# ESTÁNDAR EMV FULL ATMS

**CLÁUSULA DE CONFIDENCIALIDAD 2011**

Este documento es propiedad de Promoción y Operación S.A. DE C.V. Y es para uso exclusivo de Promoción y Operación S.A. DE C.V. Bajo ninguna circunstancia deberá de entregarse el presente documento a cualquier individuo, proveedor o compañía no autorizados; ni se podrá reproducir parcial o totalmente sin el consentimiento expreso del área de Normatividad de Promoción y Operación S.A. DE C.V.

# Objetivo

El siguiente documento tiene el Objetivo de proporcionar los elementos necesarios para lograr que las transacciones financieras que contengan los elementos de EMV FULL entre los bancos de la Red, puedan realizarse sin ningún problema, así mismo contar con los elementos necesarios a fin de ser enviadas por el Host adquirente con Cajeros Automáticos (ATM) y recibidas por el Host Emisor de la tarjeta con Chip.

# Premisas y Alcance

1) Este documento contiene la estructura, descripción y operación de los tokens B's utilizados en la mensajería ISO8583 para transacciones de EMV FULL basado en el estándar de ISO internacional 8583:1987 con las variantes utilizadas en México.
2) Está dirigido a personal externo, desarrolladores y personal en general que requiera conocer la mensajería y estructura de lsa transacciones en EMV FULL para Cajeros Automáticos.
3) Este documento está basado en las normas mexicanas emitidas por la ABM y Banco de México, así como del apoyo de los manuales de EMV de Visa y Master Card.

# HISTORIAL

| Fecha | Versión |
|---|---|
| 13.Agosto.2012 | 4.0 |
| 20.Febrero.2013 | 4.1 |
| 13.Febrero.2015 | 5.1 |

# CONTROL DE CAMBIOS

| Descripción del Cambio | Versión | Solicitante del Cambio | Fecha de Actualización |
|---|---|---|---|
| • Se adiciona para el Token BJ su estructura así como en que tipo de transacciones irá se ajusta en el descriptivo del Token la parte indicar en que mensajes se enviaran respuestas. | 4.0 | Estándares Switch | Ago 2012 |
| • Se adiciona los descriptivos a los campos de EMV | 4.1 | Estándares Switch | Feb 2013 |
| • Actualización de logotipo empresarial.<br>• Integración de gráficos para su mejor entendimiento.<br>• Se detalla funcionamiento del token B4 para su mejor entendimiento acorde al cumplimiento con los documentos emitidos por la ABM “Directrices estándar para el intercambio de indicadores EMV en transacciones de Cajeros Automáticos”. | 5.1 | Estándares Switch | Feb 2015 |

# TABLA DE APROBACIÓN

| Nivel | Nombre | Fecha de Actualización |
|---|---|---|
| Elaboración | Beatriz Elena Huesca Guevara | Feb 2015 |
| Aprobación | Claudio Copérnico Ávila Luna | |

# ÍNDICE

# Capítulo 1: INTRODUCCIÓN

Este documento proporciona información acerca del uso y descripción de los tokens B's que son utilizados en las transacciones de EMV de la mensajería ISO8583:1987 utilizada en México.

## 1.1 Convenciones utilizadas en este manual

En esta sección se describe los acuerdos para la utilización de caracteres y formatos especiales.

⚠ El documento, se describe en 2 idiomas **Español e Inglés.** La parte correspondiente al idioma Ingles contiene los descriptivos internos de los mensajes respetando así la interpretación original de estos.

Formato: Los valores usados para representar los atributos de los elementos de datos se describen a continuación

| | |
|---|---|
| A | = Caracteres Alfabéticos |
| N | = Caracteres Numéricos |
| S | = Caracteres Especiales |
| AN | = Caracteres Alfabéticos y Numéricos |
| AS | = Caracteres Alfabéticos y Especiales |
| NS | = Caracteres Numéricos y Especiales |
| ANS | = Caracteres Alfabéticos, Numéricos y Especiales |

El formato utilizado para representar la fecha así como la hora será la siguiente:

| | |
|---|---|
| YY or YYYY | = Año |
| MM | = Mes |
| DD | =Día |
| HH | = Hora |
| MM | = Minuto |
| SS | = Segundos |
| hh | = Centésimas de segundo |
| mmmmmm | = Microsegundos |

ESPACIOS EN BLANCO

Dentro de este manual será requerido distinguir los espacios en blanco para lo cual se utilizara el símbolo **b-** indicando el espacio mencionado.

Además de las siguiente abreviaciones propias de EMV :

µA - *Microampere*

µm - *Micro metre*

µs -*Microsecond*

a -*Alphabetic (see section 4.3, Data Element Format Convention)*

AAC -*Application Authentication Cryptogram*

AAR - Application Authorisation Referral

AC - *Application Cryptogram*

ACK - *Acknowledgment*

ADF - *Application Definition File*

AEF - *Application Elementary File*

AFL - *Application File Locator*

AID - *Application Identifier*

AIP - *Application Interchange Profile*

An - *Alphanumeric (see section 4.3)*

Ans - *Alphanumeric Special (see section 4.3)*

APDU -*Application Protocol Data Unit*

API - *Application Program Interface*

ARC - *Authorisation Response Code*

ARPC - *Authorisation Response Cryptogram*

ARQC - *Authorisation Request Cryptogram*

ASI - *Application Selection Indicator*

ASN - *Abstract Syntax Notation*

ATC - *Application Transaction Counter*

ATM - *Automated Teller Machine*

ATR - *Answer to Reset*

AUC -*Application Usage Control*

B - *Binary (see section 4.3)*

BCD - *Binary Coded Decimal*

BER - *Basic Encoding Rules (defined in ISO/IEC 8825-1)*

BIC - *Bank Identifier Code*

BGT - *Block Guardtime*

BWI - *Block Waiting Time Integer*

BWT - *Block Waiting Time*

C - *Celsius or Centigrade*

CAD - *Card Accepting Device*

C-APDU - *Command APDU*

CBC - *Cipher Block Chaining*

CCD - *Common Core Definitions*

CCI - *Common Core Identifier*

CDA - *Combined DDA/Application Cryptogram Generation*

CDOL - *Card Risk Management Data Object List*

CID - *Cryptogram Information Data*

CIN- *Input Capacitance*

CLA - *Class Byte of the Command Message*

CLK - *Clock*

Cn - *Compressed Numeric (see section 4.3)*

CPU - *Central Processing Unit*

CSU - *Card Status Update*

C-TPDU- *Command TPDU*

CV - *Cryptogram Version*

CVM- *Cardholder Verification Method*

CVR - *Card Verification Results*

CV Rule - *Cardholder Verification Rule*

CWI - *Character Waiting Time Integer*

CWT - *Character Waiting Time*

D - *Bit Rate Adjustment Factor*

DAD- *Destination Node Address*

DC - *Direct Current*

DDA - *Dynamic Data Authentication*

DDF - *Directory Definition File*

DDOL - *Dynamic Data Authentication Data Object List*

DES - *Data Encryption Standard*

DF - *Dedicated File*

DIR - *Directory*

DOL - *Data Object List*

ECB - *Electronic Code Book*

EDC - *Error Detection Code*

EF - *Elementary File*

EN - *European Norm*

Etu - *Elementary Time Unit*

F - *Frequency*

FC - *Format Code*

FCI - *File Control Information*

FIPS - *Federal Information Processing Standard*

GND - *Ground*

GP - *Grandparent key for session key generation*

Hex - *Hexadecimal*

HHMMSS - *Hours, Minutes, Seconds*

I/O - *Input/Output*

IAC - *Issuer Action Code (Denial, Default, Online)*

IAD - *Issuer Application Data*

IBAN -*International Bank Account Number*

I-block -*Information Block*

IC -*Integrated Circuit*

ICC - *Integrated Circuit(s) Card*

ICC - *Current drawn from VCC*

IE C - *International Electrotechnical Commission*

IFD - *Interface Device*

IFS - *Information Field Size*

IFSC - *Information Field Size for the ICC*

IFSD - *Information Field Size for the Terminal*

IFSI - *Information Field Size Integer*

IIN -*Issuer Identification Number*

IK -*Intermediate Key for session key generation*

INF -*Information Field*

INS - *Instruction Byte of Command Message*

IOH - *High Level Output Current*

IOL - *Low Level Output Current*

ISO - *International Organization for Standardization*

IV - *Initial Vector for session key generation*

KM - *Master Key*

KS - *Session Key*

L - *Length*

l.s. - *Least Significant*

Lc - *Exact Length of Data Sent by the TAL in a Case 3 or 4 Command*

LCOL - *Lower Consecutive Offline Limit*

LDD - *Length of the ICC Dynamic Data*

Le - *Maximum Length of Data Expected by the TAL in Response to a Case 2 or 4 Command*

LEN - *Length*

Licc - *Exact Length of Data Available or Remaining in the ICC (as Determined by the ICC) to be Returned in Response to the Case 2 or 4 Command Received by the ICC*

