Errata for EMV Book C-2 (Version 2.6)

This Specification Bulletin contains modifications for Book C-2.

This Specification Bulletin describes proposed changes to the EMV® Integrated Circuit Card Specifications for Payment Systems.

Applicability

This Specification Bulletin applies to:

- *EMV Contactless Specifications for Payment Systems, Book C-2, Kernel 2 Specification, Version 2.6, February 2016*

Related Documents

- *EMV® Specification Bulletin No. 195, February 2017 — Errata for EMV Book C-2 (Version 2.6)*

Effective Date

- *1 January 2019*

Description

This Specification Bulletin describes the following changes to EMV Book C-2:

1. Modification to processing logic to protect against bad configuration data for RRP in Kernel or cardholder device
2. Reinstate missing text from step S910.53
3. Definition of Kernel Configuration data object
4. Clarification of format checking of track data in Magstripe mode transaction
5. Clarification of format checking of response to Get Processing Options command
6. Clarification of format checking of response to Generate AC command
7. Clarification of data format in response to Exchange Relay Resistance Data
8. Definition of POS Cardholder Interaction Information data object

1. Relay Resistance Protocol - Bad Configuration Data

If either of the data objects
- *Device Estimated Transmission Time for Relay Resistance R-APDU*, or
- *Terminal Expected Transmission Time For Relay Resistance R-APDU*

has the value of zero, then the Kernel should consider that Relay Resistance checks have been performed and thresholds exceeded.

The processing of step SR1.30 is modified as shown:

IF   [(*Device Estimated Transmission Time For Relay Resistance R-APDU ≠ 0*)
   AND
   (*Terminal Expected Transmission Time For Relay Resistance R-APDU ≠ 0*)]
THEN
       IF   [(((*Device Estimated Transmission Time For Relay Resistance R-APDU* * 100) div *Terminal Expected Transmission Time For Relay Resistance R-APDU*) < *Relay Resistance Transmission Time Mismatch Threshold*)
          OR
          (((*Terminal Expected Transmission Time For Relay Resistance R-APDU* * 100) div *Device Estimated Transmission Time For Relay Resistance R-APDU*) < *Relay Resistance Transmission Time Mismatch Threshold*)
          OR
          (MAX(0, (*Measured Relay Resistance Processing Time – Min Time For Processing Relay Resistance APDU*)) > *Relay Resistance Accuracy Threshold*)]
       THEN
          GOTO SR1.31
       ELSE
          GOTO SR1.32
       ENDIF
ELSE
       GOTO SR1.31
ENDIF

2. Reinstate missing text

The text indicated below was incorrectly removed from step S910.53 in version 2.6 of EMV Book C-2. It is reinstated as shown.

<u>S910.53</u>

'Status' in *Outcome Parameter Set* := END APPLICATION

'Msg On Error' in *Error Indication* := ERROR – OTHER CARD

CreateEMVDiscretionaryData ()

SET 'UI Request on Outcome Present' in *Outcome Parameter Set*

Send OUT(GetTLV(TagOf(*Outcome Parameter Set*)), GetTLV(TagOf(*Discretionary Data*)), GetTLV(TagOf(*User Interface Request Data*))) Signal

3. Definition of Kernel Configuration

The definition of the Kernel Configuration data object is modified as follows:

A.1.91   Kernel Configuration

Tag: 'DF811B'

Template: —

Length: 1

Format: b

Update: K

Description: Indicates the Kernel configuration options.

Kernel Configuration		
Byte 1	b8	Mag-stripe mode contactless transactions not supported
	b7	EMV mode contactless transactions not supported
	b6	On device cardholder verification supported
	b5	Relay resistance protocol supported
	<u>b4</u>	<u>Reserved for Payment System</u>
	b<u>3</u>-1	Each bit RFU

4. Clarification of Format Checking of Track Data

The last paragraph in step S7.22 is modified as shown here:

> However, if the Kernel is not able to localize ~~a required data field in~~ the discretionary part of *Track 1 Data* or *Track 2 Data* due to one or more format errors, the Kernel must terminate the transaction as described in S7.24.1.

5. Clarification of Format Checking of Get Processing Options Response

The structure of a format 1 response to the GET PROCESSING OPTIONS command is clarified in Table 5.19 as shown:

Table Error! No text of specified style in document.**.1—Get Processing Options Response Message Data Field (Format 1)**

Tag	Length	Value	Presence
'80'	Var.	*Application Interchange Profile*	M
		Application File Locator	M

The processing of the response to the GET PROCESSING OPTIONS command in step 3.10 is clarified as follows:

S3.10

Parsing Result := FALSE

IF   [(Length of Response Message Data Field > 0) AND
       (Response Message Data Field[1] = '77')]

THEN

     Parsing Result := ParseAndStoreCardResponse(Response Message Data Field)

ELSE

     IF   [(Length of Response Message Data Field > 0) AND (Response Message Data Field[1] = '80')]

     THEN

       Parse the Response Message Data Field according to section 5.6.3 to retrieve the value field as follows:

       IF   [Response Message Data Field does not parse correctly OR
         The length of the value field of the Response Message Data Field is less than 6 OR

         ……

6. Clarification of Format Checking of Generate AC Response

The structure of a format 1 response to the GENERATE AC command is clarified in Table 5.19 as shown:

Table Error! No text of specified style in document.**.2—Generate AC Response Message Data Field (Format 1)**

Tag	Length	Value	Presence
'80'	Var.	*Cryptogram Information Data*	M
		Application Transaction Counter	M
		Application Cryptogram	M
		Issuer Application Data	O

The processing of the response to the GENERATE AC command in step 9.18 is clarified as follows:

S9.18

Parsing Result := FALSE
IF   [(Length of Response Message Data Field > 0) AND (Response Message Data Field[1] = '77')]
THEN
     Parsing Result := ParseAndStoreCardResponse(Response Message Data Field)
ELSE
     IF   [(Length of Response Message Data Field > 0) AND (Response Message Data Field[1] = '80')]
     THEN
          Parse the Response Message Data Field according to section 5.4.3 to retrieve the value field
          ~~Retrieve *Cryptogram Information Data, Application Transaction Counter, Application Cryptogram* and *Issuer Application Data* from Response Message Data Field according to section 5.4.3 as follows:~~
          IF   [Response Message Data Field does not parse correctly OR
               The length of the value field of the Response Message Data Field is less than 11 OR
               …

The processing of the response to the GENERATE AC command in step 11.8 is clarified as follows:

S11.8

Parsing Result := FALSE
IF   [(Length of Response Message Data Field > 0) AND (Response Message Data Field[1] = '77')]
THEN
     Parsing Result := ParseAndStoreCardResponse(Response Message Data Field)
ELSE
     IF   [(Length of Response Message Data Field > 0) AND (Response Message Data Field[1] = '80')]
     THEN
          Parse the Response Message Data Field according to section 5.4.3 to retrieve the value field

~~Retrieve *Cryptogram Information Data, Application Transaction Counter, Application Cryptogram* and *Issuer Application Data* from Response Message Data Field according to section 5.4.3 as follows~~:

IF   [Response Message Data Field does not parse correctly OR
        The length of the value field of the Response Message Data Field is less than 11 OR
        …

7. Clarification of Response to Exchange Relay Resistance Data

The structure of the response to the EXCHANGE RELAY RESISTANCE DATA command is clarified in Table 5.7 as shown:

Table Error! No text of specified style in document.**.3—Exchange Relay Resistance Data Response Message Data Field**

Tag	Length	Byte	Value	Presence
'80'	'0A'	1-4	*Device Relay Resistance Entropy*	M
		5-6	*Min Time For Processing Relay Resistance APDU*	M
		7-8	*Max Time For Processing Relay Resistance APDU*	M
		9-10	*Device Estimated Transmission Time For Relay Resistance R-APDU*	M

8. Definition of POS Cardholder Interaction Information

The definition of the POS Cardholder Interaction Information data object in section A.1.124 is modified as shown:

POS Cardholder Interaction Information		
Byte 1	b8-1	Version Number
Byte 2	b8-6	Each bit RFU
	b5	OD-CVM verification successful
	b4	Context is conflicting
	b3	Offline change PIN required
	b2	ACK required
	b1	OD-CVM required
Byte 3	b8-2~~1~~	Each bit RFU
	1	Wallet requires second tap

The default value for the Phone Message Table in Table 4.4 is updated as shown:

Table Error! No text of specified style in document.**.4—Phone Message Table – Default Value**

PCII Mask	PCII Value	Message Identifier	Status
'000001'	'000001'	SEE PHONE	NOT READY
'000800'	'000800'	SEE PHONE	NOT READY
'000400'	'000400'	SEE PHONE	NOT READY
'000100'	'000100'	SEE PHONE	NOT READY
'000200'	'000200'	SEE PHONE	NOT READY
'000000'	'000000'	DECLINED	NOT READY

Legal Notice

The EMV® Specifications are provided "AS IS" without warranties of any kind, and EMVCo neither assumes nor accepts any liability for any errors or omissions contained in these Specifications. EMVCO DISCLAIMS ALL REPRESENTATIONS AND WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT, AS TO THESE SPECIFICATIONS.

EMVCo makes no representations or warranties with respect to intellectual property rights of any third parties in or in relation to the Specifications. EMVCo undertakes no responsibility to determine whether any implementation of the EMV® Specifications may violate, infringe, or otherwise exercise the patent, copyright, trademark, trade secret, know-how, or other intellectual property rights of third parties, and thus any person who implements any part of the EMV® Specifications should consult an intellectual property attorney before any such implementation.

Without limiting the foregoing, the Specifications may provide for the use of public key encryption and other technology, which may be the subject matter of patents in several countries. Any party seeking to implement these Specifications is solely responsible for determining whether its activities require a license to any such technology, including for patents on public key encryption technology. EMVCo shall not be liable under any theory for any party's infringement of any intellectual property rights in connection with the EMV® Specifications.