minimum Chip Data Elements Authorization Request and Clearing Data (DE 55) for M/Chip Select

Tag	Sub-element	Format	Different?
'82'	*Application Interchange Profile*	b2	Yes
'9F26'	*Application Cryptogram*	b8	Yes
'9F27'	*Cryptogram Information Data*	b1	Yes
'9F10'	*Issuer Application Data*	b..32 var	Yes
'95'	*Terminal Verification Results*	b5	Yes
'9F37'	*Unpredictable Number*	b4	No
'9F36'	*Application Transaction Counter*	b2	No
'9A'	*Transaction Date*	b3	No
'9C'	*Transaction Type*	b1	No
'9F02'	*Amount Authorized*	b6	No
'5F2A'	*Transaction Currency Code*	b2	No

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 237

Tag	Sub-element	Format	Different?
'9F1A'	*Terminal Country Code*	b2	No

8.2.1 Application Interchange Profile

M/Chip Select 4 introduces a new value for the *Application Interchange Profile* to support the DDA and CDA, which were not previously supported by M/Chip Select 2. The CDA generation supported by the application uses the "Combined DDA - generate AC supported" bit in the *Application Interchange Profile*.

The new value for the *Application Interchange Profile* does not impact your authorization and clearing systems.

8.2.2 Application Cryptogram

The verification of the *Application Cryptogram* can be broken down into the following steps:

1. Derive the session key.
2. Build the MAC input.
3. Compute the MAC.

The following sections describe the impact of the migration on each of these steps.

8.2.2.1 Step 1: Derive the Session Key

The impact of the migration to the M/Chip Select 4 application on the session key derivation depends upon the session key derivation algorithm used:

- If the M/Chip Select 4 application is personalized to allow the use of the EPI/MCI session key derivation algorithm, session key derivation is unchanged from M/Chip Select 2.
- If the M/Chip Select 4 application is personalized to allow the use of the EMV 2000 session key derivation algorithm, session key derivation is different to M/Chip Select 2. Refer to the *M/Chip 4 Security and Key Management* manual for details of this method.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 238

8.2.2.2 Step 2: Build the MAC Input

8.2.2.2.1 Online Counters not Included in the MAC

Table 8.2 compares the content of the input to the MAC for the M/Chip Select 2 application and the M/Chip Select 4 application when the offline counters are not included in the input to the MAC.

Table 8.2—Input to AC for M/Chip Select 2 and M/Chip Select 4

		Length	
Tag	**Data Element**	**M/Chip Select 2**	**M/Chip Select 4**
'9F02'	*Amount Authorised (Numeric)*	6	6
'9F03'	*Amount Other(Numeric)*	6	6
'9F1A'	*Terminal Country Code*	2	2
'95'	*Terminal Verification Results*	5	5
'5F2A'	*Transaction Currency Code*	2	2
'9A'	*Transaction Date*	3	3
'9C'	*Transaction Type*	1	1
'9F37'	*Unpredictable Number*	4	4
'82'	*Application Interchange Profile*	2	2
'9F36'	*ATC*	2	2
'9F52'	*Card Verification Results*	4	6

The impact of the migration is as follows:

- For Clearing, the *Terminal Verification Results* for the M/Chip Select 4 application may require modification, as described in the "Clearing" section in chapter 4, "Issuer Host Processing of Transactions." There is no impact for authorization.
- The *Card Verification Results* length in the M/Chip Select 4 application is longer than in the M/Chip Select 2, as indicated in bold in Table 8.2.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 239

8.2.2.2.2 Online Counters Included in the MAC

If the offline counters are included in the MAC input, the MAC input for the M/Chip Select 4 application contains eight additional bytes as follows:

- The concatenation of the *Cumulative Offline Transaction Amount*, the *Consecutive Offline Transactions Number* and 'FF' if the counters are sent in clear (i.e. if the *Application Control* [1][1] = '0b')
- The encrypted counters (eight bytes), if the counters are sent encrypted (i.e. if the *Application Control* [1][1] = '1b'). Refer to the *M/Chip 4 Security and Key Management* manual for details.

8.2.2.3 Step 3: Compute the MAC

There is no difference for this step between the M/Chip Select 2 and the M/Chip Select 4 applications.

8.2.3 Cryptogram Information Data

The M/Chip Select 4 application uses less values for the *Cryptogram Information Data* as the bits b4 to b1 are no longer used. The *Cryptogram Information Data* set of values for the M/Chip Select 4 application is a subset of the set of values used for M/Chip Select 2.

There is no impact on your authorization and clearing systems

8.2.4 Issuer Application Data

Table 8.3 compares the content of *Issuer Application Data* for the M/Chip Select 2 application and the M/Chip Select 4 application.

Table 8.3—Issuer Application Data Content for M/Chip Select 2 and M/Chip Select 4 Application

Data Element	M/Chip Select 2 Length	M/Chip Select 4 Length
Length of Issuer Application Data	1	Not supported
Key Derivation Index	1	1
Cryptogram Version Number	1	1
Card Verification Results	4	6
DAC/ICC Dynamic Number 2 Bytes	2	2
Plaintext/Encrypted Counters	Not supported	8

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 240

8.2.4.1 Length of Issuer Application Data

In M/Chip Select 2, the *Issuer Application Data* contains the *Length of Issuer Application Data* data element (one-byte in length). This data element contains the value '08' indicating the length of *Issuer Application Data*. The M/Chip Select 4 application does not contain this data element. This difference will have an impact on your authorization and clearing systems.

8.2.4.2 Key Derivation Index

As the *Key Derivation Index* is a data element that you control, there is no impact on your authorization and clearing system.

8.2.4.3 Cryptogram Version Number

In M/Chip Select 2, you control the *Cryptogram Version Number* data element. However, in M/Chip Select 4, the *Cryptogram Version Number* is controlled by the application.

In M/Chip Select 2, the recommended value for the *Cryptogram Version Number* is '01'. Therefore, the values of the *Cryptogram Version Number* differentiate between application versions as follows:

If	Indicates
Cryptogram Version Number [8-5] = '0000b'	M/Chip Select 2 Application.
Cryptogram Version Number [8-5] = '0001b'	M/Chip Select 4 Application.

For the M/Chip Select 4 application, the values of the *Cryptogram Version Number* indicate the session key derivation type used and whether online counters are included in AC data as follows:

***If Cryptogram Version Number [8-5]* = '0001b' and ...**	**Indicates**
Cryptogram Version Number [2]= '0b'	EPI/MCI session key derivation.
Cryptogram Version Number [2]= '1b'	EMV2000 session key derivation.
Cryptogram Version Number [1]= '0b'	Counters are not included in AC data.
Cryptogram Version Number [1]= '1b'	Counters are included in AC data, as they appear in the *Issuer Application Data*, i.e. in plaintext or encrypted.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 241



Note **The M/Chip Select 4 application controls the value of the *Cryptogram Version Number* and will adapt to any modification of the cryptographic features activated. A modification of the *Application Control [1][2]* or of the *Application Control [2][1]* via a script will be automatically reflected in the value of the *Cryptogram Version Number* provided by the application.**

8.2.4.4 Card Verification Results

In M/Chip Select 4, the *Card Verification Results* have been reorganized and enhanced to reflect new features. Therefore, the way in which your authorization and clearing systems interpret the *Card Verification Results* will be different between M/Chip Select 2 and M/Chip Select 4.

Refer to appendix D, "Interpreting the Card Verification Results" for detailed information.

8.2.4.5 DAC/ICC Dynamic Number 2 Bytes

The M/Chip Select 2 application compares the value of *DAC/ICC Dynamic Number 2 Bytes* with the value created and held in the card. If these values are different, the M/Chip Select 2 application sets the two bytes output to zero.

The M/Chip Select 4 application does not perform this check.

8.2.4.6 Plaintext/Encrypted Counters

The *Plaintext/Encrypted Counters* is not present in the M/Chip Select 2 application. In the M/Chip Select 4 application, it provides you with additional information. You can choose whether or not to interpret the *Plaintext/Encrypted Counters*. Therefore, if you choose not to interpret these counters, there is no impact on your authorization and clearing systems.

8.2.5 Terminal Verification Results

The M/Chip Select 4 application supports the Combined DDA/AC generation feature not previously supported by the M/Chip Select 2 application.

The M/Chip Select 4 application does not support the 'critical script' – '71' that was supported by the M/Chip Select 2 application.

8.2.6 Unpredictable Number

The *Unpredictable Number* is controlled by the terminal. There is therefore no impact on your authorization and clearing systems.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 242

8.2.7 Remaining Data Elements

There are no further differences between the M/Chip Select 2 and the M/Chip Select 4 application for the remaining data elements in Table 8.1.

8.3 Preparing the Authorization Response

Table 8.4 lists the minimum chip sub-elements in the authorization response. The following sections describe the impact of the migration on each of these sub-elements.

Table 8.4—Minimum Chip Sub-elements in Authorization Response

Tag	Data Element
91	*Issuer Authentication Data*
72	*Issuer Script*

8.3.1 Issuer Authentication Data

You build the *Issuer Authentication Data* with the following steps:

1. Build the *ARPC Response Code*.
2. Build the *Authorization Response Cryptogram*.

8.3.1.1 Building the ARPC Response Code

There are differences in the *ARPC Response Code* values between the M/Chip Select 2 and M/Chip Select 4 applications. Refer to chapter 4, "Issuer Host Processing of Transactions" for an explanation of how to build the *ARPC Response Code* for the M/Chip Select 4 application.

8.3.1.2 Building the Authorization Response Cryptogram

The impact of the migration to the M/Chip Select 4 application on the Authorization Response Cryptogram depends upon the session key derivation algorithm used:

- If the M/Chip Select 4 application is personalized to allow the use of the EPI/MCI session key derivation algorithm, the computation of the *Authorization Response Cryptogram* is unchanged from M/Chip Select 2.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 243

- If the M/Chip Select 4 application is personalized to allow the use of the EMV 2000 session key derivation algorithm, the computation of the *Authorization Response Cryptogram* is different from M/Chip Select 2. This difference relates to session key derivation and not to the input to the cryptogram or the algorithm used to compute it.

8.3.2 Issuer Script

If the M/Chip Select 4 application is personalized to use the EPI/MCI session key derivation algorithm, the approach for deriving the SMI and SMC session keys used for computing the Message Authentication Code is unchanged from M/Chip Select 2.