Lr - *Length of Response Data Field*

LRC - *Longitudinal Redundancy Check*

M - *Mandatory*

mΩ - *Milliohm*

MΩ - *Megohm*

m.s. -*Most Significant*

m/s -*Meters per Second*

mA - *Milliampere*

MAC -*Message Authentication Code*

max. -*Maximum*

MF - *Master File*

MHz -*Megahertz*

min. *Minimum*

MK - *ICC Master Key for session key generation*

Mm -Millimetre

MMDD -Month, Day

MMYY -Month, Year

N -*Newton*

n -*Numeric (see section 4.3)*

NAD -*Node Address*

NAK -*Negative Acknowledgment*

nAs -*Nanoampere-second*

NCA -*Length of the Certification Authority Public Key Modulus*

NF - *Norme Française*

NI - *Length of the Issuer Public Key Modulus*

NIC - *Length of the ICC Public Key Modulus*

NPE - *Length of the ICC PIN Encipherment Public Key Modulus*

Ns - *Nanosecond*

O - *Optional*

O/S - *Operating System*

P - *Parent key for session key generation*

P1 - *Parameter 1*

P2 - *Parameter 2*

P3 - *Parameter 3*

PAN -*Primary Account Number*

PC -*Personal Computer*

PCA -*Certification Authority Public Key*

PCB -*Protocol Control Byte*

PDOL -*Processing Options Data Object List*

pF -*Picofarad*

PI -*Issuer Public Key*

PIC -*ICC Public Key*

PIN - *Personal Identification Number*

PIX -*Proprietary Application Identifier Extension*

POS -*Point of Service*

pos. - *Position*

PSE - *Payment System Environment*

PTS - *Protocol Type Selection*

R-APDU -*Response APDU*

R-block - *Receive Ready Block*

RFU - *Reserved for Future Use*

RID - *Registered Application Provider Identifier*

RSA - *Rivest, Shamir, Adleman Algorithm*

RST - *Reset*

SAD - *Source Node Address*

S-block - *Supervisory Block*

SCA - *Certification Authority Private Key*

SDA - *Static Data Authentication*

SFI - *Short File Identifier*

SHA- 1 - *Secure Hash Algorithm 1*

SI -*Issuer Private Key*

SIC - *ICC Private Key*

SK - *Session Key for session key generation*

SW1 - *Status Byte One*

SW2 - *Status Byte Two*

TAC - *Terminal Action Code(s) (Default, Denial, Online)*

TAL - *Terminal Application Layer*

TC - *Transaction Certificate*

TCK - *Check Character*

TDOL - *Transaction Certificate Data Object List*

tF - *Fall Time Between 90% and 10% of Signal Amplitude*

TLV - *Tag Length Value*

TPDU - *Transport Protocol Data Unit*

tR -*Rise Time Between 10% and 90% of Signal Amplitude*

TS - *Initial Character*

TSI - *Transaction Status Information*

TTL - Terminal Transport Layer

TVR - *Terminal Verification Results*

UCOL - *Upper Consecutive Offline Limit*

UL - *Underwriters Laboratories Incorporated*

V - *Volt*

var. - *Variable (see section 4.3)*

VCC - *Voltage Measured on VCC Contact*

VCC - *Supply Voltage*

VIH - *High Level Input Voltage*

VIL -*Low Level Input Voltage*

VOH - *High Level Output Voltage*

VOL - *Low Level Output Voltage*

VPP - *Programming Voltage*

VPP - *Voltage Measured on VPP contact*

WI - *Waiting Time Integer*

WTX - *Waiting Time Extension*

WWT - *Work Waiting Time*

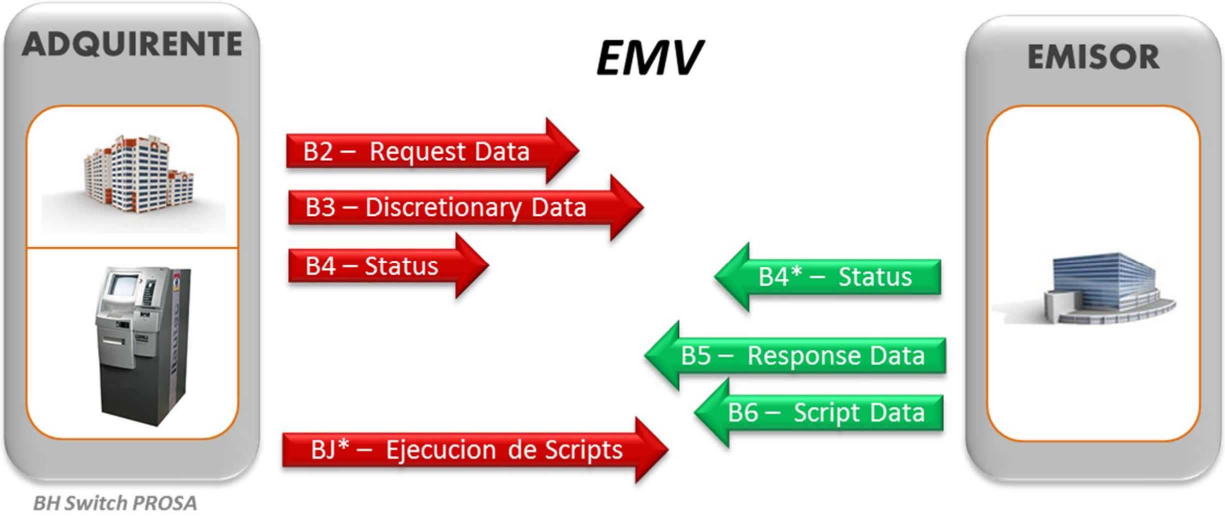
YYMM - *Year, Month*

YYMMDD - *Year, Month, Day*

⚠ Nota : Para mayor información respecto a la especificación de la aplicación deberá de referirse al manual de Visa EMV Book 3 Application Specification

# Capítulo 2: EMV FULL

Esta sección nos permite conocer cuales elementos son necesarios para el envío de los valores para poder transaccionar con mensajes de EMV FULL.



| TOKEN | DESCRIPCION | ADQUIRENTE | EMISOR |
|---|---|---|---|
| **B2** | REQUEST DATA TOKEN | M | |
| **B3** | DISCRETIONARY DATA TOKEN | M | |
| **B4** | STATUS TOKEN | M | C |
| **B5** | RESPONCE DATA TOKEN | | M |
| **B6** | SCRIPT DATA TOKEN | | M |
| **BJ** | RESULT SCRIPT DATA TOKEN | C | |

Descripción :

1. ***EMV REQUEST DATA TOKEN (B2)*** Contiene los 13 Data Elements mínimos para la realización de la transacción de EMV. *(Para mayor información del detalle de campos ir al descriptivo del token B2 descrito en este manual)*

2. ***EMV DISCRETIONARY DATA TOKEN (B3)*** contiene otros Data Elements definidos en más de una norma de la aplicación del mensaje que a sido implementado junto al proceso de EMV *(Para mayor información del detalle de campos ir al descriptivo del token B3 descrito en este manual)*

3. ***EMV STATUS TOKEN (B4)*** contiene el control de información que no es necesariamente especificada para transacciones de EMV *(Para mayor información del detalle de campos ir al descriptivo del token B4 descrito en este manual)*

4. ***EMV RESPONSE DATA TOKEN (B5)*** contiene los Data Elements necesarios para generar la respuesta de la transacción, junto con los Falgs para el Script Command *(Para mayor información del detalle de campos ir al descriptivo del token B5 descrito en este manual)*

5. ***EMV SCRIPT DATA TOKEN (B6)*** contiene los comandos necesarios para la realización del Script Command *(Para mayor información del detalle de campos ir al descriptivo del token B6 descrito en este manual)*

6. ***RESULT SCRIPT DATA TOKEN (BJ)*** contiene La respuesta necesaria para indicar si fue aplicada o no Script Command *(Para mayor información del detalle de campos ir al descriptivo del token B6 descrito en este manual)*

Todos los elementos viajaran a través de Tokens , los cuales deberán de cumplir con las especificaciones que se indican mas adelante en este manual.

# Capítulo 3: DATA ELEMENT 126

En esta sección se nombra el Data Element en donde viajarán los Tokens correspondientes tanto para un adquirente como un emisor tal y como se indica en la tabla de Conversión descrita anteriormente

### S-126 BASE24-ATM ADDITIONAL DATA

**Format:** ANS . .800 (includes a 3-position field length indicator)
**Used By:** BASE24-atm

The Additional Data element contains System message tokens. This data element is conditional for all messages. For incoming messages, any token included in the message is appended to the STM. For outgoing messages, the tokens included in this data element are specified in the Token File (TKN). For more information on configuring tokens to be included in outgoing external messages.

The tokens are carried in the external message in the same general structure as they are carried in the internal message. The major difference is that, in the external message, all tokens are in ASCII format.

If token data is added to this data element, the first item following the field length indicator is a Header token. The Header token contains a count of the number of tokens associated with the message and the overall length of all token data. The Header token is added to the message when the first token is added, and is updated each time a subsequent token is added.

The token header for the first token is located after the Header token. Each token that is added to the message has its own token header. Unlike the Header token, which contains information about all tokens in the message, the token header contains information about one specific token. The token header identifies the individual token and contains the length of the individual token. The token header is followed by the token data. Together, the token header and the token data form a single token. The combination of token header and token data is repeated for each token in the message.

**Standard Internal Message with Tokens**

| | | | | | |
|---|---|---|---|---|---|
| STM/PSTM/TSTM | Header Token | Token | Token | Token | ... |

**Header Token**

The Header token contains a count of the number of tokens associated with the message and the overall length of all token data. The Header token is added to the message when the first token is added, and is updated each time a subsequent token is added. The Header token is illustrated below.

| Eye Catcher | Count | Length |
|---|---|---|
| & | 02 | 30 |

The first field in the Header token contains an eye catcher. The eye catcher makes it easy to locate
token information when viewing internal messages. The eye catcher in the Header token is an ampersand **(&)**.

The second field contains the token count. In the example, the token count field contains the value 2. This indicates that there are two tokens in the internal message—the Header token plus one additional token.

Among the symbol **(&)** Eye catcher and the Count will exist a space the one which this represented
by "   ".

The final field contains the overall length of token data. The length includes the total length of the Header token, plus the length of each individual token added  to the message.

**Description  Header Token:**

| Position | Level | Field Name and Description | Data Type |
|---|---|---|---|
| **1–12** | | **HEADER-TKN** | |
| **1** | **02** | **EYE-CATCHER**<br>Indicates the start of token data. The only valid value is an ampersand **(&)**. | **PIC X(1)** |
| **2** | **02** | **USER-FLD1**<br>space “  ” | **PIC X(1)** |
| **3–7** | **02** | **CNT**<br>The count of the number of tokens, including the Header token, that are present in the token data buffer. | **PIC 9(5)** |
| **8–12** | **02** | **LGTH**<br>The length of all token data, including the Header token and token header structures, present in a token data buffer. | **PIC 9(5)** |

## 3. 1 Tokens

### Token Headers

Each token that is added to the message has its own token header. Unlike the Header token, which contains information about all tokens in the message, the token header contains information about one specific token. The token header identifies the individual token and contains the binary length of the individual token. The token header is followed by the token data. Together, the token header and the token data form a single token. The general format of a token is illustrated below.

**Data Token**

| Eye Catcher | Token ID | Token | Length Token Data |
|---|---|---|---|
| ! | 13 | 30 | 11101361109261209... |

The first field in the data token is another eye catcher. The eye catcher separates each token in the message from the previous token. The eye catcher in data tokens is always an exclamation point **(!)**.

