EMV Swipe Specification

Jimmy Tang, Derek Chan

7/10/2013

Version 3.10

Revision Sheet

Date	Revision	Author	Description	Checked
2013-05-01	1.0	Nicole	Initial Draft	Derek
2013-05-09	2.0	Nicole	Add details for packing algorithm in ENCRYPTED TRACK DATA	Derek
2013-09-18	3.0	Derek	Update Track format, key management, and encryption mode.	Jimmy
2013-10-07	3.1	Jimmy	Update	Derek

Table of Content

1. Encryption

Unless otherwise specified, **Triple DES encryption** with **CBC** with **DUKPT** key management is assumed.

i. Encrypted track data

Unless otherwise specified, **Data key** (ANSI 9.24-1 2009) is assumed.

Padding algorithm: Zero Padding

ii. Encrypted online PIN block

Unless otherwise specified, **PIN key** is assumed.

ISO 9654 Format 0 is used for online PIN.

iii. Encrypted Online message/ Encrypted Batch Data Capture/Encrypted Reversal

Unless otherwise specified, **Data key** (ANSI 9.24-1 2009) is assumed.

Padding algorithm: PKCS 7

2. Message Format

Messages within data communication protocols of EMV chip card transactions are encoded as a **BER-TLV** (Basic Encoding Rules- Tag-Length-Value) as defined in ISO/IEC 8825.

i. Encoding Structure

Identifier octets	Length octets	Contents octets
Type	Length	Value

ii. Tag field

The tag field (T) consists of one or more consecutive bytes. It indicates a class, a type, and a number. The tag field of the data objects described in this specification is coded on one or two bytes. The bit 1-5 indicates if there is a 2nd byte tag value or not.

Coding of the Tag

b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Explanation**
0	0							Universal class
0	1							Application class
1	0							Context specific class
1	1							Private class
		0						Primitive data object
		1						Constructed data object
			x	x	x	x	x	Tag Value
			1	1	1	1	1	There is a 2nd byte with tag value

Optional Byte:

b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**	**Explanation**
0								This is the last Tag byte
1								Have another Tag byte
	x	x	x	x	x	x	x	Tag Value

iii. Length field

The length field (L) consists of one or more consecutive bytes. It indicates the length of the following field. The length field of the data objects described in this specification which are transmitted over the card-terminal interface is coded on one, two or three bytes.

Coding of the Length field

Byte	Length	Coding
1	0-127	0xxx xxxx
2	128-255	1000 0001 xxxx xxxx
3	256-65535	1000 0010 xxxx xxxx xxxx xxxx

iv. Value field

The value field (V) indicates the value of the data object. If L = '00', the value field is not present.

3. Proprietary tags description

Tag	Description	Length(Bytes)
0xC0	KSN of Online message	10
0xC1	KSN of Online PIN	10
0xC2	Enc. Online message (EMV Key)	Var.
0xC3	KSN of Batch/Reversal	10
0xC4	Masked PAN	0-10.
0xC5	Enc. Batch message (EMV Key)	Var.
0xC6	Enc. Reversal message (EMV Key)	Var.
0xC7	KSN of Encrypted Tag 57	10
0xC8	Encrypted Tag 57 (Track Key)	Var.

The tags C0 – C8 are returned by the EMV process and appear in online request message, EMV batch data and reversal message.

The function getEmvCardData returns these tags C3, C4 and C5.

4. Tags included

The reader now included the below EMV standards tags in onRequestOnlineProcess, onReturnBatchData.

The existence of tags which sourced from ICC depends on ICC card.

Tag	Name	Description	Source
4F	Application Identifier (AID) – card	Identifies the application as described in ISO/IEC 7816-5	ICC
50	Application Labe	Mnemonic associated with the AID according to ISO/IEC 7816-5	ICC
57	Track 2 Equivalent Data	Contains the data elements of track 2 according to ISO/IEC 7813, excluding start sentinel, end sentinel, and Longitudinal Redundancy Check (LRC), as follows: Primary Account Number (n, var. up to 19) Field Separator (Hex 'D') (b) Expiration Date (YYMM) (n 4) Service Code (n 3) Discretionary Data (defined by individual payment systems) (n, var.) Pad with one Hex 'F' if needed to ensure whole bytes (b)	ICC
5A	Application Primary Account Number (PAN)	Valid cardholder account number	ICC
5F 20	Cardholder Name	Indicates cardholder name according to ISO 7813	ICC
5F 24	Application Expiration Date	Date after which application expires	ICC
5F 25	Application Effective Date	Date from which the application may be used	ICC
5F 30	Service Code	Service code as defined in ISO/IEC 7813 for track 1 and track 2	ICC
5F 34	Application Primary Account Number (PAN) Sequence Number	Identifies and differentiates cards with the same PAN	ICC