The script commands that are not supported by the M/Chip Select 4 application but supported by the M/Chip Select 2 application, are:

- The **CARD BLOCK** command
- The **END OF SCRIPT** command

You build the issuer script with the following steps:

1. Build the cryptogram input.
2. Compute the cryptogram.
3. Build the C-APDUs.
4. Build the script.

8.3.2.1 Step 1: Build the Cryptogram Input

This step is unchanged between the M/Chip Select 2 and M/Chip Select 4 applications with the exceptions of some new data elements. Refer to the "PUT DATA to Modify Data Elements" section in chapter 5 for a description of these data elements.

8.3.2.2 Step 2: Compute the Cryptogram

If the M/Chip Select 4 application is personalized to use the EPI/MCI key derivation algorithm, this step is unchanged between M/Chip Select 2 and M/Chip Select 4.

8.3.2.3 Step 3: Build the C-APDUs

This step is unchanged between M/Chip Select 2 and M/Chip Select 4.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 244

8.3.2.4 Step 4: Build the Script

This step is different between M/Chip Select 2 and M/Chip Select 4. The M/Chip Select 2 application uses both script '71' and '72'. The M/Chip Select 4 uses script '72'.

8.4 Personalization

8.4.1 Overview

The current M/Chip Select 2 application does not use personalization commands. Instead, it uses the application load unit for personalization and this unit is loaded onto the card. Therefore, this section cannot describe potential differences in the personalization process.

Personalization can be broken down into two steps:

1. Build the personalization values.
2. Personalize the application with the personalization values.

The following section describes the impact of the migration on step 1 only.

8.4.2 Step 1: Build the Personalization Values

The migration impact between M/Chip Select 2 and M/Chip Select 4 is minimal for this step.

Table 8.5 describes the personalization data elements for the M/Chip Select 4 implementations and identifies potential differences with the M/Chip Select 2 application.



Note **Depending on the actual implementation of each application, there may be other data elements requiring personalization. This section does not consider such data elements.**

Table 8.5—Personalization Data Elements

Data Element	Select 2	Select 4	Migration Impact
AID	Y	Y	No impact.
FCI	Y	Y	No impact.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 245

Data Element	Select 2	Select 4	Migration Impact
Application Currency Code (or CRM Currency Code)	Y	Y	No impact.
Application Effective Date	Y	Y	No impact.
Application Expiration Date	Y	Y	No impact.
Application Usage Control	Y	Y	No impact.
Application Primary Account Number	Y	Y	No impact.
Application PAN Sequence Number	Y	Y	No impact.
Issuer Action Code – Default	Y	Y	New bit for CDA.
Issuer Action Code – Denial	Y	Y	New bit for CDA.
Issuer Action Code – Online	Y	Y	New bit for CDA.
Application Version Number	Y	Y	No impact.
CDOL 1	Y	Y	Values differ for the two applications.
CDOL 2	Y	Y	Values differ for the two applications.
Cardholder Name	Y	Y	No impact.
Cardholder Verification Method (CVM) List	Y	Y	No impact.
Issuer Country Code	Y	Y	No impact.
SDA Tag List	Y	Y	No impact.
Track-2 Equivalent Data	Y	Y	No impact.
DDOL	Y	Y	No impact.
Certification Authority Public Key Index	Y	Y	No impact.
Issuer Public Key Certificate	Y	Y	No impact.
Issuer Public Key Exponent	Y	Y	No impact.
Issuer Public Key Remainder	Y	Y	No impact.
Signed Application Data	Y	Y	No impact.
ICC Public Key Certificate	Y	Y	No impact.
ICC Public Key Exponent	Y	Y	No impact.
ICC Public Key Remainder	Y	Y	No impact.
ICC PIN Encipherment Public Key Certificate	O	O	No impact.
ICC PIN Encipherment Public Key Exponent	O	O	No impact.
ICC PIN Encipherment Public Key Remainder	O	O	No impact.
Application Control	Y	Y	Values differ for the two applications.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 246

Data Element	Select 2	Select 4	Migration Impact
Default ARPC Response Code	N	Y	New data element.
Lower Consecutive Offline Limit	Y	Y	Values differ for the two applications.
Upper Consecutive Offline Limit	Y	Y	Values differ for the two applications.
Lower Cumulative Offline Transaction Amount	Y	Y	No impact.
Upper Cumulative Offline Transaction Amount	Y	Y	No impact.
Card Issuer Action Code – Default	Y	Y	Values differ for the two applications.
Card Issuer Action Code – Online	Y	Y	Values differ for the two applications.
Card Issuer Action Code – Decline	Y	Y	Values differ for the two applications.
Currency Conversion Table	Y	Y	Values differ for the two applications.
ICC Dynamic Number Master Key (MK_{IDN})	Y	Y	No impact.
SM for Integrity Master Key (MK_{SMI})	Y	Y	No impact.
SM for Confidentiality Master Key (MK_{SMC})	Y	Y	No impact.
AC Master Key (MK_{AC})	Y	Y	No impact.
CFDC_limit for Integrity Session Key	N	Y	New data element.
CFDC_limit for Confidentiality Session Key	N	Y	New data element.
CFDC_limit for AC Session Key	N	Y	New data element.
Length of ICC Public Key Modulus (N_{IC})	Y	Y	Maximum length increased to 128 bytes.
ICC Private Key	Y	Y	No impact.
Length of ICC PIN Encipherment Public Key Modulus (N_{PE})	O	O	Maximum length increased to 128 bytes.
ICC PIN Encipherment Private Key	O	O	No impact.
CRM Country Code	N	Y	New data element.
Key Derivation Index	Y	Y	No impact.
Application Life Cycle Data	N	Y	New data element.
Previous Transaction History	N	Y	New data element.
Application File Locator	Y	Y	The value of the *Application File Locator* depends on the method you choose for organizing data in your files. The maximum length increased to 32 bytes.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 247

Data Element	Select 2	Select 4	Migration Impact
Application Interchange Profile	Y	Y	New value for M/Chip Select 4.
PIN Try Limit	Y	Y	No impact.
PIN Try Counter	Y	Y	No impact.
Reference PIN	Y	Y	No impact.
Last Online Application Transaction Counter ('9F13')	Y	N	No longer used in M/Chip 4 Implementation.
Card TVR Action Code	Y	N	No longer used in M/Chip 4 Implementation.
Non-Domestic Control Factor	Y	N	No longer used in M/Chip 4 Implementation.
Maximum Offline Transaction Amount	Y	N	No longer used in M/Chip 4 Implementation.
Decline if Data Authentication Failed	Y	N	No longer used in M/Chip 4 Implementation.
DAC/ICC Present	Y	N	No longer used in M/Chip 4 Implementation.
Online Terminal Types	Y	N	No longer used in M/Chip 4 Implementation.
MCC and TCC Tables and Related Data	Y	N	No longer used in M/Chip 4 Implementation.
CDOL1 and CDOL2 Offsets	Y	N	No longer used in M/Chip 4 Implementation.
CDOL Data Lengths	Y	N	No longer used in M/Chip 4 Implementation.
CDOL1 and CDOL2 AC Truncation Lengths	Y	N	No longer used in M/Chip 4 Implementation.
PDOL and DDOL Lengths	Y	N	No longer used in M/Chip 4 Implementation.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 248

9 Migration from M/Chip Lite 4 to M/Chip Select 4

This chapter describes the migration of your authorization and clearing system from M/Chip Lite 4 to M/Chip Select 4.

9.1 Overview 9-1

9.2 Authorization Request and Clearing Data Handling 9-1

9.3 Online Interface 9-1

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 249

9.1 Overview

This chapter describes the differences between M/Chip Lite 4 and M/Chip Select 4 applications for you to consider when preparing your migration.

The following sections describes differences that impact your authorization and clearing systems, covering the following tasks:

- Handling the authorization request
- Preparing the authorization response
- Handling the clearing data

9.2 Authorization Request and Clearing Data Handling

These sections only consider the migration impact on the chip sub-elements in the ICC System Related Data (DE 55) data element. There are no differences for other data elements.

Table 9.1 summarizes the impacted sub-elements.

Table 9.1—Impacted Authorization and Clearing Sub-elements (DE 55) in Migration from M/Chip Lite 4 to M/Chip Select 4

Sub-Element	M/Chip Select 4 …..
Application Interchange Profile	Uses bits not used by M/Chip Lite 4.
ICC Dynamic Number	May replace the DAC in the *Issuer Application Data.*
Terminal Verification Results	Uses bits not used by M/Chip Lite 4.
Card Verification Results	Uses bits not used by M/Chip Lite 4.

None of the differences summarized in Table 9.1 impact the online interface.

9.3 Online Interface

The online interface for M/Chip Lite 4 and M/Chip Select 4 are almost identical. The only difference is that some values linked to the RSA capability are supported by the M/Chip Select 4 application but are not supported by the M/Chip Lite 4 application.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 250

A Data Dictionary

This appendix provides a dictionary of data element definitions.

A.1 Additional Check Table A-1

A.2 Application Control A-3

A.3 Application Interchange Profile A-6

A.4 Application Life Cycle Data A-7

A.5 Application Transaction Counter Limit A-9

A.6 ARPC Response Code A-10

A.7 Card Issuer Action Code—Decline, Default, Online A-12

A.8 CDOL 1 (Card Risk Management Data Object List 1) A-15

A.9 CDOL 1 Related Data Length A-17

A.10 CDOL 2 (Card Risk Management Data Object List 2) A-18

A.11 Consecutive Offline Transactions Number A-19

A.12 CRM Country Code A-19

A 13 CRM Currency Code A-20

A.14 Cryptogram Information Data A-20

A.15 Cryptogram Version Number A-21

A.16 Cumulative Offline Transaction Amount A-22

A.17 Currency Conversion Parameters A-23

A.18 Currency Conversion Table A-24

A.19 CVR (Card Verification Results) A-25

A.20 Default ARPC Response Code A-31

A.21 DDOL (Dynamic Data Authentication Data Object List) A-33

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 251

A.22 ICC Dynamic Number A-33
A.23 Issuer Action Code – Default, Denial, Online A-34
A.24 Issuer Application Data A-36
A.25 Issuer Authentication Data A-37
A.26 Key Derivation Index A-37
A.27 Lower Consecutive Offline Limit A-38
A.28 Lower Cumulative Offline Transaction Amount A-38
A.29 Log Format A-39
A.30 Offline Balance A-40
A.31 PIN Try Counter A-40
A.32 PIN Try Limit A-41
A.33 Previous Transaction History A-42
A.34 Script Counter A-43
A.35 Consecutive Offline Limit A-44
A.36 Cumulative Offline Transaction Amount A-44

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 252

A.1 Additional Check Table

Tag: 'D3'

Purpose: The *Additional Check Table* contains values that are compared to values given by the terminal in *CDOL 1 Related Data*. The result of the comparison is reflected in the decision-making part of the *Card Verification Results*.