Among the symbol **(!)** Eye Catcher and the Token ID will exist a space the one which this represented by "   ".

The tokens are carried in their entirety in ASCII format. The general structure of this data element is provided below:

**Description Token Header**:

| **Position** | **Level** | **Field Name and Description** | **Data Type** |
|---|---|---|---|
| **1–10** | | **TKN-HEADER** | |
| **1** | **02** | **EYE-CATCHER**<br>Indicates the start of an individual token. The only valid value is an exclamation point (!).<br>**Note:** If the Super Extract process converts a token to EBCDIC, the exclamation point in this field is translated to a vertical bar (\|). | **PIC X(1)** |
| **2** | **02** | **USER-FLD1**<br>Space “  ” | **PIC X(1)** |
| **3–4** | **02** | **TKN-ID**<br>The two-byte ASCII representation of the token ID. The token ID uniquely identifies a token. | **PIC X(2)** |
| **5–9** | **02** | **LGTH**<br>The length of the token data for the token identified by the TKN-ID field. | **PIC 9(5)** |
| **10** | **02** | **USER-FLD2**<br>Space “” | **PIC X(1)** |

## Descripción General de Token

| Position | Length | Description |
|---|---|---|
| **1–3** | **3** | **Field Length Indicator**<br>The field length indicator value is the sum of the lengths of the Header token, all token headers, and token data being used. |
| **4–15** | **12** | **Header Token** |
| **15–24** | **10** | **Token Header** |
| ***a–b*** | ***n*** | **Token Data** |
| **...** | **...** | **...** |
| ***w–x*** | **10** | **Token Header** |
| ***y–z*** | ***n*** | **Token Data** |

# Capítulo 4: Tokens EMV FULL

## 4.1 TOKEN B2 REQUEST DATA TOKEN

**Message : 0200**

The EMV Request Data token contains the thirteen minimum request data elements required for inclusion in request messages, as defined by EMV. The Device Handler process or the Interchange Interface process creates this token and adds it to the transaction message before sending it to the Authorization process.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification.*

**Descripción de los Campos :**

| **#** | **Lenght** | **Descriptivo** | **valor** |
|---|---|---|---|
| 1–158 | | EMV-RQST-TKNX | |
| 1–4 | 02 | BIT-MAP | PIC X(4) |

Indicates whether data in each of the remaining fields in the token is present or absent. The token itself is a fixed format structure, so the absence of a data item means that the appropriate field is present but that its contents are undefined.

Note that the positions of the bits within the bit map follow the ISO 8583 convention (i.e., the highest order bit represents the first field in the token, following the BIT-MAP field).

| Posición | Nombre | Etiqueta |
|---|---|---|
| 1 | USER-FLD1 | n/a |

| | | |
|---|---|---|
| 2 | CRYPTO-INFO-DATA | 9F27 |
| 3 | TVR | 95 |
| 4 | ARQC | 9F26 |
| 5 | AMT-AUTH | 9F02 |
| 6 | AMT-OTHER | 9F03 |
| 7 | AIP | 82 |
| 8 | ATC | 9F36 |
| 9 | TERM-CNTRY-CDE | 9F1A |
| 10 | TRAN-CRNCY-CDE | 5F2A |
| 11 | TRAN-DAT | 9A |
| 12 | TRAN-TYPE | 9C |
| 13 | UNPREDICT-NUM | 9F37 |
| 16 | ISS-APPL-DATA | 9F10 |

5–8 02 USER-FLD1 PIC X(4)

Must contain zeros.

9–10 02 CRYPTO-INFO-DATA PIC X(2)

The type of cryptogram and the actions to be performed by the terminal. Valid values are shown in the table below.

In the EMV specifications, definitions that include bit positions indicate that bit 8 is the leftmost bit. **Caution:** In TAL programming, the highest order bit is the zero bit.

| Posición del Bit de Emv | Descripción |
|---|---|
| 8-7 | Type of cryptogram. Valid values are as follows:<br>00 = AAC<br>01 = TC<br>10 = ARQC<br>11 = AAR |
| 6 | Reserved for future use |
| 5 | Reserved for future use |
| 4 | Advice required flag. Valid values are as follows:<br>0 = Advice is Not Requires.<br>1 = Advice is required |
| 3-1 | The reason, advice, or referral code.<br>Valid values are as follows:<br>000 = No information given<br>001 = Service not allowed<br>010 = PIN try limit exceeded<br>011 = Issuer authentication failed |

| | | | |
|---|---|---|---|
| 11–20 | 02 | TVR | PIC X(10) |

The terminal verification results. This field indicates the status of the different functions as seen from the terminal. Valid values are shown in the tables below. The default for all bit settings is a value of 0.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

Bit positions not listed are reserved for future use.

**Caution:** In TAL programming, the highest order bit is the zero bit.

## Byte 1

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Offline data authentication flag. Valid values are as follows:<br>0 = Offline data authentication was performed.<br>1 = Offline data authentication was not performed. |
| 7 | Offline static data authentication flag. Valid values are as follows:<br>0 = Offline static data authentication passed.<br>1 = Offline static data authentication failed. |
| 6 | Integrated circuit card (ICC) data flag. Valid values are as follows:<br>0 = ICC data is present.<br>1 = ICC data is missing. |
| 5 | Card on exception file flag. Valid values are as follows:<br>0 = Card does not appear on terminal exception file.<br>1 = Card appears on terminal exception file. |

| | |
|---|---|
| 4 | Offline dynamic data authentication flag. Valid values are as follows:<br>0 = Offline dynamic data authentication passed.<br>1 = Offline dynamic data authentication failed. |

**Byte 2**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | ICC and terminal version flag. Valid values are as follows:<br>0 = The ICC and the terminal have the same application versions.<br>1 = The ICC and the terminal have different application versions. |
| 7 | Expired application flag. Valid values are as follows:<br>0 = The application has not expired.<br>1 = The application expired. |
| 6 | Application effective flag. Valid values are as follows:<br>0 = The application is effective.<br>1 = The application is not yet effective. |
| 5 | Requested service flag. Valid values are as follows:<br>0 = The requested service is allowed for the card product.<br>1 = The requested service is not allowed for the card product. |
| 4 | New card flag. Valid values are as follows:<br>0 = The transaction was not initiated with a new card.<br>1 = The transaction was initiated with a new card. |

## Byte 3

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Cardholder verification flag. Valid values are as follows:<br>0 = Cardholder verification was successful.<br>1 = Cardholder verification was not successful. |
| 7 | Unrecognized cardholder verification method (CVM) flag. Valid values are as follows:<br>0 = The CVM was recognized.<br>1 = The CVM was not recognized. |
| 6 | PIN tries flag. Valid values are as follows:<br>0 = The PIN try limit was not exceeded.<br>1 = The PIN try limit was exceeded. |
| 5 | PIN required/PIN pad not available condition. Valid values are as follows:<br>0 = PIN entry is not required or the PIN pad is present and operable.<br>1 = PIN entry is required and the PIN pad is not present or inoperable. |
| 4 | PIN required/PIN not entered condition. Valid values are as follows:<br>0 = PIN entry is not required or the PIN pad is not present or the PIN was entered.<br>1 = PIN entry is required, PIN pad is present, PIN not entered. |
| 3 | OnLine PIN Flag.<br>Valid Values are as follows:<br>0 = Online PIN not entered.<br>1 = On line PIN entered. |

*Todos los desarrollos realizados deberán basarse en los estándares definidos por PROSA.*

## Byte 4

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Floor limit flag. Valid values are as follows:<br>0 = The transaction amount does not exceed the floor limit.<br>1 = The transaction amount exceeds the floor limit. |
| 7 | Lower consecutive offline limit flag. Valid values are as follows:<br>0 = The lower consecutive offline limit was not exceeded.<br>1 = The lower consecutive offline limit was |
| 6 | Upper consecutive offline limit flag. Valid values are as follows:<br>0 = The upper consecutive offline limit was not exceeded.<br>1 = The upper consecutive offline limit was |
| 5 | Random selection flag. Valid values are as follows:<br>0 = The transaction was not selected at random for online processing.<br>1 = The transaction was selected at random for online processing. |
| 4 | Merchant forced online flag. Valid values are as follows:<br>0 = The merchant did not force the transaction online.<br>1 = The merchant forced the transaction online. |

## Byte 5

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Transaction certificate data object list (TDOL) status. Valid values are as follows:<br>0 = The default TDOL was not used.<br>1 = The default TDOL was used. |

| | |
|---|---|
| 7 | Issuer authentication flag. Valid values are as follows:<br>0 = Issuer authentication was successful.<br>1 = Issuer authentication was not successful. |
| 6 | Script processing before final GENERATE AC command flag.<br>Valid values are as follows:<br>0 = Script processing did not fail before final GENERATE AC command.<br>1 = Script processing failed before final GENERATE AC command. |
| 5 | Script processing after final GENERATE AC flag. Valid values are as follows:<br>0 = Script processing did not fail after final GENERATE AC command.<br>1 = Script processing failed after final GENERATE AC command. |

21–36 02 ARQC PIC X(16)

The authorization request cryptogram. The cryptogram returned by the ICC in response to the GENERATE AC command.

37–48 02 AMT-AUTH PIC X(12)

The authorized amount of the transaction (excluding adjustments). Data in this field is right-justified, zero-filled packed data (i.e., binary coded decimal).

49–60 02 AMT-OTHER PIC X(12)

A secondary amount associated with the transaction, representing a cash-back amount. Data in this field is right-justified, zero-filled packed data (i.e., binary coded decimal).

61–64 02 AIP PIC X(4)

The application interchange profile. This field indicates the capabilities of the card to support specific functions in the application. Valid values are shown in the tables below.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

Bit positions not listed are reserved for future use.

**Caution:** In TAL programming, the highest order bit is the zero bit.

## Byte 1

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Initiate flag. Valid values are as follows:<br>0 = Do not initiate.<br>1 = Initiate. |
| 7 | Offline static data authentication support flag. Valid values are as follows:<br>0 = Offline static data authentication is not supported.<br>1 = Offline static data authentication is supported. |
| 6 | Offline dynamic data authentication support flag. Valid values are as follows:<br>0 = Offline dynamic data authentication is not supported.<br>1 = Offline dynamic data authentication is supported. |
| 5 | Cardholder verification support flag. Valid values are as follows:<br>0 = Cardholder verification is not supported.<br>1 = Cardholder verification is supported. |
| 4 | Terminal risk management support flag. Valid values are as follows:<br>0 = Terminal risk management will not be performed.<br>1 = Terminal risk management will be performed. |
| 3 | Issuer authentication support flag. Valid values are as follows:<br>0 = Issuer authentication is not supported<br>1 = Issuer authentication is supported. |

### Byte 2

All bits in byte 2 are reserved for future use.

