CPACE Kernel Specification Update

This specification Update applies to CPACE-Kernel Specification Version 1.0 12.07.2018.

This bulletin is effective immediately

Description **#1**

External References

EMV Contactless Specification Book D v2.7, 2018 has never been published. Current version is v3.0, dated February 2018.

Specification Change

Section 2.1 Reference

Replace the entry for EMV Book D with:

EMV® Level 1 Specifications for Payment Systems, EMV Contactless Interface Specification, Version 3.0 - February 2018.

Description **#2**

In order to achieve required transaction execution time, contactless kernels often parallelize the processing. The READ RECORD response is being processed while in parallel a next READ RECORD command is being sent. This behaviour is not described in the requirements of Book 3 – Section 10.2.

Specification Change

Section 11 – Read Application Data:

Add the below sentence:

It is allowed to parallelize the processing of a card response to a READ RECORD command, and the sending of the next READ RECORD command.

Description **#3**

In Section 12.2 (*Modifications in [EMV Book 2] Section 6.6*) with changes related to Section 6.6.1 in the EMV specification, both Format 1 and Format 2 response templates are allowed. To align with the CPA specification, Format 1 shall not be allowed.

Specification Change

On p.38:

3. If the terminal did not request an AAC, or CDA on AAC is not supported by the ICC, and the ICC responds with an AAC, the ICC response shall be coded according to ~~either format 1 or~~ format 2 as specified in section 6.5.5.4 of Book 3 and shall contain at least the mandatory data elements specified in Table 21, and optionally the Issuer Application Data.

Description **#4**

The presence of the Issuer Application Data in the Generate AC response is not consistent throughout the specification. It is marked as mandatory in Table 8 and Table 9 and it is mandatory according to the checks in Section 17. However, in Section 12.2 (*Modifications in [EMV Book 2] Section 6.6*) with changes related to Section 6.6.1 in the EMV specification, it is defined as optional.

Specification Change

In Section 7.2, change the Presence condition of the Issuer Application Data in Table 8:

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F26'	*Application Cryptogram (AC)*	M
	'9F10'	*Issuer Application Data (IAD)*	~~M~~ O
	'DF4B'	*Cardholder Verification and Confirmation Status (CHV&CS)*	O

Change the Presence condition of the Issuer Application Data in Table 9:

Tag	Value		Presence
'77'	*Response Message Template Format 2*		M
	'9F27'	*Cryptogram Information Data (CID)*	M
	'9F36'	*Application Transaction Counter (ATC)*	M
	'9F4B'	*Signed Dynamic Application Data (SDAD)*	M
	'9F10'	*Issuer Application Data (IAD)*	~~M~~ O
	'DF4B'	*Cardholder Verification and Confirmation Status (CHV&CS)*	O

In Section 17, change

If **all** the following are true:
- SW1 SW2 = '9000' is returned in the response to GENERATE AC
- **and** *Cryptogram Information Data* is returned in the response to GENERATE AC
- **and** *Application Transaction Counter* is returned in the response to GENERATE AC
- ~~**and** *Issuer Application Data* is returned in the response to GENERATE AC~~
- **and any** of the following is true:
  - an AAC is returned
  - **or** a TC is returned and the Kernel requested a TC
  - **or** an ARQC is returned and the Kernel requested a TC or ARQC

…

Description **#5**

In Table 22 (*Application Interchange Profile (AIP) Coding*):

Byte 1- b1 is set to "Not Used". This is not in line with the AIP as defined in the CPACE DIC specification.

Byte 2–b6 is set to "HCE Supported". This is not in line with the AIP as defined in the CPACE HCE specification.

Specification Change (if any)

Byte	b8	b7	b6	b5	b4	b3	b2	b1	Meaning
1	x	-	-	-	-	-	-	-	RFU
	-	x	x	-	-	-	-	-	Not Used
	-	-	-	x	-	-	-	-	Cardholder Verification Supported
	-	-	-	0	-	-	-	-	Cardholder Verification is not Supported
	-	-	-	1	-	-	-	-	Cardholder Verification Supported
	-	-	-	-	x	-	-	-	Terminal risk management is to be Performed
	-	-	-	-	0	-	-	-	Terminal risk management is not to be Performed
	-	-	-	-	1	-	-	-	Terminal risk management is to be Performed
	-	-	-	-	-	0	-	-	Issuer Authentication using EXTERNAL AUTHENTICATE is not Supported
	-	-	-	-	-	-	x	-	CDCVM is Supported
	-	-	-	-	-	-	0	-	CDCVM is not Supported
	-	-	-	-	-	-	1	-	CDCVM is Supported
	-	-	-	-	-	-	-	x	CDA supported~~Not Used~~
	-	-	-	-	-	-	-	0	CDA is not supported/not used
	-	-	-	-	-	-	-	1	CDA is supported
2	1	-	-	-	-	-	-	-	EMV Mode is Supported
	~~-~~	~~x~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~Not Used~~

	~~-~~	~~-~~	~~1~~	~~-~~	~~-~~	~~-~~	~~-~~	~~-~~	~~HCE is Supported~~
	-	~~x-~~	~~x-~~	x	x	x	x	-	RFU
	-	-	-	-	-	-	-	x	Relay Resistance Protocol Support
								0	Relay Resistance Protocol not Supported
								1	Relay Resistance Protocol Supported

Description **#6**

Section 21.3 Erroneous or missing data contains a cross-check between PAN and Track 2 equivalent Data. If values don't match, the control is returned to Entry Point. This cross-check is not present in other kernels, nor in the contact card processing flow. To align with the contact card processing flow, the cross-check is removed.