The check with the *Additional Check Table* is only performed if the *Application Control [2][3]* is set to '1b' (Activate additional check table).

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 18 bytes, binary.

The *Additional Check Table* is the concatenation (without TLV coding) of the data elements identified in Table A.1.

Table A.1—Additional Check Table

Data Element		Length	Format
Position In CDOL 1 Related Data		1	binary
Length In CDOL 1 Related Data		1	binary
Number Of Entries		1	binary
Entries		15	binary
	Bit Mask	Length In CDOL 1 Related Data	binary
	Value 1	Length In CDOL 1 Related Data	binary
	…	…	…
	Value Number Of Entries - 1	*Length In CDOL 1 Related Data*	binary
	Padding	*15 – Number Of Entries * Length In CDOL 1 Related Data*	'FF ... FF'

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 253

Position in CDOL 1 Related Data

This data element contains the position of the portion of *CDOL 1 Related Data* that is compared to the table entries. The position of the first byte is 1.

Length in CDOL 1 Related Data

This data element contains the length of the portion of *CDOL 1 Related Data* that is compared to the table entries.

Number of Entries

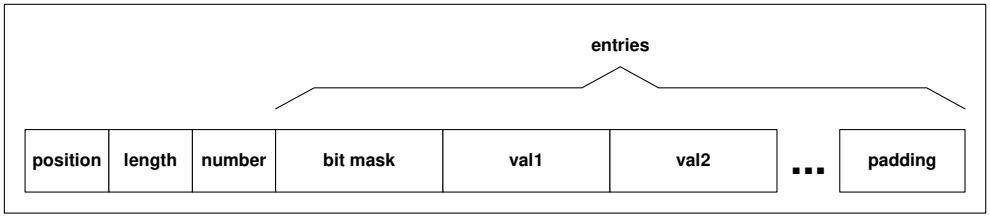
This data element contains the number of values (including the bit mask) in the *Additional Check Table* that are used for the comparison.

Entries

This data element contains the concatenation of the values used for the comparison, optionally padded with 'FF' to make up 15 bytes. The first value is used as a *bit mask*.

Table A.1 illustrates the *Additional Check Table*.

Figure A.1—Additional Check Table



© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 254

A.2 Application Control

Tag: 'D5'

Purpose: The *Application Control* activates or de-activates functions in the application. This activation or de-activation is dynamic: the *Application Control* can be modified with a **PUT DATA** during the application lifetime and in such a case, the behavior of the application is modified.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 2 bytes, binary.

Table A.2 describes the coding of the byte 1 of the Application Control for the M/Chip Select 4 application.

Table A.2—Application Control for M/Chip Select 4, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								Magstripe grade issuer activated
0								Magstripe grade issuer not activated
1								Magstripe grade issuer activated
	x							Skip CIAC-default on CAT3
	0							Do not skip CIAC-default on CAT3
	1							Skip CIAC-default on CAT3
		x						Reserved
		0						Other value RFU
			x					Key for offline encrypted PIN verification
			0					DDA key
			1					Dedicated key
				x				Offline encrypted PIN verification
				0				Not supported
				1				Supported
					x			Offline plaintext PIN verification
					0			Not supported
					1			Supported

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 255

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
						x		Session key derivation
						0		EPI/MCI
						1		EMV 2000
							x	Encrypt offline counters
							0	Do not encrypt offline counters
							1	Encrypt offline counters

Table A.3 describes the coding for byte 1 of the *Application Control* for the M/Chip Lite 4 application.

Table A.3—Application Control for M/Chip Lite 4, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								Magstripe grade issuer activated
0								Magstripe grade issuer not activated
1								Magstripe grade issuer activated
	x							Skip CIAC-default on CAT3
	0							Do not skip CIAC-default on CAT3
	1							Skip CIAC-default on CAT3
		x						Reserved
		0						Other value RFU
			x					Reserved
			0					Other value RFU
				x				Reserved
				0				Other value RFU
					x			Offline plaintext PIN verification
					0			Not supported
					1			Supported
						x		Session key derivation
						0		EPI/MCI
						1		EMV 2000
							x	Encrypt offline counters

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 256

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
							0	Do not encrypt offline counters
							1	Encrypt offline counters

Table A.4 describes the coding for byte 2 of the Application Control for the M/Chip Lite 4 and M/Chip Select 4 applications.

Table A.4—Application Control for M/Chip Lite 4 and M/Chip Select 4, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x				Reserved
0	0	0	0	0				Other values RFU
					x			Activate additional check table
					0			Do not activate additional check table
					1			Activate additional check table
						x		Allow retrieval of balance
						0		Do not allow retrieval of balance
						1		Allow retrieval of balance
							x	Include counters in AC
							0	Do not include counters in AC
							1	Include counters in AC

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 257

A.3 Application Interchange Profile

Tag: '82'

Purpose: The *Application Interchange Profile* indicates the capabilities of the card to support specific functions in the application.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 2 bytes, binary.

Table A.5 describes the coding for the first byte of the *Application Interchange Profile* for the M/Chip Select 4 application, supporting SDA, DDA and Combined DDA – Generate AC.

Table A.5—Application Interchange Profile for M/Chip 4 Select, Byte 1

b8	b7	b6	B5	b4	b3	b2	b1	Meaning
0								Reserved – no meaning
	1							Offline static data authentication is supported
		1						Offline Dynamic data authentication is supported
			1					Cardholder verification is supported
				1				Terminal risk management is to be performed
					0			Issuer authentication data is sent using the **EXTERNAL AUTHENTICATE** command
						0		Reserved – no meaning
							1	Combined DDA – **GENERATE AC** supported

Table A.6 describes the coding for the first byte of the *Application Interchange Profile* for the M/Chip Lite 4 application, supporting SDA.

Table A.6—Application Interchange Profile for M/Chip 4 Select, Byte 1

b8	b7	b6	b5	B4	b3	b2	b1	Meaning
0								Reserved – no meaning
	1							Offline static data authentication is supported
		0						Offline Dynamic data authentication is not supported
			1					Cardholder verification is supported

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 258

b8	b7	b6	b5	B4	b3	b2	b1	Meaning
				1				Terminal risk management is to be performed
					0			Issuer authentication data is sent using the second **GENERATE AC** command
						0		Reserved – no meaning
							0	Combined DDA – GENERATE AC Is not supported

Table A.7 describes the coding for the first byte of the Application Interchange Profile for the M/Chip Lite 4 application, supporting SDA.

Table A.7—Application Interchange Profile for M/Chip 4 Select and M/Chip Lite 4, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
0	0	0	0	0	0	0	0	Reserved – no meaning

A.4 Application Life Cycle Data

Tag: '9F7E'

Purpose: The purpose of the *Application Life Cycle Data* is to uniquely identify the application code and the application issuer.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 48 bytes, organized in four data elements:

- The first byte is version number, with value '00' for M/Chip Lite 4 and '01' for M/Chip Select 4.
- The next seven bytes are for Type Approval identification code.
- The next 20 bytes are reserved for the application issuer identification, format and content are application issuer-specific.
- The last 20 bytes are reserved for the application code identification, format and content are implementation-specific.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 259

Table A.8—Application Life Cycle DataEnter Caption Text

Data Element	Length	Format
Version Number	1	'00' for M/Chip Lite 4 '01' for M/Chip Select 4.
Type Approval ID	7	binary
Application Issuer ID	20	binary
Application Code ID	20	binary

The seven bytes reserved for the *Type Approval ID* contain an identifier given by MasterCard when the application passes the Type Approval process.

Twenty bytes are reserved to identify the application issuer, which is usually the card issuer. Using this value, the issuer should be able to identify the personalizer and the personalization batch.

The last 20 bytes are used to uniquely identify the application code. This identifier supports differentiation between different application behavior. Typically, this data element contains the identifier of the application provider and the identifier of the application code. It is the responsibility of the application provider to ensure that this data element always differentiates between the two different application behaviors. The easiest way to implement this feature is to modify the value of this data element, each time there is a modification to the following:

- Application (version identifier)
- Application code (release identifier)
- Platform on which the application is actually running (e.g. virtual machine version x or y)
- Hardware on which the platform or the application is actually running

The way in which these data elements are stored in the application is left to the implementation. The last data element may be coded in the application itself (i.e. in the code) whilst the others are set as part of personalization.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 260

A.5 Application Transaction Counter Limit

Tag: None.

Purpose: The *Application Transaction Counter Limit* limits the number of transactions processed by the application. When the *Application Transaction Counter* reaches the *Application Transaction Counter Limit*, the application will no longer process transactions.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 2 bytes, binary.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 261

A.6 ARPC Response Code

Tag: None.

Purpose: The *ARPC Response Code* informs the application about the actions that you decide upon. The *ARPC Response Code* is sent to the application in the *Issuer Authentication Data* (last two bytes). It replaces the *Issuer Authentication Response Code* in previous versions of *EPI/MCI Implementation Specifications for Debit and Credit.*

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 2 bytes, binary.

Table A.9 describes the content of byte 1 of the ARPC Response Code.

Table A.9—ARPC Response Code, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Reserved
0	0	0	0					Other value RFU
				x	x	x	x	*PIN Try Counter*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 262

Table A.10 describes the content of byte 2 of the ARPC Response Code.

Table A.10—ARPC Response Code, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x						Reserved
0	0	0						Other value RFU
			x					Approve online transaction
			0					Do not approve online transaction
			1					Approve online transaction
				x				Update *PIN Try Counter*
				0				Do not update *PIN Try Counter*
				1				Update *PIN Try Counter*
					x			Set go online on next transaction
					0			Reset go online on next transaction
					1			Set go online on next transaction
						x	x	Update counters
						0	0	Do not update offline counters
						1	0	Reset counters to zero
						0	1	Set counters to upper offline limits
						1	1	Add transaction to counter

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 263

A.7 Card Issuer Action Code—Decline, Default, Online

Tag: *Card Issuer Action Code—Decline*: 'C3'.

Card Issuer Action Code—Default: 'C4'.

Card Issuer Action Code—Online: 'C5'.

Purpose: The M/Chip 4 application compares the *Card Issuer Action Codes* with the decisional part of the *Card Verification Results* to take decisions.

You use the *Card Issuer Action Code—Decline* to set the situations when a transaction is always declined at the first **GENERATE AC**.

You use the *Card Issuer Action Code—Online* to set the situations when a transaction goes online if the terminal is online capable.