65–68 02 ATC PIC X(4)

The application transaction counter. The application on the chip maintains and increments this counter.

69–7 1 02 TERM-CNTRY-CDE PIC X(3)

A code indicating the country of the terminal, according to the ISO 3166 standard, ***Codes for the Representation of Names of Countries.*** Data in this field is right-justified, zero-filled packed data (i.e., binary coded decimal).

72–74 02 TRAN-CRNCY-CDE PIC X(3)

A code indicating the currency code of the transaction, as received from the device or interchange, according to the ISO 4217 standard, ***Codes for the Representation of Currencies and Funds.*** Data in this field is right-justified, zero-filled packed data (i.e., binary coded decimal).

75–80 02 TRAN-DAT PIC X(6)

The local date (in YYMMDD format) that the transaction was authorized. Data in this field is stored as packed data (i.e., binary coded decimal).

8 1–82 02 TRAN-TYPE PIC X(2)

A code indicating the type of financial transaction, represented by the first two digits of the processing code from the 1987 ISO 8583 standard, ***Bank Card Originated Messages— Interchange Message Specifications—Content for Financial Transactions.*** Data in this field is stored as packed data (i.e., binary coded decimal).

83–90 02 UNPREDICT-NUM PIC X(8)

An unpredictable number used to provide variability and uniqueness to the generation of a cryptogram.

91–94 02 ISS-APPL-DATA-LGTH PIC X(4)

Indicates the length of the issuer application data in the following field. The ASCII and binary versions of the token must contain the same value in this field. The ASCII version of the token must contain the decimal (not hexadecimal) representation of the length value.

95–158 02 ISS-APPL-DATA PIC X(64)

The proprietary issuer application data for transmission to the issuer in an online transaction. The data is left-justified and padded to the right with binary zeroes.

02 VISA-APPL-DATA REDEFINES ISS-APPL-DATA The

| | | | | |
|---|---|---|---|---|
| | | | | Visa/UKIS definition of the issuer application data. |
| 95–96 | 04 | LGTH | PIC X(2) | Length of the binary representation of the following data. The ASCII and binary versions of the token must contain the same value in this field. |
| 97–98 | 04 | DERIV-KEY-INDEX | PIC X(2) | The derivation key index. This value identifies to the issuer the derivation key required to derive the card's unique DEA keys to be used to perform on-line card and issuer authentication. The derivation key index is not used by the card. |
| 99–100 | 04 | CRYPTO-VER-NUM | PIC X(2) | The cryptogram version number. This value indicates the version of the TC/AAC/ARQC algorithm used by the application. Values are assigned by card schemes. Valid values are as follows:<br>**0A** = Decimal 10<br>**0E** = Decimal 14<br>**11** = Decimal 17 |
| 101–108 | 04 | CRD-VRFY-RSLTS | PIC X(8) | The card verification results. The contents of this field indicate the exception conditions that occurred during card risk management, as shown below.<br>In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit. Bit positions not listed are reserved for future use. |

## Byte 1

Length Indicator

## Byte 2

| EMV Defined Bit Position | Description |
|---|---|
| 8–7 | Type of cryptogram. Valid values are as follows:<br>00 = AAC returned in second GENERATE AC<br>01 = TC returned in second GENERATE AC<br>10 = Second GENERATE AC not requested<br>11 = Reserved for future use |
| 6 | Reserved for future use |
| 5 | Reserved for future use |

| | |
|---|---|
| 4 | Issuer authentication failure flag. Valid values are as follows:<br>0 = Issuer authentication did not fail.<br>1 = Issuer authentication failed. |
| 3 | Off-line PIN verification performed. Valid values are as follows:<br>0 = Off-line PIN verification was not performed.<br>1 = Off-line PIN verification was performed. |
| 2 | Off-line PIN verification failed. Valid values are as follows:<br>0 = Off-line PIN verification did not fail.<br>1 = Off-line PIN verification failed. |

| | |
|---|---|
| 1 | Unable to go on-line. Valid values are as follows:<br>0 = Able to go on-line.<br>1 = Unable to go on-line |

## Byte 3

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Last on-line transaction not completed. Valid values are as follows:<br>0 = Last on-line transaction completed.<br>1 = Last on-line transaction did not complete. |
| 7 | PIN try limit exceeded. Valid values are as follows:<br>0 = PIN try limit was not exceeded.<br>1 = PIN try limit exceeded. |
| 6 | Exceeded velocity checking counters. Valid values are as follows:<br>0 = Velocity checking counters were not exceeded.<br>1 = Velocity checking counters were exceeded. |

| | |
|---|---|
| 5 | New card flag. Valid values are as follows:<br>0 = New card not used to initiate the transaction.<br>1 = New card used to initiate the transaction. |
| 4 | Issuer authentication failure on last online transaction. Valid values are as follows:<br>0 = Issuer authentication did not fail on last on-line transaction.<br>1 = Issuer authentication failed on last on-line transaction. |
| 3 | Issuer authentication not performed after on-line authorization. Valid values are as follows:<br>0 = Issuer authentication performed after on-line authorization.<br>1 = Issuer authentication not performed after on-line authorization. |
| 2 | Application blocked by card because PIN try limit exceeded. Valid values are as follows:<br>0 = Application not blocked by card because PIN try limit exceeded.<br>1 = Application blocked by card because PIN try limit exceeded. |

| | |
|---|---|
| 1 | Static data authentication failed on last transaction and transaction declined off-line. Valid values are as follows:<br>0 = Static data authentication did not fail on the last transaction and transaction was declined off-line.<br>1 = Static data authentication failed on the last transaction and transaction was declined off-line. |

## Byte 4

| EMV Defined Bit Position | Description |
|---|---|
| 8–5 | Number of issuer script commands containing secure messaging processed on last transaction. Valid values are as follows:<br>0 = Number of issuer script commands containing secure messaging not processed on last transaction.<br>1 = Number of issuer script commands containing secure messaging processed on last transaction. |
| 4 | Reserved for future use. |
| 3 | Reserved for future use. |
| 2 | Reserved for future use. |
| 1 | Reserved for future use. |

109–158 04 INFO PIC X(50)

This field contains the issuer discretionary data.

02 MCPA-APPL-DATA REDEFINES ISS-APPL-DATA

The MasterCard/Europay (MCPA) M/Chip 2.1 definition of the issuer application data.

95–96 04 DERIV-KEY-INDEX PIC X(2)

The derivation key index. This value identifies to the issuer the derivation key required to derive the card's unique DEA keys to be used to perform on-line card and issuer authentication. The derivation key index is not used by the card.

97–98 04 CRYPTO-VER-NUM PIC X(2)

The cryptogram version number. This value indicates the version of the TC/AAC/ARQC algorithm used by the application. Currently the only supported value is 0*x*, where *x* represents any hexadecimal digit.

99–106 04 CRD-VRFY-RSLTS PIC X(8)

The card verification results. The contents of this field indicate the exception conditions that occurred during card risk management, as shown below.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

**Caution:** In TAL programming, the highest order bit is the zero bit.

**Byte 1**

Length Indicator

**Byte 2**

| EMV Defined Bit Position | Description |
|---|---|
| 8–7 | Type of cryptogram. Valid values are as follows:<br>00 = AAC returned in second GENERATE AC<br>01 = TC returned in second GENERATE AC<br>10 = Second GENERATE AC not requested<br>11 = Reserved for future use |
| 6 | Reserved for future use |
| 5 | Reserved for future use |
| 4 | Issuer authentication failure flag. Valid values are as follows:<br>0 = Issuer authentication did not fail.<br>1 = Issuer authentication failed. |
| 3 | Off-line PIN verification performed. Valid values are as follows:<br>0 = Off-line PIN verification was not performed.<br>1 = Off-line PIN verification was performed. |
| 2 | Off-line PIN verification failed. Valid values are as follows:<br>0 = Off-line PIN verification did not fail.<br>1 = Off-line PIN verification failed. |

| | |
|---|---|
| 1 | Unable to go on-line. Valid values are as follows:<br>0 = Able to go on-line.<br>1 = Unable to go on-line |

**Byte 3**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Last on-line transaction not completed. Valid values are as follows:<br>0 = Last on-line transaction completed.<br>1 = Last on-line transaction did not complete. |
| 7 | PIN try limit exceeded. Valid values are as follows:<br>0 = PIN try limit was not exceeded.<br>1 = PIN try limit exceeded. |
| 6 | Exceeded velocity checking counters. Valid values are as follows:<br>0 = Velocity checking counters were not exceeded.<br>1 = Velocity checking counters were exceeded. |

| | |
|---|---|
| 5 | New card flag. Valid values are as follows:<br>0 = New card not used to initiate the transaction.<br>1 = New card used to initiate the transaction. |
| 4 | Issuer authentication failure on last online transaction. Valid values are as follows:<br>0 = Issuer authentication did not fail on last on-line transaction.<br>1 = Issuer authentication failed on last on-line transaction. |
| 3 | Issuer authentication not performed after on-line authorization. Valid values are as follows:<br>0 = Issuer authentication performed after on-line authorization.<br>1 = Issuer authentication not performed after on-line authorization. |
| 2 | Application blocked by card because PIN try limit exceeded. Valid values are as follows:<br>0 = Application not blocked by card because PIN try limit exceeded.<br>1 = Application blocked by card because PIN try limit exceeded. |

| | |
|---|---|
| 1 | Static data authentication failed on last transaction and transaction declined off- line. Valid values are as follows:<br>0 = Static data authentication did not fail on the last transaction and transaction was declined off-line.<br>1 = Static data authentication failed on the last transaction and transaction was declined off-line. |

## Byte 4

| EMV Defined Bit Position | Description |
|---|---|
| 8–5 | Number of issuer script commands containing secure messaging processed on last transaction. Valid values are as follows:<br>0 = Number of issuer script commands containing secure messaging not processed on last transaction.<br>1 = Number of issuer script commands containing secure messaging processed on last transaction. |
| 4 | Issuer script processing failed on last transaction. Valid values are as follows:<br>0 = Issuer script processing did not fail on last transaction.<br>1 = Issuer script processing failed on last transaction. |
| 3 | Reserved for future use. |
| 2 | Reserved for future use. |
| 1 | Reserved for future use. |

107–110 04 DAC PIC X(4)

The Dynamic Authentication Code, or two leftmost bytes of the ICC Dynamic Number. This value can be used to prove that the terminal correctly performed static or dynamic data authentication.