Specification Change (if any)

This section describes how the Kernel shall behave when the transaction is to be terminated due to erroneous or missing data:

If, during transaction processing, any of the following is true:

- The application of the rules defined in [EMV Book 3] Section 7.5, results in transaction termination
- ~~Or the Application PAN (tag '5A') does not match the Primary Account Number contained in Track 2 Equivalent data (tag '57'), if present in the card~~
- Or a mandatory data object is missing in a command response
- Or a command response does not parse correctly
- Or the transaction has to be terminated according to the EMV specification

Then the Kernel shall:

….

Description **#7**

In Section 7.1.3, Table 7 the positions of the bytes in the EXCHANGE RELAY RESISTANCE DATA Response Message Data Field are incorrect.

Specification Change

Position	**Value**	**Length (in bytes)**	**Format**
Byte 1	'80'	1	b
Byte 2	'0A'	1	b
Byte ~~5 – 8~~ 3 - 6	*Device Relay Resistance Entropy*	4	b
Byte ~~9 – 10~~ 7 - 8	*Min Time For Processing Relay Resistance APDU*	2	b
Byte ~~11 – 12~~ 9 - 10	*Max Time For Processing Relay Resistance APDU*	2	b
Byte ~~13 – 14~~ 11 - 12	*Device Estimated Transmission Time For Relay Resistance R-APDU*	2	B

Description **#8**

The transaction type terminology in Section 17 and Section 4.1 (p 49) are not in line.

With the proposed change, it will be aligned with terminology used in the ECSG Volume.

Specification Change

In Section 4.1

~~Purchase~~Payment

Cash Advance

Cash Withdrawal

~~Cashback~~ Payment with Cashback

In Section 17

Transaction Type = '01' (Cash Withdrawal)

o or Transaction Type = '17' (~~Cash Disbursement~~ Cash Advance)

o or Transaction Type = '00' (Payment)

o or Transaction Type = '09' (Payment with Cashback)

Description **#9**

1. The terminology *"Contactless Transaction Limit without CDCVM"* and *"Contactless Transaction Limit with CDCVM"* may be misleading.

2. In addition in Section 9 (p. 29), the decision process on the Contactless Transaction Limit can be updated to be more readable.

Specification Change

1. Replace as shown below:

"Contactless Transaction Limit without CDCVM" change to *"Contactless Transaction Limit – CDCVM not Supported"*

"Contactless Transaction Limit with CDCVM" change to *"Contactless Transaction Limit – CDCVM Supported"*

2. Change

If **all** of the following are true:
• 'CDCVM is Supported' (byte 1, bit 2) in *Application Interchange Profile* has the value 1b
• **and** 'CDCVM is Supported' (bit 6) in *Kernel Configuration* has the value 1b
• **and** *Amount, Authorized > Contactless Transaction Limit with CDCVM*

Then the kernel shall:
• Return the Control to Entry Point with an Outcome "Select Next" as in Section 22.2.10

Else
• If the following is true:
○ *Amount, Authorized > Contactless Transaction Limit without CDCVM*

Then the kernel shall:
• Return the Control to Entry Point with an Outcome "Select Next" as in Section 22.2.10.

To

If **all** of the following are true:

- 'CDCVM is Supported' (byte 1, bit 2) in *Application Interchange Profile* has the value 1b
- **and** 'CDCVM is Supported' (bit 6) in *Kernel Configuration* has the value 1b

Then

- If the following is true:
  - *Amount, Authorized > Contactless Transaction Limit - CDCVM Supported*

  Then the kernel shall:
  - Return the Control to Entry Point with an Outcome “Select Next” as in Section 22.2.10

Else

- If the following is true:
  - *Amount, Authorized > Contactless Transaction Limit - CDCVM not Supported*

  Then the kernel shall:
  - Return the Control to Entry Point with an Outcome “Select Next” as in Section 22.2.10.

Description **#10**

The Section 9 on Initiate Application Processing describes modification and additions to [EMV Book 3] Section 10.1. Check are added (1) on presence of Amount, Authorized and Transaction Currency code and (2) Amount, Authorized exceeding the Contactless Transaction Limit. In other kernel implementations these checks are done at the moment of Read Application Data (corresponding to [EMV Book 3] Section 10.2). The text will be adapted to allow for performing these checks at a later moment.

Specification Change

At the end of Section 9, add

Note that even though these checks are mentioned in this Section, they may be performed later in the processing, until the moment of Read Application Data (see Section 11).