You use the *Card Issuer Action Code—Default* to set the situations when a transaction is declined if the terminal is not online capable or if the terminal cannot connection to your host.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 3 bytes, binary. The three bytes have the format provided in Table A.11, Table A.12, and Table A.12.

Table A.11 describes the content of byte 1. Byte 1 contains information for the current transaction.

Table A.11—Card Issuer Action Code, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								*Reserved-No Meaning*
	x							*Unable To Go Online Indicated*
	0							*Do Not Take Action If Unable To Go Online Indicated*
	1							*Take Action If Unable To Go Online Indicated*
		x						*Offline PIN Verification Not Performed*
		0						*Do Not Take Action If Offline PIN Verification Not Performed*
		1						*Take Action If Offline PIN Verification Not Performed*
			x					*Offline PIN Verification Failed*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 264

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
			0					*Do Not Take Action If Offline PIN Verification Failed*
			1					*Take Action If Offline PIN Verification Failed*
				x				*PTL Exceeded*
				0				*Do Not Take Action If PTL Exceeded*
				1				*Take Action If PTL Exceeded*
					x			*International Transaction*
					0			*Do Not Take Action If International Transaction*
					1			*Take Action If International Transaction*
						x		*Domestic Transaction*
						0		*Do Not Take Action If Domestic Transaction*
						1		*Take Action If Domestic Transaction*
							x	*Terminal Erroneously Considers Offline PIN OK*
							0	*Do Not Take Action If Terminal Erroneously Considers Offline PIN OK*
							1	*Take Action If Terminal Erroneously Considers Offline PIN OK*

Table A.12 describes the content of byte 2. Byte 2 contains information from the current transaction and from the transaction that preceded it (i.e. current transaction – 1).

Table A.12—Card Issuer Action Code, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								*Lower Consecutive Offline Limit Exceeded*
0								*Do Not Take Action If Lower Consecutive Offline Limit Exceeded*
1								*Take Action If Lower Consecutive Offline Limit Exceeded*
	x							*Upper Consecutive Offline Limit Exceeded*
	0							*Do Not Take Action If Upper Consecutive Offline Limit Exceeded*
	1							*Take Action If Upper Consecutive Offline Limit Exceeded*
		x						*Lower Cumulative Offline Limit Exceeded*
		0						*Do Not Take Action If Lower Cumulative Offline Limit Exceeded*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 265

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
		1						*Take Action If Lower Cumulative Offline Limit Exceeded*
			x					*Upper Cumulative Offline Limit Exceeded*
			0					*Do Not Take Action If Upper Cumulative Offline Limit Exceeded*
			1					*Take Action If Upper Cumulative Offline Limit Exceeded*
				x				*Go Online On Next Transaction Was Set*
				0				*Do Not Take Action If Go Online On Next Transaction Was Set*
				1				*Take Action If Go Online On Next Transaction Was Set*
					x			*Issuer Authentication Failed*
					0			*Do Not Take Action If Issuer Authentication Failed*
					1			*Take Action If Issuer Authentication Failed*
						x		*Script Received*
						0		*Do Not Take Action If Script Received*
						1		*Take Action If Script Received*
							x	*Script Failed*
							0	*Do Not Take Action If Script Failed*
							1	*Take Action If Script Failed*

Table A.13 describes the content of byte 3. Byte 3 contains decision-making information from the current transaction.

Table A.13—Card Issuer Action Code, Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			*Reserved-No Meaning*
						x		*Match Found In Additional Check Table*
						0		*Do Not Take Action If Match Found In Additional Check Table*
						1		*Take Action If Match Found In Additional Check Table*
							x	*No Match Found In Additional Check Table*
							0	*Do Not Take Action If No Match Found In Additional Check Table*
							1	*Take Action If No Match Found In Additional Check Table*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 266

A.8 CDOL 1 (Card Risk Management Data Object List 1)

Tag: '8C'

Purpose: Tells the terminal what data is needed in the first **GENERATE AC**.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: Binary.

Table A.14 defines the initial content of the *CDOL 1* for the M/Chip Select 4 application.

Table A.14—CDOL 1 Initial Content for M/Chip Select 4

Data Element	Tag	Length
Amount, Authorised (Numeric)	'9F02'	6
Amount, Other (Numeric)	'9F03'	6
Terminal Country Code	'9F1A'	2
Terminal Verification Results	'95'	5
Transaction Currency Code	'5F2A'	2
Transaction Date	'9A'	3
Transaction Type	'9C'	1
Unpredictable Number	'9F37'	4
Terminal Type	'9F35'	1
Data Authentication Code	'9F45'	2
ICC Dynamic Number	'9F4C'	8
CVM Results	'9F34'	3
Total CDOL1 Length		43 bytes

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 267

Table A.15 defines the initial content of *CDOL 1* for the M/Chip Lite 4 application.

Table A.15—CDOL 1 Initial Content for M/Chip Lite 4

Data Element	Tag	Length
Amount, Authorised (Numeric)	'9F02'	6
Amount, Other (Numeric)	'9F03'	6
Terminal Country Code	'9F1A'	2
Terminal Verification Results	'95'	5
Transaction Currency Code	'5F2A'	2
Transaction Date	'9A'	3
Transaction Type	'9C'	1
Unpredictable Number	'9F37'	4
Terminal Type	'9F35'	1
Data Authentication Code	'9F45'	2
CVM Results	'9F34'	3
Total CDOL1 Length		35 bytes

The M/Chip Lite 4 and M/Chip Select 4 applications allow the extension of the *CDOL 1* with additional data elements, i.e. append new data elements to the *CDOL 1* initial content. The applications must support a minimum of ten additional bytes in the *CDOL 1 Related Data*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 268

A.9 CDOL 1 Related Data Length

Tag: 'C7'

Purpose: Length of *CDOL 1 Related Data*.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

If no extension to *CDOL 1 Related Data* is used, the *CDOL 1 Related Data Length* value is:

- '23' for M/Chip Lite 4
- '2B' for M/Chip Select 4.

Both applications allow the extension of this value by at least ten bytes. The personalization value for *CDOL 1 Related Data Length* must be consistent with the personalization value for *CDOL 1*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 269

A.10 CDOL 2 (Card Risk Management Data Object List 2)

Tag: '8D'

Purpose: Tells the terminal what data is needed in second **GENERATE AC**.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 29 bytes, binary for M/Chip Select 4.

17 bytes, binary for M/Chip Lite 4.

Table A.16 defines the content of *CDOL 2* for the M/Chip Select 4 application.

Table A.16—CDOL 2 content for M/Chip Select 4

Data Element	Tag	Length
Issuer Authentication Data	'91'	10
Authorisation Response Code	'8A'	2
Terminal Verification Results	'95'	5
Unpredictable Number	'9F37'	4
ICC Dynamic Number	'9F4C'	8

Table A.17 defines the content of the *CDOL 2* for the M/Chip Lite 4 application.

Table A.17—CDOL 2 Content for M/Chip Lite 4

Data Element	Tag	Length
Issuer Authentication Data	'91'	10
Authorisation Response Code	'8A'	2
Terminal Verification Results	'95'	5

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 270

A.11 Consecutive Offline Transactions Number

Tag: None.

Purpose: The *Consecutive Offline Transactions Number* represents the number of transactions accepted offline and which have not been cumulated in the *Cumulative Offline Transaction Amount.*

The offline counters are internally compared to the offline limits. If a counter has exceeded its lower or upper limit, the relevant CVR bit is set.

It is included in the *Issuer Application Data* in plaintext or encrypted.

Note that if you so decide, transactions that you approve online can also be cumulated in this counter.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

A.12 CRM Country Code

Tag: 'C8'

Purpose: The *CRM Country Code* is used to differentiate between domestic transactions (when the *CRM Country Code* matches the Terminal Country Code) and international transactions (when the *CRM Country Code* does not match the *Terminal Country Code*). This may impact Card Risk Management, depending on the *Card Issuer Action Codes* settings.

Application: M/Chip Select 4 and the M/Chip Lite 4.

Format: Same as *Terminal Country Code.* 2 bytes.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 271

A 13 CRM Currency Code

Tag: 'C9'

Purpose: The *CRM Currency Code* is the currency of the *Cumulative Offline Transaction Amount*.

Application: M/Chip Select 4 and the M/Chip Lite 4.

Format: Same as *Currency Code*. 2 bytes.

A.14 Cryptogram Information Data

Tag: '9F27'

Purpose: The *Cryptogram Information Data* is returned in the response to the **GENERATE AC** command. M/Chip Select 4 and M/Chip Lite 4 application will only fill in bits 7 – 8 of *CID*, the remaining bits are no longer supported.

The *CID* values are:

'00' AAC

'40' TC

'80' ARQC.

Application M/Chip Select 4 and the M/Chip Lite 4.

Format: 1 byte, binary.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 272

A.15 Cryptogram Version Number

Tag: None.

Purpose: The *Cryptogram Version Number* informs you about the algorithm and data used for the Application Cryptogram computation during online transactions (in the authorization request) and after transaction completion in the clearing record.

Application M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

Table A.18 describes the coding for the *Cryptogram Version Number*.

Table A.18—Cryptogram Version Number

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Cryptogram version
0	0	0	1					4, other values RFU
				x	x			Reserved
				0	0			Other value RFU
						x		Session key used for AC computation
						0		EPI/MCI session key
						1		EMV2000 session key
							x	Counters included in AC computation
							0	Counters not included in AC data
							1	Counters included in AC data

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 273

A.16 Cumulative Offline Transaction Amount

Tag: None.

Purpose: The *Cumulative Offline Transaction Amount* represents the cumulative amount of transactions accepted offline. Transactions can be cumulated if they are in the counter currency or if they are in a currency that can be converted into the counter currency by the application.

The offline counters are internally compared to the offline limits. If a counter has exceeded its lower or upper limit, a specific action can be triggered.

It is included in the *Issuer Application Data* in plaintext or encrypted.

Note that if you so decide, transactions that you approve online can also be cumulated in this counter.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 12 numeric.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 274

A.17 Currency Conversion Parameters

Tag: None.

Purpose: Used to convert transactions in recognized currencies into transactions in the counter currency.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 5 bytes. Refer to Table A.19.

Table A.19—Currency Conversion Parameters

Position	Data	Length	Value
byte 1-2	*Currency Code*	2	Issuer-specific
byte 3-4	*Conversion Rate*	2	Decimal, BCD coding of multiplication factor
byte 5	*Conversion Exponent*	1	Binary coding of 10-power (most significant bit is the sign)

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 275

A.18 Currency Conversion Table

Tag: 'D1'

Purpose: The *currency conversion table* is used to convert transactions in recognized currencies into transactions in the counter currency.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 25 bytes. Refer to Table A.20.