111–158 04 INFO PIC X(48)

This field contains the issuer discretionary data.

02 MCHIP4-APPL-DATA REDEFINES ISS-APPL-DATA

Contains the MasterCard/Europay M/Chip 4 definition of the issuer application data.

95–96 04 DERIV-KEY-INDEX PIC X(2)

The derivation key index. This value identifies to the issuer the derivation key required to derive the card's unique DEA keys to be used to perform on-line card and issuer authentication. The derivation key index is not used by the card.

97–98 04 CRYPTO-VER-NUM PIC X(2)

The cryptogram version number. This value indicates the version of the TC/AAC/ARQC algorithm used by the application. Currently the supported values are 10, 11, 12, 13, 14, and 15.

99–110 04 CRD-VRFY-RSLTS PIC X(12)

The card verification results. The contents of this field indicate the exception conditions that occurred during card risk management, as shown below.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

**Byte 1**

| EMV Defined Bit Position | Description |
|---|---|
| 8–7 | AC returned in second GENERATE AC. Valid values are as follows:<br>0 = AC was not returned in the second GENERATE AC.<br>1 = AC was returned in the second GENERATE AC. |
| 6–5 | AC returned in first GENERATE AC. Valid values are as follows:<br>0 = AC was not returned in the first GENERATE AC.<br>1 = AC was returned in the first GENERATE AC. |
| 4 | Reserved for future use. |
| 3 | Offline PIN verification flag. Valid values are as follows:<br>0 = Offline PIN verification was not successful.<br>1 = Offline PIN verification was successful. |

| | |
|---|---|
| 2 | Offine encrypted PIN verification flag. Valid values are as follows:<br>0 = Offline encrypted PIN verification was not successful.<br>1 = Offline encrypted PIN verification was successful. |
| 1 | Offline PIN verification successful. Valid values are as follows:<br>0 = Offline PIN verification was not successful.<br>1 = Offline PIN verification was successful. |

**Byte 2**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | DDA returned. Valid values are as follows:<br>0 = DDA was not returned.<br>1 = DDA was returned. |
| 7 | Combined DDA/AC generation returned in first GENERATE AC. Valid values are as follows:<br>0 = The combined DDA/AC generation was not returned in the first GENERATE AC.<br>1 = The combined DDA/AC generation was returned in the first GENERATE AC. |

| | |
|---|---|
| 6 | Combined DDA/AC generation returned in second GENERATE AC. Valid values are as follows:<br>0 = The combined DDA/AC generation was not returned in the second GENERATE AC.<br>1 = The combined DDA/AC generation was returned in the second GENERATE AC. |
| 5 | Issuer authentication performed. Valid values are as follows:<br>0 = Issuer authentication was not performed.<br>1 = Issuer Authentication was performed. |
| 4 | Card risk management skipped on CAT3. Valid values are as follows:<br>0 = Card risk management was not skipped on CAT3.<br>1 = Card risk management was skipped on CAT3. |
| 3 | Reserved for future use. |
| 2 | Reserved for future use. |
| 1 | Reserved for future use. |

**Byte 3**

| EMV Defined Bit Position | Description |
|---|---|
| 8–5 | Right nibble of Script Counter. |
| 4–1 | Right nibble of PIN Try Counter. |

**Byte 4**

**Current transaction**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Reserved for future use. |
| 7 | Unable to go online. Valid values are as follows:<br>0 = The transaction was able to go online.<br>1 = The transaction was not able to go online. |
| 6 | Offline PIN verification not performed. Valid values are as follows:<br>0 = Offline PIN verification was performed.<br>1 = Offline PIN verification was not performed. |
| 5 | Offline PIN verification failed. Valid values are as follows:<br>0 = Offline PIN verification did not fail.<br>1 = Offline PIN verification failed. |
| 4 | PTL exceeded. Valid values are as follows:<br>0 = PTL was not exceeded.<br>1 = PTL was exceeded. |
| 3 | International transaction. Valid values are as follows:<br>0 = The current transaction is not an international transaction.<br>1 = The current transaction is an international transaction. |

| | |
|---|---|
| 2 | Domestic transaction. Valid values are as follows:<br>0 = The current transaction is not a domestic Transaction.<br>1 = The current transaction is a domestic transaction. |
| 1 | Terminal erroneously considers offline PIN OK. Valid values are as follows:<br>0 = Terminal does not erroneously consider offline PIN OK.<br>1 = Terminal erroneously considers offline PIN OK. |

**Byte 5**

**Current plus last online transaction**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Lower consecutive offline limit exceeded. Valid values are as follows:<br>0 = The lower consecutive offline limit was not exceeded.<br>1 = The lower consecutive offline limit was exceeded. |
| 7 | Upper consecutive offline limit exceeded. Valid values are as follows:<br>0 = The upper consecutive offline limit was not exceeded.<br>1 = The upper consecutive offline limit was Exceeded. |
| 6 | Lower cumulative offline limit exceeded. Valid values are as follows:<br>0 = The lower cumulative offline limit was not exceeded.<br>1 = The lower cumulative offline limit was exceeded. |

| | |
|---|---|
| 5 | Upper cumulative offline limit exceeded. Valid values are as follows:<br>0 = The upper cumulative offline limit was not exceeded.<br>1 = The upper cumulative offline limit was exceeded. |
| 4 | Go online on next transaction was set. Valid values are as follows:<br>0 = Go online on next transaction was not set.<br>1 = Go online on next transaction was set. |
| 3 | Issuer authentication failed. Valid values are as follows:<br>0 = Issuer authentication did not fail. 1 = Issuer authentication failed. |
| 2 | Script received. Valid values are as follows:<br>0 = The script was not received.<br>1 = The script was received. |
| 1 | Script failed. Valid values are as follows:<br>0 = The script did not fail.<br>1 = The script failed. |

**Byte 6**

**Current transaction**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Reserved for future use. |

| | |
|---|---|
| 7 | Reserved for future use. |
| 6 | Reserved for future use. |
| 5 | Reserved for future use. |
| 4 | Reserved for future use. |
| 3 | Reserved for future use. |
| 2 | Match found in additional check table. Valid values are as follows:<br>0 = No match not found in additional check table.<br>1 = Match found in additional check table. |
| 1 | No match found in additional check table. Valid values are as follows:<br>0 = Match found in additional check table.<br>1 = No match found in additional check table. |

111–114 04 DAC PIC X(4)

The Dynamic Authentication Code, or two leftmost bytes of the ICC Dynamic Number. This value can be used to prove that the terminal correctly performed static or dynamic data authentication.

115–130 04 CNTR PIC X(16)

This field contains plain text or encrypted counter information.

131–158 04 INFO PIC X(28)

This field contains the issuer discretionary data

| | | | | |
|---|---|---|---|---|
| | 02 | CCD-A-APPL-DATA | REDEFINES ISS-APPL-DATA | Contains Format A of the EMV Common Core Definition of the issuer application data. |
| 95–96 | 04 | LGTH | PIC X(2) | Length of the binary representation of the following data. The ASCII and binary versions of the token must contain the same value in this field. |
| 97–98 | 04 | COMMON-CORE-ID | PIC X(2) | The first four bits of the Common Core IAD Format Code and the second four bits of the Common Core Cryptogram Version. Valid value is A5 |
| 99–100 | 04 | DERIV-KEY-INDEX | PIC X(2) | The derivation key index. This value identifies to the issuer the derivation key required to derive the card's unique DEA keys to be used to perform on-line card and issuer authentication. The derivation key index is not used by the card |
| 101–110 | 04 | CRD-VRFY-RSLTS | PIC X(10) | The card verification results. The contents of this field indicate the exception conditions that occurred during card risk management, as shown below.<br>In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.<br>**Caution:** In TAL programming, the highest order bit is the zero bit |

**Byte 1**

| EMV Defined<br>Bit Position | Description |
|---|---|
| 8–7 | AC returned in second GENERATE AC. Valid values are as follows:<br>0 = AC was not returned in the second GENERATE AC.<br>1 = AC was returned in the second GENERATE AC. |
| 6–5 | AC returned in first GENERATE AC. Valid values are as follows:<br>0 = AC was not returned in the first GENERATE AC.<br>1 = AC was returned in the first GENERATE AC. |
| 4 | CDA performed. Valid values are as follows:<br>0 = CDA was not performed.<br>1 = CDA was performed. |
| 3 | Offline DDA performed. Valid values are as follows:<br>0 = Offline DDA was not performed.<br>1 = Offline DDA was performed. |

| | |
|---|---|
| 2 | Issuer authentication not performed. Valid values are as follows:<br>0 = Issuer authentication was performed.<br>1 = Issuer authentication was not performed. |
| 1 | Issuer authentication failed. Valid values are as follows:<br>0 = Issuer authentication did not fail.<br>1 = Issuer authentication failed. |

**Byte 2**

| EMV Defined Bit Position | Description |
|---|---|
| 8–5 | Right nibble of PIN Try Counter. |
| 4 | Offline PIN verification performed. Valid values are as follows:<br>0 = Offline PIN verification was not performed.<br>1 = Offline PIN verification was performed. |

| | |
|---|---|
| 3 | Offline PIN verification performed and PIN not successfully verified. Valid values are as follows:<br>0 = Offline PIN verification performed and PIN was successfully verified.<br>1 = Offline PIN verification performed and PIN was not successfully verified. |
| 2 | PIN try limit exceeded. Valid values are as follows:<br>0 = PIN try limit was not exceeded.<br>1 = PIN try limit was exceeded. |
| 1 | Last online transaction not completed. Valid values are as follows:<br>0 = Last online transaction completed.<br>1 = Last online transaction was not completed. |