5F2A	Transaction Currency Code	Indicates the currency code of the transaction according to ISO 4217	Terminal
82	Application Interchange Profile	Indicates the capabilities of the card to support specific functions in the application	ICC
84	Dedicated File (DF) Name	Identifies the name of the DF as described in ISO/IEC 7816-4	ICC
89	Authorisation Code	Value generated by the authorisation authority for an approved transaction	Issuer
8A	Authorisation Response Code	Code that defines the disposition of a message	Issuer/Terminal
8E	Cardholder Verification Method (CVM) List	Identifies a method of verification of the cardholder supported by the application	ICC
95	Terminal Verification Results	Status of the different functions as seen from the terminal	Terminal
99	Transaction Personal Identification Number (PIN) Data	Data entered by the cardholder for the purpose of the PIN verification	Terminal
9A	Transaction Date	Local date that the transaction was authorised	Terminal
9B	Transaction Status Information	Indicates the functions performed in a transaction	Terminal
9C	Transaction Type	Indicates the type of financial transaction, represented by the first two digits of ISO 8583:1987 Processing Code	Terminal
9F 02	Amount, Authorised (Numeric)	Authorised amount of the transaction (excluding adjustments)	Terminal
9F 03	Amount, Other (Numeric)	Secondary amount associated with the transaction representing a cashback amount	Terminal
9F 06	Application Identifier (AID) – terminal	Identifies the application as described in ISO/IEC 7816-5	Terminal
9F 07	Application Usage Control	Indicates issuer’s specified restrictions on the geographic usage and services allowed for the application	ICC
9F 09	Application Version Number	Version number assigned by the payment system for the application	Terminal

9F0D	Issuer Action Code – Default	Specifies the issuer's conditions that cause a transaction to be rejected if it might have been approved online, but the terminal is unable to process the transaction online	ICC
9F 0E	Issuer Action Code – Denial	Specifies the issuer's conditions that cause the denial of a transaction without attempt to go online	ICC
9F 0F	Issuer Action Code – Online	Specifies the issuer's conditions that cause a transaction to be transmitted online	ICC
9F 10	Issuer Application Data	Contains proprietary application data for transmission to the issuer in an online transaction	ICC
9F 12	Application Preferred Name	Preferred mnemonic associated with the AID	ICC
9F 16	Merchant Identifier	When concatenated with the Acquirer Identifier, uniquely identifies a given merchant	Terminal
9F1A	Terminal Country Code	Indicates the country of the terminal, represented according to ISO 3166	Terminal
9F 1E	Interface Device (IFD) Serial Number	Unique and permanent serial number assigned to the IFD by the manufacturer	Terminal
9F 26	Application Cryptogram	Cryptogram returned by the ICC in response of the GENERATE AC command	ICC
9F 27	Cryptogram Information Data	Indicates the type of cryptogram and the actions to be performed by the terminal	ICC
9F 33	Terminal Capabilities	Indicates the card data input, CVM, and security capabilities of the terminal	Terminal
9F 34	Cardholder Verification Method (CVM) Results	Indicates the results of the last CVM performed	Terminal
9F 35	Terminal Type	Indicates the environment of the terminal, its communications capability, and its operational control	Terminal
9F 36	Application Transaction Counter (ATC)	Counter maintained by the application in the ICC (incrementing the ATC is managed by the ICC)	ICC
9F 37	Unpredictable Number	Value to provide variability and uniqueness	Terminal

		to the generation of a cryptogram	
9F 39	Point-of-Service (POS) Entry Mode	Indicates the method by which the PAN was entered, according to the first two digits of the ISO 8583:1987 POS Entry Mode	Terminal
9F 40	Additional Terminal Capabilities	Indicates the data input and output capabilities of the terminal	Terminal
9F 41	Transaction Sequence Counter	Counter maintained by the terminal that is incremented by one for each transaction	Terminal
9F 4E	Merchant Name and Location	Indicates the name and location of the merchant	Terminal
9F 53	Transaction Category Code	Transaction Category Code	Terminal

5. Encrypted track data

i. Magnetic Stripe Encoding

Track	Character configuration (Including parity bit)	Information Content (Including control characters)
1	7 bits per character	79 alphanumeric characters
2	5 bits per character	40 numeric characters
3	5 bits per character	107 numeric characters

ii. Track 1 data format

The data is in ASCII format. Unless otherwise specified, track 1 data will be padded with zero.

iii. Track 2 data format

The data is in BCD format. That's 2 characters are packed into 1 byte.
Unless otherwise specified, track 2 data will be padded with zero to form 8 byte block for encryption.

Each character in track 2 is 4 bits in length. When data are in plain text format, add 0x30 to each nibble to convert it into ASCII. You can also use the following table to decode A, B, C, D, E and F

HEX	ASCII
0xA	:
0xB	;
0xC	<
0xD	=
0xE	>
0xF	?

If track data is present but fail to decode, the track data will be filled with all zero.

iv. Track 3 data format

The format of track 3 is the same as Track 2

6. Encrypted online PIN block

The PIN block is constructed by XORing two 64-bit fields: the *plain text PIN field* and the *account number field*, both of which comprise 16 four-bit nibbles.

The plain text PIN field is:

- one nibble with the value of 0, which identifies this as a format 0 block
- one nibble encoding the length *N* of the PIN
- *N* nibbles, each encoding one PIN digit
- 14−*N* nibbles, each holding the "fill" value 15

The account number field is:

- four nibbles with the value of zero
- 12 nibbles containing the right-most 12 digits of the primary account number (PAN), excluding the check digit