Table A.20—Currency Conversion Table

Data Element	Length
Currency Conversion Table	25
Currency Conversion Parameters 1	5
Currency Conversion Parameters 2	5
Currency Conversion Parameters 3	5
Currency Conversion Parameters 4	5
Currency Conversion Parameters 5	5

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 276

A.19 CVR (Card Verification Results)

Tag: '9F52'

Purpose: The purpose of the *Card Verification Results* is twofold:

- To inform you about the "context" of a transaction, as part of the *Issuer Application Data*
- To take the decision on your behalf to accept a transaction offline, go online to the issuer for a transaction, or decline a transaction.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: Six bytes, binary. See below for format.

The first three bytes of the *Card Verification Results* are used for information only.

Bytes 4 to 6 are used for information and decision-making. They are checked against the *Card Issuer Action Code—Decline*, *Card Issuer Action Code—Online* and *Card Issuer Action Code—Default* during Card Risk Management.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 277

Table A.21 describes the content of byte 1. This is the most significant byte. Byte 1 does not contain decision-making information.

Table A.21—Card Verification Results, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							AC Returned in Second Generate AC
0	0							AAC
0	1							TC
1	0							Not requested
1	1							RFU
		x	x					AC Returned in First Generate AC
		0	0					*AAC*
		0	1					TC
		1	0					ARQC
		1	1					RFU
				x				Reserved
				0				Other value RFU
					x			Offline PIN Verification Performed
					0			Offline PIN Verification Not Performed
					1			Offline PIN Verification Performed
						x		Offline Encrypted PIN Verification Performed
						0		Offline Encrypted PIN Verification Not Performed
						1		• M/Chip Select 4: Offline Encrypted PIN Verification Performed • M/Chip Lite 4: Value Not Allowed
							x	Offline PIN Verification Successful
							0	Offline PIN Verification Not Successful
							1	Offline PIN Verification Successful

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 278

Table A.22 describes the content of byte 2. Byte 2 does not contain decision-making information.

Table A.22—Card Verification Results, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								DDA Returned
0								DDA Not Returned
1								• M/Chip Select 4: DDA Returned • M/Chip Lite 4: Value Not Allowed
	x							Combined DDA/AC Generation Returned In First Generate AC
	0							Combined DDA/AC Generation Not Returned In First Generate AC
	1							• M/Chip Select 4: Combined DDA/AC Generation Returned In First Generate AC • M/Chip Lite 4: Value Not Allowed
		x						Combined DDA/AC Generation Returned In Second Generate AC
		0						Combined DDA/AC Generation Not Returned In Second Generate AC
		1						• M/Chip Select 4: Combined DDA/AC Generation Returned In Second Generate AC • M/Chip Lite 4: Value Not Allowed
			x					Issuer Authentication Performed [a]
			0					Issuer Authentication Not Performed
			1					Issuer Authentication Performed
				x				CIAC-Default Skipped On CAT3
				0				No CIAC-Default Skipped On CAT3
				1				CIAC-Default Skipped On CAT3
					x	x	x	Reserved
					0	0	0	All other values RFU

[a] Successful or unsuccessful.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 279

Table A.23 describes the content of byte 3. Byte 3 does not contain decision-making information.

Table A.23—Card Verification Results, Byte 3

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Right nibble of *Script Counter*
				x	x	x	x	Right nibble of *PIN Try Counter*

Table A.24 describes the content of byte 4. Byte 4 contains decision-making information for the current transaction.

Table A.24—Card Verification Results, Byte 4

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								Reserved
0								Other Value RFU
	x							Unable To Go Online Indicated
	0							Unable To Go Online Not Indicated
	1							Unable To Go Online Indicated
		x						Offline PIN Verification Not Performed
		0						Offline PIN Verification Performed
		1						Offline PIN Verification Not Performed
			x					Offline PIN Verification Failed
			0					No Failure Of Offline PIN Verification
			1					Offline PIN Verification Failed
				x				*PTL* Exceeded
				0				*PTL* Not Exceeded
				1				*PTL* Exceeded
					x			International Transaction
					0			Domestic Transaction
					1			International Transaction
						x		Domestic Transaction
						0		International Transaction
						1		Domestic Transaction

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 280

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
							x	Terminal Erroneously Considers Offline PIN OK
							0	Terminal Does Not Erroneously Consider Offline PIN OK
							1	Terminal Erroneously Considers Offline PIN OK

Table A.25 describes the content of byte 5. Byte 5 contains decision-making information from the current transaction and from the transaction that preceded it (i.e. current transaction – 1).

Table A.25—Card Verification Results, Byte 5

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x								Lower Consecutive Offline Limit Exceeded
0								Lower Consecutive Offline Limit Not Exceeded
1								Lower Consecutive Offline Limit Exceeded
	x							Upper Consecutive Offline Limit Exceeded
	0							Upper Consecutive Offline Limit Not Exceeded
	1							Upper Consecutive Offline Limit Exceeded
		x						Lower Cumulative Offline Limit Exceeded
		0						Lower Cumulative Offline Limit Not Exceeded
		1						Lower Cumulative Offline Limit Exceeded
			x					Upper Cumulative Offline Limit Exceeded
			0					Upper Cumulative Offline Limit Not Exceeded
			1					Upper Cumulative Offline Limit Exceeded
				x				Go Online On Next Transaction Was Set [a]
				0				Go Online On Next Transaction Was Not Set
				1				Go Online On Next Transaction Was Set
					x			Issuer Authentication Failed [a]
					0			No Issuer Authentication Failed
					1			Issuer Authentication Failed
						x		Script Received [b]
						0		No Script Received
						1		Script Received
							x	Script Failed [b]

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 281

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
							0	No Script Failed
							1	Script Failed

a In this transaction or in a previous one.

b In a previous transaction.

Table A.26 describes the content of byte 6. Byte 6 contains decision-making information from the current transaction.

Table A.26—Card Verification Results, Byte 6

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x	x	x			Reserved
0	0	0	0	0	0			Other value RFU
						x		Match Found In Additional Check Table
						0		No Match Found In Additional Check Table
						1		Match Found In Additional Check Table
							x	No Match Found In Additional Check Table
							0	Match Found In Additional Check Table
							1	No Match Found In Additional Check Table

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 282

A.20 Default ARPC Response Code

Tag: 'D6'

Purpose: The *Default ARPC Response Code* replaces the *ARPC Response Code*:

If *Issuer Authentication Data* is not present in an online transaction

and the magstripe grade issuer mode is activated (i.e. *Application Control* [1][8] is set to '1b')

and the transaction is approved by the terminal and issuer (i.e. *Authorisation Response Code* < > 'Y3' or 'Z3' and the terminal requests a TC).

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 2 bytes, binary.

Table A.27 describes the content for byte 1 of the *Default ARPC Response Code*.

Table A.27—Default ARPC Response Code, Byte 1

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Reserved
0	0	0	0					Other value RFU
				x	x	x	x	*PIN Try Counter*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 283

Table A.28 describes the content for byte 2 of the *Default ARPC Response Code*.

Table A.28—Default ARPC Response Code, Byte 2

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x						Reserved
0	0	0						Other value RFU
			x					Approve online transaction
			0					Do not approve online transaction
			1					Approve online transaction
				X				Update *PIN Try Counter*
				0				Do not update *PIN Try Counter*
				1				Value not allowed.
					x			Set go online on next transaction
					0			Reset go online on next transaction
					1			Set go online on next transaction
						x	x	Update counters
						0	0	Do not update offline counters
						1	0	Reset counters to zero
						0	1	Set counters to upper offline limits
						1	1	Add transaction to counter

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 284

A.21 DDOL (Dynamic Data Authentication Data Object List)

Tag: '9F49'

Purpose: Tells the terminal what data is needed in first **INTERNAL AUTHENTICATE**.

Application: M/Chip Select 4.

Format: Variable up to 252 bytes, binary.

Table A.29 defines the content of the *DDOL* for the M/Chip Select 4 application.

Table A.29—DDOL Content

Data Element	Tag	Length
Unpredictable Number	'9F37'	4

A.22 ICC Dynamic Number

Tag: '9F4C'

Purpose: Time-variant number generated by the ICC, to be captured by the terminal

Application: M/Chip Select 4

Format: 8 bytes, binary.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 285

A.23 Issuer Action Code – Default, Denial, Online

Tag: *Issuer Action Code* – Default: '9F0D'

Issuer Action Code – Denial: '9F0E'

Issuer Action Code – Online: '9F0F'

Purpose: *Issuer Action Code* – Default specifies the conditions that you define that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online.

Issuer Action Code – Denial specifies the conditions that you define that cause the denial of a transaction without attempt to go online.

Issuer Action Code – Online specifies the conditions that you define that cause a transaction to be transmitted online.

Application: M/Chip Select 4 and M/Chip Lite 4

Format: 5 bytes, binary. Table A.30 provides the format.

Table A.30—Issuer Action Code – Default, Denial, Online for M/Chip Select 4

Byte	Bit	Meaning
1	8	Data authentication was not performed
	7	Offline static data authentication failed
	6	ICC data missing
	5	Card appears on terminal exception file
	4	Offline dynamic data authentication failed
	3	Combined DDA/AC generation failed
	2 – 1	RFU
2	8	Chip card and terminal have different application versions
	7	Expired application
	6	Application not yet effective
	5	Requested service not allowed for card product
	4	New card
	3 – 1	RFU

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 286

Byte	Bit	Meaning
3	8	Cardholder verification was not successful
	7	Unrecognized Cardholder Verification Method (CVM)
	6	PIN Try Limit exceeded
	5	PIN entry required but PIN pad not present/working
	4	PIN entry required, PIN pad present but PIN not entered
	3	Online PIN entered
	2 – 1	RFU
4	8	Transaction exceeds floor limit
	7	Lower consecutive offline limit exceeded
	6	Upper consecutive offline limit exceeded
	5	Transaction selected randomly for online processing
	4	Merchant forced transaction online
	3 – 1	RFU
5	8	Default TDOL used
	7	Issuer Authentication was unsuccessful
	6	Script processing failed before final **GENERATE AC**
	5	Script processing failed after final **GENERATE AC**
	4 – 1	RFU

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 287

A.24 Issuer Application Data

Tag: '9F10'

Purpose: The *Issuer Application Data* informs you about the application during online transactions (in the authorization request) and after transaction completion in the clearing record.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 18 bytes, binary.