**Byte 3**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Lower offline transaction count limit exceeded. Valid values are as follows:<br>0 = The lower offline transaction count limit was not exceeded.<br>1 = The lower offline transaction count limit was exceeded. |
| 7 | Upper offline transaction count limit exceeded. Valid values are as follows:<br>0 = The upper offline transaction count limit was not exceeded.<br>1 = The upper offline transaction count limit was exceeded. |
| 6 | Lower cumulative offline amount limit exceeded. Valid values are as follows:<br>0 = The lower cumulative offline amount limit was not exceeded.<br>1 = The lower cumulative offline amount limit was exceeded. |
| 5 | Upper cumulative offline amount limit exceeded. Valid values are as follows:<br>0 = The upper cumulative offline amount limit was not exceeded.<br>1 = The upper cumulative offline amount limit was exceeded. |

| | |
|---|---|
| 4 | Issuer-discretionary bit 1. |
| 3 | Issuer-discretionary bit 2. |
| 2 | Issuer-discretionary bit 3. |
| 1 | Issuer-discretionary bit 4. |

**Byte 4**

| EMV Defined Bit Position | Description |
|---|---|
| 8–5 | Right nibble of Script Counter. |
| 4 | Issuer script processing failed. Valid values are as follows:<br>0 = Issuer script processing did not fail.<br>1 = Issuer script processing failed. |
| 3 | Offline data authentication failed on previous transaction. Valid values are as follows:<br>0 = Offline data authentication did not fail on previous transaction.<br>1 = Offline data authentication failed on previous transaction. |

| | |
|---|---|
| 2 | Go online on next transaction was set. Valid values are as follows:<br>0 = Go online on next transaction was not set.<br>1 = Go online on next transaction was set. |
| 1 | Unable to go online. Valid values are as follows:<br>0 = The transaction was able to go online.<br>1 = The transaction was not able to go online. |

**Byte 5**

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Reserved for future use. |
| 7 | Reserved for future use. |
| 6 | Reserved for future use. |
| 5 | Reserved for future use. |
| 4 | Reserved for future use. |
| 3 | Reserved for future use. |

| | |
|---|---|
| 2 | Reserved for future use. |
| 1 | Reserved for future use. |

111–126 04 COUNTERS PIC X(16)

The contents of this field are at the discretion of the payment system.

127–128 04 ISS-DISCR-DATA-LGTH PIC X(2)

The length of the binary representation of the data that follows. The ASCII and binary versions of the token must contain the same value in this field.

129–158 04 ISS-DISCR-DATA PIC X(30)

This field contains the issuer discretionary data.

## 4.2 TOKEN B3 EMV DISCRETIONARY TOKEN

**Message : 0200**

The EMV Discretionary Request Data token consists of EMV-related data that is not required for authorization. However, each data element is supported by more than one EMV-compliant interface and, therefore, can be mapped between interfaces by BASE24.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification*.

**Descripción de los Campos :**

| # | Lenght | Descripcion | Valor |
|---|---|---|---|
| 1–80 | | EMV-DISCR-TKNX | |
| 1–4 | 02 | BIT-MAP | PIC X(4) |

Indicates whether data in each of the remaining fields in the token is present or absent. The token itself is a fixed format structure, so the absence of a data item means that the appropriate field is present but that its contents are undefined.

Note that the positions of the bits within the bit map follow the ISO 8583 convention (i.e., the highest order bit represents the first field in the token, following the BIT-MAP field). There are 16 bits in the BIT-MAP field, but only 8 fields (excluding the BIT-MAP field) in the token; therefore the lowest order 8 bits in the BIT-MAP field are reserved for future use.

| Bit Map Position | Field Name | EMV Tag |
|---|---|---|
| 1 | TERM-SER-NUM | 9F1E |
| 2 | EMV-TERM-CAP | 9F33 |

| | | |
|---|---|---|
| 3 | USER-FLD1 | n/a |
| 4 | USER-FLD2 | n/a |
| 5 | EMV-TERM-TYPE | 9F35 |
| 6 | APPL-VER-NUM | 9F09 |
| 7 | CVM-RSLTS | 9F34 |
| 8 | This field will contain one of the following data elements:<br>DF-NAME<br>APPLICATION ID | 844F |

5–12 02 TERM-SERL-NUM PIC X(8)

The interface device (IFD) number, a unique and permanent serial number assigned to the terminal by the manufacturer.

13–20 02 EMV-TERM-CAP PIC X(8)

The card data input, cardholder verification method (CVM), and security capabilities of the terminal. Valid values are shown in the tables below. The default for all bit settings is a value of 0.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

Bit positions not listed are reserved for future use.

**Caution:** In TAL programming, the highest order bit is the zero bit.

### Byte 1 (Card Data Input Capability)

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Manual key entry capability. Valid values are as follows:<br>0 = The terminal does not support manual key entry to input the card data.<br>1 = The terminal supports manual key entry to input the card data. |
| 7 | Magnetic stripe capability. Valid values are as follows:<br>0 = The terminal does not support data capture from the magnetic stripe on the card.<br>1 = The terminal supports data capture from the magnetic stripe on the card. |
| 6 | IC with contacts capability. Valid values are as follows:<br>0 = The terminal does not support data capture from the integrated chip card.<br>1 = The terminal supports data capture from the integrated chip card. |

### Byte 2 (CVM Capability)

| EMV Defined<br>Bit Position | Description |
|---|---|
| 8 | Plaintext PIN for integrated chip card (ICC) verification capability. Valid values are as follows:<br>0 = The terminal does not use plaintext PIN for ICC verification for CVM.<br>1 = The terminal uses plaintext PIN for ICC verification for CVM |
| 7 | Enciphered PIN for online verification capability. Valid values are as follows:<br>0 = The terminal does not use enciphered IN Vfor online verification for CVM.<br>1 = The terminal uses enciphered PIN for online verification for CVM. |
| 6 | Signature (paper) capability. Valid values are as follows:<br>0 = The terminal does not use signature (paper) verification for CVM.<br>1 = The terminal uses signature (paper) verification for CVM. |
| 5 | Enciphered PIN for offline verification capability. Valid values are as follows:<br>0 = Enciphered PIN for offline verification was not used for CVM by the terminal.<br>1 = Enciphered PIN for offline verification was used for CVM by the terminal. |

## Byte 3 (Security Capability)

| EMV Defined Bit Position | Description |
|---|---|
| 8 | Static data authentication capability. Valid values are as follows:<br>0 = Static data authentication security is not used by this terminal.<br>1 = Static data authentication security is used by this terminal. |
| 7 | Dynamic data authentication capability. Valid values are as follows:<br>0 = Dynamic data authentication security is not used by this terminal.<br>1 = Dynamic data authentication security is used by this terminal. |
| 6 | Card capture capability. Valid values are as follows:<br>0 = The terminal does not have card capture capability.<br>1 = The terminal does have card capture capability. |

## Byte 4

| | | | |
|---|---|---|---|
| 21–24 | 02 | USER-FLD1<br>This field is used to ensure word ılignment. | PIC X(4) |
| 25–32 | 02 | USER-FLD2<br>Must contain binary zeroes. | PIC X(8) |
| 3 3–34 | 02 | EMV-TERM-TYPE | PIC X(2) |

The EMV terminal type, indicating the environment of the terminal, its communications capability, and its operational control, as shown in the table below.

| | Control de Operación | | |
|---|---|---|---|
| **Ambiente** | **Institución** | **Comercio** | **Tarjeta Habiente** |
| Attended Terminal | | | |
| Online only | 11 | 21 | N/A |
| Offline with online capability | 12 | 22 | N/A |
| Offline only | 13 | 23 | N/A |
| Unattended Terminal | | | |
| Online only | 14 | 24 | 34 |
| Offline with online capability | 15 | 25 | 35 |
| Offline only | 16 | 26 | 36 |

35–38 02 APPL-VER-NUM PIC X(4)

The version number assigned by the payment system for the terminal application.

39–44 02 CVM-RSLTS PIC X(6)

The results of the last cardholder verification method (CVM) performed. Valid values are shown in the tables below. The default for all bit settings is a value of 0.

In the EMV specifications, definitions that include bit positions indicate that bit position 8 is the leftmost bit.

### Byte 1 (CVM Performed)

| EMV Defined Bit Position | Description |
|---|---|
| 7 | 0 = Fail cardholder verification if this cardholder verification method (CVM) is unsuccessful<br>1 = Apply succeeding card verification rule (CVR) if this CVM is usuccessful |
| 6–1 | 000000= Fail CVM processing<br>000001= Plaintext PIN verification performed by ICC<br>000010= Enciphered PIN verified online<br>000011= Plaintext PIN verification performed by ICC and signature (paper)<br>000100= Enciphered PIN verification performed by ICC<br>000101= Enciphered PIN verification performed by ICC and signature (paper)<br>0*xxxxx* = Values in the range 000110–011101 reserved for future use by the EMV specification<br>011110= Signature (paper)<br>011111= No CVM required<br>10*xxxx* = Values in the range 100000–101111 reserved for use by the individual payment systems<br>1 1*xxxx* = Values in the range 110000–111110 reserved for future use by the issuer<br>111111= Not available for use |

### Byte 2 (CVM Condition)

| Value | Description |
|---|---|
| 00 | Always |
| 01 | If cash or cashback |
| 02 | If not cash or cashback |
| 03 | If terminal supports the CVM |
| 04 | Reserved for future use |
| 05 | Reserved for future use |
| 06 | If transaction is in the application currency and is under *x* value |
| 07 | If transaction is in the application currency and is over *x* value |
| 08 | If transaction is in the application currency and is under *y* value |
| 09 | If transaction is in the application currency and is over *y* value |
| 0A–7F | Reserved for future use |
| 80–FF | Reserved for future use by individual payment systems |

### Byte 3 (CVM Result)

Result of the last CVM performed, as known by the terminal. Valid values are as follows:

| Value | Description |
|---|---|
| 0 | Unknown (for example, for signature) |
| 1 | Failed (for example, for offline PIN) |
| 2 | Successful (for example, for offline PIN) |

Bit positions not listed are reserved for future use.

**Caution:** In TAL programming, the highest order bit is the zero bit.

45–48 02 DF-NAME-LGTH PIC X(4)

The length of the dedicated file name or application identifier in the following field. The ASCII and binary versions of the token must contain the same value in this field. The ASCII version of the token must contain the decimal (not hexadecimal) representation of the length value.

