CPACE-DIC Specification Update

This specification Update applies to CPACE-DIC Specification Version 1.0 18.10.2017.

This bulletin is effective immediately

Description	**#1**

Requirement modification on MAC length support

A CPACE implementation that supports 'Other MAC lengths' implementer-option (IO6) shall support 4-byte and 8-byte MACs and may in addition support 5-byte to 7-byte MACs.

Specification Change (if any)

CPACE – Table 2 – IO6: Other MAC Lengths

Replace the description with:

'A CPACE implementation that supports this implementer-option shall support 4-byte and 8-byte MACs and may in addition support 5-byte to 7-byte MACs according to Section 19.3.7 of [CPA]'.

Table 4:

Replace description of Additional Function Other MAC Lengths, if implementer-option Other MAC Lengths is supported with:

'Issuer choice to use 4-byte and 8-byte MACs or 4-byte to 8-byte MACs'

Req C.124 Message Authentication (MACing)

Replace the second paragraph with:

'If the Other MAC Lengths implementer-option is supported the CPACE application shall support 4-byte and 8-byte MACs and may in addition support 5-byte to 7-byte MACs'.

Description	**#2**

Section 13.2.9.1 Reference error

Specification Change (if any)

In the first sentence, replace Req 15.87 with Req 17.87

Description	**#3**
Req C.132 Typo **Specification Change (if any)** In the first bullet replace P2 with P1	

Description	**#4**
Section 21.50 VLP Modification of Table 71 Profile Control x Coding As VLP may be supported the meaning of Byte 6 b4-b1 shall be changed **Specification Change (if any)** In Table 71, change the meaning of Byte 6 b4-b1 with the following: VLP Profile Control ID with the footnote: 'If VLP is not supported in the CPACE application, this field is set to 'F' to indicate it is not used.'	

Description	**#5**
Req C.49 & Req C.98 Clarification on the use on Environment in use Data Object Environment in use is dedicated to implementer option Internal Data Logging (IO5) and should not be used for other implementer option (e.g. Relay Resistance Protocol (IO8)) **Specification Change (if any)** In Req C.49 replace the second bullet with: or the interface currently used is not contactless (see Req C.7), In Req C.98 replace the seventh bullet with: and the interface currently used is contactless (see Req C.7),	

Description	**#6**
Table 56 Card Issuer Action Code modification bit 8, b7, b6 of Byte 5 are used for the management of Cyclic Accumulator **Specification Change (if any)** Replace the meaning of b8 of Byte 5 with Cyclic Accumulator 1 Limit Exceeded Replace the meaning of b7 of Byte 5 with Cyclic Accumulator 2 Limit Exceeded Replace the meaning of b6 of Byte 5 with Additional Cyclic Accumulator Limit Exceeded	

Description **#7**

Section 21.39 Clarification on the use of Authorization Response Code (ARC) and Issuer Authentication in ILDOL (Table 66)

In the seventh paragraph of Section 21.39; it is said 'if the tag of IATD or ARC is included in the ILDOL, the CPACE application shall fill the part of the list representing the respective data object with hexadeciman zeroes; it is true only during the first GEN AC command processing

Specification Change (if any)

Change the last sentence of the seventh paragraph with the following:

If the tag of IATD (91) or ARC (8A) is included in the ILDOL and if the information is not available, the CPACE application must fill the part of the list representing the respective data object with hexadecimal zeroes.

Description **#8**

Updating description of of Application Life Cycle Data as defined in Annex L of CPA

Specification Change (if any)

Add Application Life Cycle Data in the CPACE Data Dictionary as described in Annex L of CPA with the following changes:

Version Number

Replace the first paragraph of the description with:

Identifies the version of the CPACE implemented in the application: '11' = CPACE RSA-capable implementation

Card Approval ID

Replace the first paragraph of the description with:

Identifier assigned by the Certification Body before the application is submitted for Card Approval.

Description **#9**

Section 21.39 Length error on the data "Previous Transaction History" (Table 66)

Specification Change (if any)

In the table 66, Tag C7, replace the length 1 with 2.

Description	**#10**
Req C.42 GPO Command Data Length is a terminology used in CPA. In CPACE, this field is renamed GPO Input Data Length. **Specification Change (if any)** In the third bullet replace GPO Command Data Length with GPO Input Data Length	

Description	**#11**
Section 4.1 Clarification regarding integration of the Relay Resistance Protocol in the CPACE specification. **Specification Change (if any)** Change the fourth bullet to 'Section 4.5 describes the implementer-optional extension of [CPA] for the Relay Resistance Protocol.'	

Description	**#12**
Req C.34 Usage of the *DF Name* in an *AID-Interface Entry* is not in line with the definition in Section 20.17. **Specification Change (if any)** Change the second bullet after 'The AID-Interface File shall be evaluated as follows:' to *AID* is equal to *DF-Name* in the *AID-Interface Entry*	

Description	**#13**
Req C.57 An additional check of *Contactless READ RECORD Access* has to be performed. **Specification Change (if any)** After the check 'If *Contactless READ RECORD Access* is present, but does not have a length of 1 + 3*n bytes, where n >= 1, then the record shall not be read on the contactless interface.' add the following new check: 'If *Contactless READ RECORD Access* is present and has a correct length, but the first byte of *Contactless READ RECORD Access* has a value different from '00' and '01', then the record shall not be read on the contactless interface.'	

Description	**#14**
Req C.69 An additional check of *Contactless GET DATA Access* has to be performed. **Specification Change (if any)** After the check 'If *Contactless GET DATA Access* is present, but does not have a length of 1 + 2*n bytes, where n >= 1, then the data object shall not be read on the contactless interface.' add the following new check: 'If *Contactless GET DATA Access* is present and has a correct length, but the first byte of *Contactless GET DATA Access* has a value different from '00' and '01', then the record shall not be read on the contactless interface.'	

Description	**#15**
Section 21.23 The result of the processing of a CSU where b8-b7 in Byte 3 is set to ‘11’b is not specified **Specification Change (if any)** Add a note below first part of Table 57 to say that, if b8-b7 is set to ‘11’b, ACTIVATE shall be performed first (b7) and DEACTIVATE shall be performed secondly (b8)	