For the M/Chip Select 4 application, the *Issuer Application Data* is the concatenation (without TLV coding) of the data elements identified in Table A.31.

Table A.31—Issuer Application Data for M/Chip Select 4

Data Element	Length
Key Derivation Index	1
Cryptogram Version Number	1
Card Verification Results	6
DAC/ICC Dynamic Number 2 Bytes	2
Plaintext/Encrypted Counters	8

For the M/Chip Lite 4 application, the Issuer Application Data is the concatenation (without TLV coding) of the data elements identified in Table A.32.

Table A.32—Issuer Application Data for M/Chip Lite 4

Data Element	Length
Key Derivation Index	1
Cryptogram Version Number	1
Card Verification Results	6
DAC	2
Plaintext/Encrypted Counters	8

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 288

A.25 Issuer Authentication Data

Tag: '91'

Purpose: The issuer computes the *Issuer Authentication Data* in an online transaction. It contains the issuer decision (in the *ARPC Response Code*) and a MAC on this decision.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 10 bytes, binary.

Table A.33 describes the coding for the *Issuer Authentication Data*.

Table A.33—Issuer Authentication Data

1	2	3	4	5	6	7	8	9	10	Meaning
x	x	x	x	x	x	x	x			*Authorisation Response Cryptogram*
								x	x	*ARPC Response Code*

A.26 Key Derivation Index

Tag: None.

Purpose: Issuer-specific.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 289

A.27 Lower Consecutive Offline Limit

Tag: '9F14'

Purpose: If the *Consecutive Offline Transactions Number* has exceeded this limit, the relevant CVR bit is set.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

A.28 Lower Cumulative Offline Transaction Amount

Tag: 'CA'.

Purpose: If the *Cumulative Offline Transaction Amount* has exceeded this limit, the relevant CVR bit is set.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 12 numeric.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 290

A.29 Log Format

Tag: '9F51'

Purpose: The *Log Format* identifies the content of records in the *Log Of Transactions*.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: The *Log Format* is coded like a DOL and is fixed for the M/Chip Lite 4 or M/Chip Select 4 application.

Table A.34 provides the data elements identified in the Log Format and the order in which they appear.

Table A.34—The Log Format

Tag	Data Element	Length
'9F27'	*Cryptogram Information Data*	1
'9F02'	*Amount, Authorised*	6
'5F2A'	*Transaction Currency Code*	2
'9A'	*Transaction Date*	3
'9F36'	*Application Transaction Counter*	2
'9F52'	*Card Verification Results*	6

The value of the *log format* is therefore:

'9F27019F02065F2A029A039F36029F5206'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 291

A.30 Offline Balance

Tag: '9F50'.

Purpose: The *Offline Balance* represents the amount of offline spending available.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 12 numeric.

The *Offline Balance* is retrievable by the **GET DATA**, if allowed by the *Application Control*, and is computed as follows:

Offline Balance = Upper Cumulative Offline Transaction Amount - Cumulative Offline Transaction Amount.

If *Upper Cumulative Offline Transaction Amount < Cumulative Offline Transaction Amount* the value returned by the **GET DATA** for the *Offline Balance* is 0 ('000000000000').

A.31 PIN Try Counter

Tag: '9F17'

Purpose: Indicates the number of PIN tries remaining.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

Table A.35 describes the coding for the *PIN Try Counter*.

Table A.35—PIN Try Counter Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Reserved
0	0	0	0					All Other Values RFU
				x	x	x	x	PTC (number of tries remaining)

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 292

A.32 PIN Try Limit

Tag: None.

Purpose: Indicates the number of PIN tries allowed.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

Table A.36 describes the coding for the *PIN Try Limit*.

Table A.36—PIN Try Limit Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					Reserved
0	0	0	0					All Other Values RFU
				x	x	x	x	PTL (number of tries allowed)

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 293

A.33 Previous Transaction History

Tag: None.

Purpose: The *Previous Transaction History* is used to store in non-volatile memory information about the previous transactions in Card Risk Management.

Application: M/Chip Select 4 and the M/Chip Lite 4.

Format: 1 byte, binary.

Table A.37 describes the coding for the *Previous Transaction History*.

Table A.37—Previous Transaction History Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x							Reserved
0	0							Other value RFU
		x						Application disabled
		0						Application is not disabled
		1						Application is disabled
			x					Application blocked
			0					Application is not blocked
			1					Application is blocked
				x				Go Online On Next Transaction
				0				Do Not Force Online On Next Transaction
				1				Go Online On Next Transaction
					x			Issuer Authentication Failed
					0			No Issuer Authentication Failed
					1			Issuer Authentication Failed
						x		Script Received
						0		No Script Received
						1		Script Received
							x	Script Failed
							0	No Script Failed

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 294

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
							1	Script Failed

A.34 Script Counter

Tag: None.

Purpose: Indicates the number of script commands processed previously. The right nibble is included in the information part of the *Card Verification Results*.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

Table A.38 describes the coding for the *Script Counter*.

Table A.38—Script Counter Coding

b8	b7	b6	b5	b4	b3	b2	b1	Meaning
x	x	x	x					*Reserved*
0	0	0	0					*All Other Values RFU*
				x	x	x	x	*Script Counter*

Only the right nibble of the *Script Counter* is used. The number of script commands is not limited to 15. The *Script Counter* is cyclic: '0F' + 1 = '00''.

The *Script Counter* is updated when a script command is processed, i.e.:

- **PUT DATA**
- **UPDATE RECORD**
- **PIN CHANGE/UNBLOCK**
- **APPLICATION BLOCK**
- **APPLICATION UNBLOCK.**

The *Script Counter* is reset:

If the transaction went online (i.e. if *Authorisation Response Code* < > Y3 **or** Z3)

- **and** *Issuer Authentication Data* is present

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 295

- **and** the *Authorisation Response Cryptogram* verification is successful

or if the transaction went online (i.e. if *Authorisation Response Code* < > Y3 or Z3)

- **and** *Issuer Authentication Data* is not present
- **and** the terminal requests a TC
- **and** the magstripe grade issuer mode is activated.

A.35 Consecutive Offline Limit

Tag: '9F23'

Purpose: If the *Consecutive Offline Transactions Number* has exceeded this limit, the relevant CVR bit is set.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 1 byte, binary.

A.36 Cumulative Offline Transaction Amount

Tag: 'CB'.

Purpose: If the *Cumulative Offline Transaction Amount* has exceeded this limit, the relevant CVR bit is set.

Application: M/Chip Select 4 and M/Chip Lite 4.

Format: 12 numeric.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 296

B Currency Conversion

This appendix describes the currency conversion process.

B.1 Currency Conversion Process B-1

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 297

B.1 Currency Conversion Process

By defining the content of the *Currency Conversion Table* and the *CRM Currency Code*, you can accumulate transactions in up to six currencies in the *Cumulative Offline Transaction Amount*. This applies to transactions:

- performed in the *Counter Currency*
- performed in the five currencies personalized in the *Currency Conversion Table*, described in Table B.1

Table B.1—Currency Conversion Table

Data Element	Length
Currency Conversion Table	25
Currency Conversion Parameter 1	5
Currency Conversion Parameter 2	5
Currency Conversion Parameter 3	5
Currency Conversion Parameter 4	5
Currency Conversion Parameter 5	5

To deactivate an entry in the *Currency Conversion Table*, the *CRM Currency Code* can be used as the *Currency Code* for this entry (first two bytes).

Table B.2 describes the *Currency Conversion Parameters*.

Table B.2—Currency Conversion Parameters

Position	Data	Length	Value
Byte 1 – 2	*Currency Code*	2	Issuer-specific
Byte 3 – 4	*Conversion Rate*	2	Decimal, BCD coding of multiplication factor
Byte 5	*Conversion Exponent*	1	Binary coding of 10-power (most significant bit is the sign)

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 298

Table B.3 provides an example of *Currency Conversion Parameter* values. The cumulative counter in this example is the USD (U.S. Dollar).

Table B.3—Currency Conversion Parameters

Conversion Parameter 1		Conversion Parameter 2	
Data	**Value**	**Data**	**Value**
JPY (Yen)	0392	GBP	0826
Rate: 1 JPY = 0.008 USD	0008	Rate: 1 GBP = 1.5 USD	0015
Conversion Exponent	83	*Conversion Exponent*	81

For Conversion Parameter 1 in Table B.3, the *Conversion Exponent* value of '83' is the equivalent of '1000 0011b' in binary representation. '8' indicates the sign, '3' indicates the 10 to the power of three.

An example of conversion using Conversion Parameter 1 is as follows:

Transaction amount is 55555 JPY: '000000055555'

Transaction currency code '0392'

Amount in Counter Currency = (000000055555 x 0008)/1000 = '000000000444'.

For Conversion Parameter 2 in Table B.3, the *Conversion Exponent* value of '81' is the equivalent of ' '1000 0001b' in binary representation. '8' indicates the sign, '1' indicates the 10 to the power of one.

An example of conversion using Conversion Parameter 2 is as follows:

Transaction amount is 125 GBP: '000000000125'

Transaction currency code '0826'

Amount in Counter Currency = (000000000125 x 0015)/10 = '000000000187'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 299

C Offline Counters Exception Processing

This chapter introduces how the M/Chip 4 application manages the offline counters.

C.1 Overview C-1

C.2 Cumulated Transactions Limit C-1

C.3 Consecutive Offline Transactions Limit C-1

C.4 How to Prohibit Offline Transactions Based on Transaction Currency ... C-2

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 300

C.1 Overview

This section describes some characteristics of the management of offline counters by the M/Chip 4 application.



Note **The settings for the *Card Issuer Action Codes* can be used to deactivate offline limits. If offline limits are deactivated, the M/Chip 4 application does not take any action when the limits are exceeded.**

C.2 Cumulated Transactions Limit

For cumulated transactions, the highest value that can be stored in the six bytes of the *Cumulative Offline Transaction Amount* (999999999999) represents a strict limit. The M/Chip 4 application rejects offline transactions that cause the '999999999999' limit to be exceeded.

Therefore, currencies cumulated in the *Cumulative Offline Transaction Amount* must be chosen so that the *Cumulative Offline Transaction Amount* will never exceed 999999999999. The value 99 … 99 represents an amount that is invalid. In the unlikely situation where the value 99 … 99 would represent a valid amount, the currency conversion of the transaction must be performed using a negative *Conversion Exponent*, to result in a valid value.