49–80 02 DF-NAME PIC X(32)

The name of the dedicated file (as described in ISO/IEC 78 16-4) or application identifier (as described in ISO/IEC 78 16-5). The data is left-justified and padded to the right with binary zeroes.

## 4.3 TOKEN B4 STATUS TOKEN

**Message : 0200 y 0210**

The EMV Status token holds data identifying the status of a transaction. Device Handler and Interchange Interface processes create this token and add it to the STM before sending it to the Authorization process. The acquiring endpoint adds the token when the transaction originates from an EMV-capable terminal, regardless of whether or not the data relates to an EMV transaction.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification.*

El token B4 es muy importante ya que interviene tanto a nivel Adquirente como a nivel Emisor puesto que refleja el estatus de la transacción en EMV. A nivel emisor es Condicional, cuya regla para poder enviarlo es: siempre que el Emisor sea EMV FULL, deberá enviar este Token en las trasnacciones de respuesta.

**NOTA**: Es considerado que un Emisor es EMV FULL cuando puede hacer la lectura y procesamiento de los Tokens enviados por el Adquirente (B2, B3 y B4); así como responder el token B4, B5 y en su caso el token B6 (cuando se le está dando la instrucciones al chip la ejecución de los Scripts).

Cuando un Emisor recibe el token B4 y es EMV FULL debe hacer la actualización de cómo se procesó la transacción a nivel de EMV y responderle al Adquirente. A continuación se muestran **algunos de los valores principales** que el Emisor debe considerar procesar e incluir en la respuesta que genere para el Adquirente (**mas no exclusivo y/o limitativo**):

| B4 STATUS TOKEN | | | | | | |
|---|---|---|---|---|---|---|
| # | Longitud | Inicio | Fin | NOMBRE | TAG (DE 55) | |
| H-1 | 1 | 1 | 1 | EYE-CATCHER | | |
| H-2 | 1 | 2 | 2 | USER-FLD1 | | |
| H-3 | 2 | 3 | 4 | ID | | |
| H-4 | 5 | 5 | 9 | Longitud del token | | |
| H-5 | 1 | 10 | 10 | USER-FLD2 | | |
| 1 | 3 | 1 | 3 | PT-SRV-ENTRY-MDE | N/A | |
| 2 | 1 | 4 | 4 | TERM-ENTRY-CAP | N/A | |
| 3 | 1 | 5 | 5 | LAST-EMV-STAT | N/A | |
| 4 | 1 | 6 | 6 | DATA-SUSPECT | N/A | |
| 5 | 2 | 7 | 8 | APPL-PAN-SEQ-NUM | 5F34 | Emisor* |
| 6 | 6 | 9 | 14 | DEV-INFO | N/A | |
| 10 | 4 | 15 | 18 | RSN-ONL-CDE | N/A | |
| 11 | 1 | 19 | 19 | ARQC-VRFY | N/A | Emisor* |
| 12 | 1 | 20 | 20 | ISO-RC-IND | N/A | Emisor* |

| C | Longitud | Inicio | Fin | NOMBRE | |
|---|---|---|---|---|---|
| 7 | | 9 | 14 | CAM-FLAGS | |
| 7A | | | | CVM-RSLTS | |
| 7* | | | | ICHG-DEF | |
| 8 | 2 | 9 | 10 | APPRVD-RC | Emisor* |
| 9 | 4 | 11 | 14 | UNUSED | |

Siendo de los más representativos, el indicador de la validación del ARQC si fue fallido o exitoso.

**Descripción de los Campos :**

| # | Lenght | Descripción | Valor |
|---|---|---|---|
| 1–20 | | EMV-STAT-TKNX | |
| 1–3 | 02 | PT-SRV-ENTRY-MDE | PIC X(3) |

The point-of-service entry mode. This field indicates the manner in which the card details were entered at the device and the PIN entry capability of the terminal.

| | | | |
|---|---|---|---|
| 4 | 02 | TERM-ENTRY-CAP | PIC X(1) |

The capability of the terminal. This field is set by the acquiring process. Valid values are as follows:

**0** = Unknown
**2** = Magnetic stripe read capability
**5** = ICC read capability

| | | | |
|---|---|---|---|
| 5 | 02 | LAST-EMV-STAT | PIC X(1) |

Indicates whether the card used to initiate a magnetic stripe transaction is a chip card. Valid values are as follows:

**0** = Not a chip card

**1** = A chip card

| | | | |
|---|---|---|---|
| 6 | 02 | DATA-SUSPECT | PIC X(1) |

Indicates whether the card authentication method (CAM) data is reliable. This flag is set by the acquiring process. Valid values are as follows:

**0** = CAM data assumed correct
**1** = CAM data is unreliable

| | | | |
|---|---|---|---|
| 7–8 | 02 | APPL-PAN-SEQ-NUM | PIC X(2) |

The application PAN sequence number (EMV Tag 5F34). This field identifies and differentiates cards with the same PAN. This field contains spaces if the card does not include an application PAN sequence number.

| | | | |
|---|---|---|---|
| 9–14 | 02 | DEV-INFO | PIC X(6) |

The device information field. This field contains device-specific data.

| | | | |
|---|---|---|---|
| 9–14 | 02 | CAM-FLAGS | REDEFINES DEV-INFO |

Identifies conditions encountered at the terminal. Valid values are shown in the tables below. The default for all bit settings is a value of 0. This field is specific to ATM transactions.

This field is specific to an NCR terminal and is defined by NCR in the ***NCR NDC+ CAM 2 Functional Specification.***

The two bytes (16 flags) of CAM data defined in the NCR specification are converted to four bytes of ASCII hexadecimal data in the native message for transmission from the ATM. Each of the two bytes is split into four 4-bit units. Each 4-bit unit is represented in the low order four bits of each of the 4 bytes in the native message. The four bytes in the native message are moved directly into the first four bytes of this token field. Bit positions not listed are reserved for future use.

**Byte 1**

**Byte 1 as defined by NCR is moved into bytes 1 and 2 of this token field**.

| NCR<br>Defined Bit<br>Position | Description |
|---|---|
| 4 | Application data retrieval indicator. Valid values are as follows:<br>0 = Application data retrieval successful.<br>1 = Application data retrieval failed. |
| 3 | Get processing options indicator. Valid values are as follows:<br>0 = Get processing options successful.<br>1 = Get processing options failed. |
| 2 | Application selection indicator. Valid values are as follows:<br>0 = Application selection successful.<br>1 = Application selection failed. |

**Byte 2**

**Byte 2 as defined by NCR is moved into bytes 3 and 4 of this token field.**

| NCR Defined Bit Position | Description |
|---|---|
| 8 | Processing options data object list (PDOL) data flag: Valid values are as follows:<br>0 = PDOL data valid.<br>1 = PDOL data invalid. |
| 7 | Card risk management data object list (CDOL1) data flag. Valid values are as follows:<br>0 = CDOL1 data valid.<br>1 = CDOL1 data invalid. |
| 6 | Generate AC command flag. Valid values are as follows:<br>0 = Generate AC successful.<br>1 = Generate AC failed. |
| 4 | Card authentication method (CAM) processing flag. Valid values are as follows:<br>0 = CAM processing not yet successful.<br>1 = CAM processing previously successful. |
| 3 | Easy entry processing flag. Valid values are as follows:<br>0 = Easy entry processing initiated.<br>1 = Easy entry processing not initiated. |

| | |
|---|---|
| 2 | CAM processing initiated flag. Valid values are as follows:<br>0 = CAM processing initiated.<br>1 = CAM processing not initiated. |

Byte 5 and 6 of this token field are reserved for future use.

9–14 02 CVM-RSLTS REDEFINES DEV-INFO

The results of the last cardholder verification method (CVM) performed. Valid values are shown in the tables below. The default for all bit settings is a value of 0. This field is specific to POS transactions.

This field is defined as 24 bits (three bytes) by EMV, but is converted to six ASCII bytes, each containing one hexadecimal character representing four bits when included in the EMV Status token.

## Byte 1 (CVM Performed)

| EMV Defined Bit Position | Description |
|---|---|
| 7 | 0 = Fail cardholder verification if this cardholder verification method (CVM) is unsuccessful<br>1 = Apply succeeding card verification rule (CVR) if this CVM is unsuccessful |

| | |
|---|---|
| 6–1 | 000000= Fail CVM processing<br>000001= Plaintext PIN verification performed by ICC<br>000010= Enciphered PIN verified online<br>000011= Plaintext PIN verification performed by ICC and signature (paper)<br>000100= Enciphered PIN verification performed by ICC<br>000101= Enciphered PIN verification performed by ICC and signature (paper)<br>0*xxxxx* = Values in the range 000110–011101 reserved for future use by the EMV specification<br>011110= Signature (paper)<br>011111= No CVM required<br>10*xxxx* = Values in the range 100000–101111 reserved for use by the individual payment systems<br>11*xxxx* = Values in the range 110000–111110 reserved for future use by the issuer<br>111111= Not available for use |

## Byte 2 (CVM Condition)

| Value | Description |
|---|---|
| 00 | Always |
| 01 | If cash or cashback |
| 02 | If not cash or cashback |
| 03 | If terminal supports the CVM |
| 04 | Reserved for future use |

| | |
|---|---|
| 05 | Reserved for future use |
| 06 | If transaction is in the application currency and is under *x* value |
| 07 | If transaction is in the application currency and is over *x* value |
| 08 | If transaction is in the application currency and is under *y* value |
| 09 | If transaction is in the application currency and is over *y* value |
| 0A–7F | Reserved for future use |
| 80–FF | Reserved for future use by individual payment systems |

### Byte 3 (CVM Result)

Result of the last CVM performed, as known by the terminal. Valid values are as follows:

| Value | Description |
|---|---|
| 0 | Unknown (for example, for signature) |
| 1 | Failed (for example, for offline PIN) |
| 2 | Successful (for example, for offline PIN) |

Bit positions not listed are reserved for future use.

9–14 02 ICHG-DEF REDEFINES DEV-INFO

The interchange definition. This token is used by the VisaNet Interface only.

9–10 04 APPRVD-RC PIC X(2)

In some authorization requests received via the VisaNet Interface, this field contains the Authorization Response Code (ARC) required for Authorization Response Cryptogram (ARPC) generation.

11–14 04 UNUSED PIC X(4)

This Field reserved for future use.