C.3 Consecutive Offline Transactions Limit

The M/Chip 4 application does not strictly apply the limit of 255 to the number of transactions counted in the *Consecutive Offline Transactions Number*. It does not reject offline transactions that would cause the '255' limit to be exceeded but leaves the value of the *Consecutive Offline Transactions Number* at '255'. Therefore, by setting the *Lower Consecutive Offline Limit* or *Upper Consecutive Offline Limit* to '255', the *Consecutive Offline Transactions Number* counter is effectively deactivated for all transactions that exceed this limit.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 301

C.4 How to Prohibit Offline Transactions Based on Transaction Currency

It is possible to prohibit offline transactions in currencies that are neither in the *Currency Conversion Table* nor in the *Counter Currency* by setting the following limits/values at personalization:

- *Lower Consecutive Offline Limit* to '00'
- *Card Issuer Action Code – Default* [1][7] to '1b' (Unable to go online indicated).

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 302

D Interpreting the Card Verification Results

This appendix describes how you interpret the Card Verification Results.

D.1 Interpreting the Card Verification Results D-1
D.1.1 Cryptogram TC in Response to First GENERATE AC D-1
D.1.2 Cryptogram ARQC in Response to First GENERATE AC D-5
D.1.3 Cryptogram TC in Response to Second GENERATE AC D-8

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 303

D.1 Interpreting the Card Verification Results

This appendix describes how to interpret the Card Verification Results in the following cases:

- *Card Verification Results* as part of *Issuer Application Data* in the response to the first **GENERATE AC**, when the cryptogram is a TC
- *Card Verification Results* as part of *Issuer Application Data* in the response to the first **GENERATE AC**, when the cryptogram is an ARQC
- *Card Verification Results* as part of *Issuer Application Data* in the response to the second **GENERATE AC**, when the cryptogram is a TC.

As there is no clearing record for an AAC, this section does not describe the case when the cryptogram is an AAC as the *Card Verification Results* are unlikely to be interpreted

D.1.1 Cryptogram TC in Response to First GENERATE AC

The tables in this section describes the Card Verification Results that are part of the *Issuer Application Data* in the response to first **GENERATE AC** when the cryptogram is a TC.

Table D.1 describes byte 1. Byte 1 is the most significant byte and does not contain decision-making information.

Table D.1—Card Verification Results Byte 1 Bit Setting for first GENERATE AC, Giving a TC

Bits	Setting
b8-b7	For first **GENERATE AC**, always set to '10b' (Second **GENERATE AC** not requested).
b6-b5	When a TC is returned in first **GENERATE AC**, set to '01b'.
b4	Always set to '0b'. Reserved for future use.
b3	If the *PIN* was presented (successfully or not) to the M/Chip 4 application for the current transaction, set to '1b', otherwise, set to '0b'.
b2	For M/Chip Select 4: If the last *PIN* presentation to the M/Chip Select 4 application (successful or not) was in encrypted form, for the current transaction, set to '1b', otherwise set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b1	If the last *PIN* presentation to the application was successful, for the current transaction (i.e. for the current value of the *Application Transaction Counter*), set to '1b', otherwise, set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 304

Table D.2 describes byte 2. Byte 2 does not contain decision-making information.

Table D.2—Card Verification Results Byte 2 Bit Setting for First GENERATE AC, Giving a TC

Bits	Setting
b8	For M/Chip Select 4: If DDA is returned, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b7	For M/Chip Select 4: If the TC was wrapped in the RSA signature for the first **GENERATE AC**, set to '1b', otherwise set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b6	For M/Chip Select 4: For first **GENERATE AC** (combined DDA/AC generation not returned in second **GENERATE AC**), set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b5	For first **GENERATE AC** (Issuer Authentication not performed), set to '0b'.
b4	If CIAC – Default skipped on a CAT LEVEL 3 terminal, set to '1b', otherwise, set to '0b'.
b3-b1	Always set to '000b'. Reserved for future use.

Table D.3 describes byte 3. Byte 3 does not contain decision-making information.

Table D.3—Card Verification Results Byte 3 Bit Setting for First GENERATE AC, Giving a TC

Bits	Setting
b8-5	For the first **GENERATE AC**, the left nibble represents the number of script commands sent to the M/Chip 4 application since the Script Counter was last reset. The initial value of the *Script Counter* is set at personalization. It is usually set to '00'.
b4-1	The number of PIN tries remaining.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 305

Table D.4 describes byte 4. Byte 4 contains decision-making information for the current transaction.

Table D.4—Card Verification Results Byte 4 Bit Setting for First GENERATE AC, Giving a TC

Bits	Setting
b8	Always set to '0b'. Reserved for future use.
b7	For first **GENERATE AC** (Unable to go online not indicated), always set to '0b'.
b6	If offline PIN verification is not performed for the current transaction, set to '1b', otherwise, set to '0b'.
b5	If the last offline PIN verification performed unsuccessfully for the current transaction, set to '1b', otherwise, set to '0b'.
b4	If the *PIN Try Counter* = '00', set to '1b', otherwise, set to '0b'.
b3	For international transactions, set to '1b', otherwise, set to '0b'.
b2	For domestic transactions, set to '1b', otherwise, set to '0b'.
b1	If the terminal erroneously considers the offline PIN OK, set to '1b', otherwise, set to '0b'.

Table D.5 describes byte 5. Byte 5 contains decision-making information for the current and last online transaction.

Table D.5—Card Verification Results Byte 5 Bit Setting for First GENERATE AC, Giving a TC

Bits	Setting
b8	If the *Consecutive Offline Transactions Number* [a] > *Lower Consecutive Offline Limit*, set to '1b', otherwise, set to '0b'.
b7	As for b8, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit*.
b6	If *Cumulative Offline Transaction Amount* [b] > *Lower Cumulative Offline Transaction Amount*, set to '1b' otherwise set to '0b'.
b5	As for b6, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit*.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 306

Bits	Setting
b4	The value set in last online transaction with online connection (when the *Authorisation Response Code* is neither equal to 'Y3' nor 'Z3') • and *Issuer Authentication Data* is present • and the *Authorisation Response Cryptogram* verification is successful • and *Set Go Online on Next Transaction* is set in the *ARPC Response Code*. Or the value that was set in last online transaction with online connection (when the Authorization Response Code is neither equal to 'Y3' nor 'Z3') • and *Issuer Authentication Data* is not present • and the terminal requests a TC • and the magstripe grade issuer mode is supported • and *Set Go Online On Next Transaction* is set in the *Default ARPC Response Code*.
b3	If Issuer Authentication failed in a previous transaction (i.e. *Issuer Authentication Data* was present but the cryptogram verification was unsuccessful), and the *Previous Transaction History* [3] c has yet to be reset, set to '1b', otherwise, set to '0b'.
b2	If a script command was previously sent to the M/Chip 4 application, and the *Previous Transaction History* [2] [d] has yet to be reset, set to '1b', otherwise, set to '0b'.
b1	If a script command was previously sent to the M/Chip 4 application and has failed, and the *Previous Transaction History* [1] [e] has yet to be reset, set to '1b', otherwise, set to '0b'.

a Including this transaction, if not cumulated in the amount.

b Including this transaction, if cumulated in the amount.

c *Issuer Authentication Failed on Online Transaction*

d *Script on Online Transaction*.

e *Script Failed on Online Transaction*.

Table D.6 describes byte 6. Byte 6 contains decision-making information for the current transaction.

Table D.6—Card Verification Results Byte 6 Bit Setting for First GENERATE AC, Giving a TC

Bits	Setting
b8-3	Always '000000b'.
b2	If a match was found performing the tests identified in the additional check table, set to '1b', otherwise, set to '0b'.
b1	If no match was found performing the tests identified in the additional check table, set to '1b', otherwise, set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 307

D.1.2 Cryptogram ARQC in Response to First GENERATE AC

The tables in this section describe the *Card Verification Results* that are part of the *Issuer Application Data* in the response to the first **GENERATE AC** when the Cryptogram is an ARQC.

Table D.7 describes byte 1. Byte 1 is the most significant byte and does not contain decision-making information.

Table D.7—Card Verification Results Byte 1 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8-b7	For first **GENERATE AC**, always set to '10b' (Second **GENERATE AC** not requested).
b6-b5	When an ARQC is returned in first **GENERATE AC**, set to '10b'.
b4	Always set to '0b'. Reserved for future use.
b3	If the *PIN* for the current transaction was presented (successfully or not) to the M/Chip 4 application, set to '1b', otherwise, set to '0b'.
b2	For M/Chip Select 4: If the last *PIN* presentation to the application (successful or not) for the current transaction was in encrypted form, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4 Always set to '0b'.
b1	If the last *PIN* presentation to the application for the current transaction was successful, i.e. for the current value of the *Application Transaction Counter*, set to '1b', otherwise, set to '0b'.

Table D.8 describes byte 2. Byte 2 does not contain decision-making information.

Table D.8—Card Verification Results Byte 2 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8	For M/Chip Select 4: If DDA is performed, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b7	For M/Chip Select 4: If the ARQC was wrapped in the RSA signature for the first **GENERATE AC**, set to '1b' otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 308

Bits	Setting
b6	For first **GENERATE AC** (combined DDA/AC generation not returned in second **GENERATE AC**), always set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b5	For first **GENERATE AC** (Issuer Authentication not performed), always set to '0b'.
b4	Always set to '0b'. No ARQC on CAT level 3 terminal.
b3-b1	Always set to '000b'. Reserved for future use.

Table D.9 describes byte 3. Byte 3 does not contain decision-making information.

Table D.9—Card Verification Results Byte 3 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8-5	For the first **GENERATE AC**, the left nibble represents the number of script commands sent to the M/Chip 4 application since the *Script Counter* was last reset. The initial value of the *Script Counter* is set at personalization. It is usually set to '00'.
b4-1	The number of PIN tries remaining.

Table D.10 describes byte 4. Byte 4 contains decision-making information for the current transaction.

Table D.10—Card Verification Results Byte 4 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8	Always set to '0b'. Reserved for future use.
b7	For first **GENERATE AC** (Unable to go online not indicated), always set to '0b'.
b6	If offline PIN verification is not performed for the current transaction, set to '1b' otherwise, set to '0b'.
b5	If the last offline PIN verification was performed unsuccessfully for the current transaction, set to '1b' otherwise, set to '0b'.
b4	If the *PIN Try Counter* has value '00', set to '1b', otherwise, set to '0b'.
b3	For international transactions, set to '1b', otherwise, set to '0b'.
b2	For domestic transactions, set to '1b', otherwise, set to '0b'.
b1	If the terminal erroneously considers the offline PIN OK, set to '1b', otherwise, set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 309

Table D.11 describes byte 5. Byte 5 contains decision-making information for the current and last online transaction.