15–18 02 RSN-ONL-CDE PIC X(4)

The message reason code specifies why a transaction is to be authorized online (rather than being completed locally), or why a transaction has been completed locally (rather than being authorized online). Values are defined in the for ***ISO 8583 (1993) Standard.*** *Refer to the **ACI Standard POS Device Message Specifications Manual***

In a request message, the valid values are as follows:

| Value | Description |
|---|---|
| 1500 | ICC application, common data file unable to process |
| 1501 | ICC application, application data file unable to process |
| 1502 | ICC random selection |
| 1503 | Terminal random selection |
| 1504 | Terminal not able to process ICC |
| 1505 | Online forced by ICC (CDF or ADF) |

| | |
|---|---|
| 1506 | Online forced by card acceptor |
| 1507 | Online forced by CAD to be updated |
| 1508 | Online forced by terminal |
| 1509 | Online forced by issuer |
| 1510 | Over floor limit |
| 1511 | Merchant suspicious |

In an advice message that the terminal previously has attempted to send to the acquirer as a request message, this field contains the same value as in the original request message.

In an advice message that the terminal previously has not attempted to send to the acquirer as a request message, the valid values are as follows:

| Value | Description |
|---|---|
| 1004 | Terminal processed |
| 1005 | ICC processed |
| 1006 | Under floor limit |
| 1007 | Stand-in processing at the acquirer's option |

19 02 ARQC-VRFY PIC X(1)

The result of the authorization request cryptogram verification. Valid values are as follows:

**0** = Authorization request cryptogram not verified

**1** = Authorization request cryptogram was checked by acquiring system but failed verification

**2** = Authorization request cryptogram was checked by acquiring system and passed verification

**3** = Authorization request cryptogram was checked by BASE24 but failed verification

**4** = Authorization request cryptogram was checked by BASE24 and passed verification

**9** = Authorization request cryptogram not verified; transaction processed as magnetic stripe instead of chip

20 02 ISO-RC-IND PIC X(1).

The ISO 8583 (1987) Response Code Indicator. This field indicates whether the ISO response code sent to the interchange should be used in generating the Authorization Response Cryptogram (ARPC), or if the ISO response code

received from the interchange should be returned to the terminal as the Authorization Response Code. Valid values are as follows:

**b-** = No information available (where b- indicates a blank space)

**0** = Do not use interchange response code

For EMV transactions where BASE24 is the issuer:

**1** = Use supplied response code in ARPC generation for approved transactions

For EMV transactions where BASE24 is the acquirer:

**9** = Use interchange response code as ARC sent to terminal

## 4.4 TOKEN B5 RESPONSE DATA TOKEN

**Message : 0210**

The EMV Response Data token contains the response cryptogram, data required to generate the response cryptogram, and flags used to identify the scripts to be returned to the acquirer. If authorization is performed on BASE24, the BASE24 Authorization process creates this token. If the transaction is routed to an interchange for authorization, the BASE24 Interchange Interface process creates the token.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification.*

**Descripción de los Campos :**

| # | Lenght | Descripción | Valor |
|---|---|---|---|
| 1–38 | | EMV-RESP-TKNX | |
| 1–4 | 02 | ISS-AUTH-DATA-LGTH | PIC X(4) |
| | | The length of the binary representation of the data in the following field. The ASCII and binary versions of the token must contain the same value in this field. The ASCII version of the token must contain the decimal (not hexadecimal) representation of the length value | |
| | 02 | EMV-ISS-AUTH-DATA | PIC X(32) |
| | | The data is left-justified and padded to the right with binary zeroes. | |
| | 02 | ISS-AUTH-DATA | REDEFINES EMV-ISS-AUTH-DATA Issuer |
| | | authentication data (EMV Tag 91) sent to the ICC foronline issuer authentication. | |
| 5–20 | 04 | ARPC | PIC X(16) |

The authorization response cryptogram computed by the card application for online issuer authentication.

| | | | |
|---|---|---|---|
| 21–36 | 04 | ADDL-DATA | PIC X(16) |
| | | Additional issuer authentication data used in the algorithm to compute the authorization response cryptogram.<br>BASE24 currently supports the following definitions for additional issuer data. For more information on these fields, refer to DDL documentation or the individual card scheme documentation. | |
| 21–36 | 04 | VISA-ADDL-DATA | REDEFINES ADDL-DATA The |
| | | Visa/UKIS definition of the additional issuer authentication data. | |
| 21–24 | 06 | ISS-RESP-CDE | PIC X(4) |
| 25–36 | 06 | INFO | PIC X(12 |
| 21–36 | 04 | MCPA-ADDL-DATA | REDEFINES ADDL-DATA The |
| | | M/Chip 2.1 definition of the additional issuer authentication data. | |
| 21–24 | 06 | ISS-AUTH-RESP-CDE | PIC X(4) |
| 25–36 | 06 | INFO | PIC X(12) |
| 21–36 | 04 | MCHIP4-ADDL-DATA | REDEFINES ADDL-DATA The |
| | | M/Chip 4 definition of the additional issuer authentication data. | |
| 21–24 | 06 | ARPC-RESP-CDE | PIC X(4) |
| 25–36 | 06 | INFO | PIC X(12) |
| 21–36 | 02 | CCD-A-AUTH-DATA | REDEFINES EMV-ISS-AUTH-DATA |
| 5–12 | 04 | ARPC | PIC X(8) |

13–20 04 CRD-STAT-UPDT PIC X(8)

21–36 04 ADDL-DATA PIC X(16)

37 02 SEND-CRD-BLK PIC X(1)

A code indicating whether a card block script is to be generated by the Authorization process and sent to the ICC. Valid values are as follows:

**C** = Send a PIN change script  
**N** = No, do not send a card block script  
**U** = Send a PIN unblock script  
**Y** = Yes, send a card block script

38 02 SEND-PUT-DATA PIC X(1)

A code indicating whether a put data script is to be generated by the Authorization process and sent to the ICC. Valid values are as follows:

**Y** = Yes, send a put data script

**N** = No, do not send a put data script

## 4.5 TOKEN B6 SCRIPT DATA TOKEN

**Message : 0210**

The EMV Script Data token holds EMV script data. The issuer process creates this token. In the context of EMV transactions, the issuer process can be an Interchange Interface process if the issuer is external to BASE24, or the Authorization process if BASE24 is configured for offline or online/offline authorization. The token is added to the STM before returning the message to the acquiring process. This token is present only if the transaction response contains script data.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification.*

**Note:** The EMV Script Data token is variable length. The values given are the maximum lengths.

**Descripción de los Campos :**

| # | Lenght | Descripción | valor |
|---|---|---|---|
| 1–260 | | EMV-SCRIPT-TKNX | |
| 1–4 | 02 | ISS-SCRIPT-DATA-LGTH<br>The length of the binary representation of the data in the following field. The ASCII and binary versions of the token must contain the same value in this field. The ASCII version of the token must contain the decimal (not hexadecimal) representation of the length value. | PIC X(4) |
| 5–260 | 02 | ISS-SCRIPT-DATA<br>The Issuer Script Templates (EMV Tag 71 and/or 72) sent to the terminal for processing by the card application. Each template may contain a script ID and one or more script commands. If generated by BASE24, this field includes a single Issuer Script Template, containing only one script command. The data is left-justified and padded to the right with binary zeroes. | PIC X(256) |

## 4.6 TOKEN BJ EMV Issuer Script Results Token (Only if is Necessary)

**Message :0200 (Respuesta Script** *se envía la respuesta en la siguiente transacción después de haberla recibido* **)**

**0220 (Respuesta a nivel criptograma** *este se aplica cuando hay sincronización de llaves en caso de no lograrlo enviara inmediatamente este mensaje.***)**

The EMV Issuer Script Results token holds information about the processing of EMV Script data. This token is created by the acquirer interface process (e.g.,Device Handler or Interchange Interface) or sent by the acquirer. It contains information about the results of EMV Script processing.

*For more information about the EMV data elements refer to the MasterCard M/Chip or the Visa Smart Debit Credit (VSDC) documentation sets or the EMVCo specification*.

NOTA: Este token es empleado por parte del Adquirente para darle comentarios al Emisor si se logró o no efectuar los scripts ordenados al chip a través del token B6**.**

| Position | Level | Field Name and Description | Data Type |
|---|---|---|---|
| | 1–82 | EMV-ISS-SCRIPT-RSLTS-TKN | |
| 1 | 02 | NUM-ISS-SCRIPT-RSLTS<br>The number of completed issuer script results contained within the token. | PIC X(1) |
| 2 | 02 | USER-FLD1<br>PIC X(1) For future use within the token. | |
| 3–82 | 02 | ISS-SCRIPT-RSLTS-DATA OCCURS 8 TIMES | |
| 3 | 04 | ISS-SCRIPT-PROC-RSLT<br>A code indicating the result of the script processing. Valid values are as follows:<br>**0** = Script not performed<br>**1** = Script processing failed<br>**2** = Script processing successful<br>**9** = Script processing unknown | PIC X(1) |
| 04 | 04 | ISS-SCRIPT-SEQ<br>The details of the Script Sequence in the processing. Valid values are as follows:<br>**0** = Script sequence not specified, script not performed, all commands successful.<br>**1–9, A–E** = Sequence number from 1–14 for failed<br>**F** = Sequence number if 15 or over for failed command**.** | PIC X(1) |
| 5–12 | 04 | ISS-SCRIPT-ID | PIC X(8) |

The issuer script
identifier.

# Consideraciones relevantes en transacciones de ATMs:

## Transacciones de Retiro, Venta genérica, cambio d eNIP y consulta

### Campos en una transacción de retiro y consulta utilizando el chip EMV

| | 0200 | 0210 |
|---|---|---|
| Pos Entry Mode 22 | M | |
| Terminal Capability | M | |
| Chip Condition Code (B4) | M | M |
| PAN Sequence Number 23 | M | M |

## Transacciones de reversos parciales y totales:

### Campos en una transacción de reverso parciales y totales utilizando el chip EMV no aplica la presencia de tokens EMV.

| | 0420 | 0430 |
|---|---|---|
| Pos Entry Mode 22 | M | |

# Documentos de Referencia

1. Directrices estándar para el intercambio de indicadores EMV en transacciones de Cajeros Automáticos
2. Especificación Técnicoa: Mensajería FULL EMV entre Switches ATMs

-------------FIN DEL DOCUMENTO -----------------