Table D.11—Card Verification Results Byte 5 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8	If the *Consecutive Offline Transactions Number* [a] > *Lower Consecutive Offline Limit*, set to '1b', otherwise set to '0b'.
b7	As for b8, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit.*
b6	If the *Cumulative Offline Transaction Amount* [b] > *Lower Cumulative Offline Transaction Amount,* set to '1b', otherwise set to '0b'.
b5	As for b6, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit.*
b4	The value set in last online transaction with online connection (if *Authorization Response Code* is neither equal to 'Y3' nor 'Z3') • and *Issuer Authentication Data* is present • and the *Authorization Response Cryptogram* verification is successful • and *Set Go Online on Next Transaction* is set in the *ARPC Response Code.* Or the value that was set in last online transaction with online connection (if Authorization Response Code is neither equal to 'Y3' nor 'Z3') • and *Issuer Authentication Data* is not present • and the terminal requests a TC • and the magstripe grade issuer mode is supported • and *Set Go Online on Next Transaction* is set in the *Default ARPC Response Code.*
b3	If Issuer Authentication has failed in a previous transaction (i.e. *Issuer Authentication Data* was present but the cryptogram verification was not successful), and the *Previous Transaction History* 3] [c] has yet to be reset, set to '1b', otherwise, set to '0b'.
b2	If a script command was previously sent to the M/Chip 4 application, and the *Previous Transaction History* [2] [d] has yet to be reset, set to '1b', otherwise, set to '0b'.
b1	If a script command was previously sent to the M/Chip 4 application and has failed, and the *Previous Transaction History* [1] [e] has yet to be reset, set to '1b', otherwise set to '0b'.

[a] Including this transaction, if not cumulated in the amount.

[b] Including this transaction, if cumulated in the amount

[c] *Issuer Authentication Failed on Online Transaction.*

[d] *Script on Online Transaction.*

[e] *Script Failed on Online Transaction.*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 310

Table D.12 describes byte 6. Byte 6 contains decision-making information for the current transaction.

Table D.12—Card Verification Results Byte 6 Bit Setting for First GENERATE AC, Giving an ARQC

Bits	Setting
b8-3	Always set to '000000b'.
b2	If a match was found performing the tests identified in the additional check table, set to '1b', otherwise, set to '0b'.
b1	If no match was found performing the tests identified in the additional check table, set to '1b', otherwise set to '0b'.

D.1.3 Cryptogram TC in Response to Second GENERATE AC

The tables in this section describes the *Card Verification Results* that are part of the *Issuer Application Data* in the response to the second **GENERATE AC** when the cryptogram is a TC.

Table D.13 describes byte 1. Byte 1 does not contain decision-making information.

Table D.13—Card Verification Results Byte 1 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8-b7	When a TC returned in the second **GENERATE AC**, set to '01b'.
b6-b5	When an ARQC returned in the first **GENERATE AC**, set to '10b'.
b4	Always set to '0b'. Reserved for future use.
b3	If the *PIN* for the current transaction was presented (successfully or not) to the M/Chip 4 application, set to '1b', otherwise, set to '0b'.
b2	For M/Chip Select 4: If the last PIN presentation to the M/Chip 4 application (successful or not) for the current transaction was in encrypted form, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b1	If the last *PIN* presentation to the application for the current transaction was successful, i.e. for the current value of the *Application Transaction Counter*, set to '1b', otherwise, set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 311

Table D.14 describes byte 2. Byte 2 does not contain decision-making information.

Table D.14—Card Verification Results Byte 2 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8	For M/Chip Select 4: If DDA is performed, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b7	For M/Chip Select 4: If the ARQC was wrapped in the RSA signature for the first **GENERATE AC**, set to '1b', otherwise, set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b6	For M/Chip Select 4: If the TC is wrapped in the RSA signature for the second **GENERATE AC**, set to '1b', otherwise set to '0b'. For M/Chip Lite 4: Always set to '0b'.
b5	If the *Issuer Authentication Data* is present for the current transaction, set to '1b', otherwise set to '0b'.
b4	For second **GENERATE AC** (CIAC – Default skipped on CAT3), always set to '0b'.
b3-b1	Always set to '000b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 312

Table D.15 describes byte 3. Byte 3 does not contain decision-making information.

Table D.15—Card Verification Results Byte 3 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8-5	The *Script Counter* is reset to '0000b' in either of the following situations: • When Issuer Authentication is successful • When the Magstripe grade issuer mode is supported and the Authorization Response Code is neither equal to 'Y3' nor 'Z3' (Unable to go online). The *Script Counter* is not reset and contains the same value as in the first **GENERATE AC** response in any of the following situations: • When Issuer Authorization failed in the current transaction • When the Magstripe grade issuer mode is not supported • When the Authorization Response Code is 'Unable to go online ('Y3' or 'Z3')
b4-1	The number of PIN tries remaining. (This is the same value as for the first **GENERATE AC** except if you have updated the value with a specific setting in the *ARPC Response Code*).

Table D.16 describes byte 4. Byte 4 contains decision-making information for the current transaction.

Table D.16—Card Verification Results Byte 4 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8	Always set to '0b'. Reserved for future use.
b7	If the terminal could not go online to the issuer (i.e. if *Authorization Response Code* = Y3 or Z3) for the current transaction, set to '1b', otherwise set to '0b'.
b6	If offline PIN verification is not performed for the current transaction, set to '1b', otherwise set to '0b'.
b5	If the last offline PIN verification was performed unsuccessfully for the current transaction, set to '1b', otherwise set to '0b'.
b4	If the *PIN Try Counter* has value '00', set to '1b', otherwise set to '0b'.
b3	For international transactions, set to '1b', otherwise, set to '0b'.
b2	For domestic transactions, set to '1b', otherwise set to '0b'.
b1	If the terminal erroneously considers offline PIN OK, set to '1b', otherwise set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 313

Table D.17 describes byte 5 contains decision-making information for the current and last online transaction.

Table D.17—Card Verification Results Byte 5 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8	If the *Consecutive Offline Transactions Number* [a] > *Lower Consecutive Offline Limit*, set to '1b', otherwise set to '0b'.
b7	As for b8, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit*.
b6	If *Cumulative Offline Transaction Amount* [b] > *Lower Cumulative Offline Transaction Amount*, set to '1b', otherwise, set to '0b'.
b5	As for b6, but using *Upper Consecutive Offline Limit* in place of *Lower Consecutive Limit*.
b4	**If unable to go online** (i.e. the *Authorization Response Code* = 'Y3' or 'Z3'), contains the same value as for the first **GENERATE AC**. **If able to go online** (i.e. the *Authorization Response Code* is not equal to 'Y3' or 'Z3'), set to reflect your decision, i.e. the value of the *Set Go Online on Next Transaction* bit: • In the ARPC Response Code, if Issuer Authentication Data is present • In the Default ARPC Response Code, if Issuer Authentication Data is not present
b3	If the Issuer Authentication failed in the current transaction or in a previous transaction (i.e. *Issuer Authentication Data* was present but the cryptogram verification was not successful), and the *Previous Transaction History* [3] [c] has yet to be reset, set to '1b', otherwise set to '0b'.
b2	If a script command was previously sent to the application, and the *Previous Transaction History* [2] [d] has not been reset, set to '1b', otherwise, set to '0b'.
b1	If a script command was previously sent to the application and failed, and the *Previous Transaction History* [1] [e] has not been reset, set to '1b', otherwise, set to '0b'.

a Including this transaction, if not cumulated in the amount.

b Including this transaction, if cumulated in the amount

c *Issuer Authentication Failed on Online Transaction.*

d *Script on Online Transaction.*

e *Script Failed on Online Transaction.*

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 314

Table D.18 describes byte 6. Byte 6 contains decision-making information for the current transaction.

Table D.18—Card Verification Results Byte 6 Bit Setting for Second GENERATE AC, Giving a TC

Bits	Setting
b8-3	Always '000000b'. Reserved for future use.
b2	If match found performing the tests identified in the additional check table, set to '1b', otherwise set to '0b'.
b1	If no match found performing the tests identified in the additional check table, set to '1b', otherwise set to '0b'.

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 315

E Non-critical Script Data Examples

This appendix provides examples of non-critical script data.

E.1 Examples E-1
E.1.1 Example 1 ..... E-1
E.1.2 Example 2 ..... E-2

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 316

E.1 Examples

This appendix provides two examples of the *Issuer Script Data* – non-critical script, Tag '72'.

E.1.1 Example 1

This example uses the **PUT DATA** command to update the *Card Issuer Action Code – Decline*, Tag 'C3' to '00 00 00'.

String of eight btye data blocks to be used for MAC calculation: '04 DA 00 C3 0B 00 0A AA BB CC DD EE FF 99 88 00 00 00 80 00 00 00 00 00'

CLA = 04

INS = DA

P1 = 00

P2 = C3

Lc = 0B

ATC = 00 0A

RAND = AA BB CC DD EE FF 99 88

Plaintext Data = 00 00 00

Padding = 80 00 00 00 00 00

Using the above string of data, the calculated MAC = 21 5B 54 FA F6 88 2D 10

When sent as non-critical script, the issuer script message would be:

Issuer Script Data "7212861004DA00C30B000000215B54FAF6882D10"

Description: Tag('72') + length('12')
+ Issuer Script Command Tag('86')
+ length('10')
+ ADPU & Data(04 DA 00 C3 0B 00 00 00)
+ MAC('215B54FAF6882D10')

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 317

E.1.2 Example 2

This example shows a non-critical script to block an application.

String of eight-btye data blocks to be used for MAC calculation: '84 1E 00 00 08 00 05 A3 77 91 88 1B A6 97 E0 80'

CLA = 84

INS = 1E

P1 = 00

P2 = 00

Lc = 08

ATC = 00 05

RAND = A3 77 91 88 1B A6 97 E0

Padding = 80

Using the above string of data, the calculated MAC = 6B AA 5A 95 6E A7 E4 1C

When sent as non-critical script, the issuer script message would be:

Issuer Script Data 72 0F 86 0D 84 1E 00 00 08 6B AA 5A 95 6E A7 E4 1C

Description Tag('72') + length('0F')
+ Issuer Script Command Tag('86')
+ length('0D')
+ ADPU(84 1E 00 00 08)
+ MAC('6BAA5A956EA7E41C')

© 2004 MasterCard International Incorporated

OV Loop Inc.
Ex. 2021 - Page 318