Draft Specification & Bulletin
Industry Feedback Form

Working Group: Contactless Kernel Task Force

Document:

EMV® Contactless Specifications for Payment Systems Book C-8
Kernel 8 Specification Version DRAFT1 February 2022

Company Name: Consolidated Comments and CKTF Feedback

Primary Contact
Name: EMVCo Contactless Kernel Task Force

Date: 3 May 2022

CKTF Consolidated Responses – C-8 Kernel Specification DRAFT1

						EMVCo Use Only	
Comment Source[1] **EA/Sub**	**Clause No./ Subclause No. / Annex**	**Paragraph/ Figure/ Table/ Note**	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Status** Accept, Reject, In progress, Acknowledge	**EMVCo observations** on each comment submitted
EA	3.9	Table 3.3	ge	Question: what is the background of the option to set/unset the Report local authentication failed in TVR. Would it make sense to clarify that in the document?		Accept	As this bit is set after the Generate AC command there may be an impact on the issuer host. With this configuration option it is possible to remove the impact. We will add a note below Table A.19 in Section A.1.73: 'Local authentication failed' bit in TVR is set after GENERATE AC command and may impact Application Cryptogram verification."
EA	4.3	Page 53	ed	I had to look up ASI in the glossary when it first appeared in the text in 4.3. Perhaps it can be introduced like…	…. or **an Algorithm Suite Indicator (ASI)** in a list of ASIs.	Accept	The change will be made.

1 **EA/Sub** = EMVCo Associate or Subscriber company (enter a 2-3 letter abbreviation for commenting)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.

CKTF Consolidated Responses – C-8 Kernel Specification DRAFT1

						EMVCo Use Only	
Comment Source[1] **EA/Sub**	**Clause No./ Subclause No. / Annex**	**Paragraph/ Figure/ Table/ Note**	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Status** Accept, Reject, In progress, Acknowledge	**EMVCo observations** on each comment submitted
EA	A.1.29	Page 244	ge	Would it make sense to explain the background of the difference between Card Qualifier version 1 vs. 2? I see the technical difference in processing the MAC, but it might help to explain it in human / business language.		Accept	We will add a note below Table A.7: The difference between VERSION 1 and VERSION 2 is the algorithm used for the IAD MAC generation. In VERSION 1 the IAD is excluded as input to the generation of the IAD MAC, whereas in VERSION 2 it is included to the generation of the IAD MAC.
EA	A.1.123	Table A.30	ed	Might it help to explain the meaning of the CVM bits with the additional text “supported” like in the example at the right. There is always quite a bit of confusion about the TRMD with customers encountering it for the first time.		Reject	The naming of the bits follows the same convention as other EMV data objects (e.g. Terminal Capabilities). Therefore, we will keep the current naming.
EA	3.1 and Annex C		te MAJOR	Will the support of some algorithms suite (Like the Curves P-521 and SM2-P256) be a configuration option ? If yes we suggest listed them in 3.1		Reject	P-521 and SM2-P256 are not configuration options. They are not supported by Process C in the current version of the specification.

1 **EA/Sub** = EMVCo Associate or Subscriber company (enter a 2-3 letter abbreviation for commenting)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.

CKTF Consolidated Responses – C-8 Kernel Specification DRAFT1

						EMVCo Use Only	
Comment Source[1] **EA/Sub**	**Clause No./ Subclause No. / Annex**	**Paragraph/ Figure/ Table/ Note**	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Status** Accept, Reject, In progress, Acknowledge	**EMVCo observations** on each comment submitted
EA	Sections 3.3 and 6.3.14 to 6.3.16	Processing between states 27 and 28	te	Splitting the Gen AC into 2 parts will create complexity in the implementation, testing and resolving field issues.	Follow a standard EMV process over the contactless interface so the card makes the final decision before it leaves the interface and you always see the 1st Gen results from the card which are final.	Reject	This is probably a misunderstanding as there is only one GENERATE AC command. The GENERATE AC command is not split into 2 parts. Kernel risk management processing is split in 2 parts: before and after GENERATE AC. Therefore, the Kernel performs a second Terminal Action Analysis after the GENERATE AC command to take into account the outcome of risk management processing performed during and after the GENERATE AC command.

1 **EA/Sub** = EMVCo Associate or Subscriber company (enter a 2-3 letter abbreviation for commenting)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.

CKTF Consolidated Responses – C-8 Kernel Specification DRAFT1

						EMVCo Use Only	
Comment Source[1] **EA/Sub**	**Clause No./ Subclause No. / Annex**	**Paragraph/ Figure/ Table/ Note**	**Type of com-ment**[2]	**Comment (justification for change)**	**Proposed change**	**Status** Accept, Reject, In progress, Acknowledge	**EMVCo observations** on each comment submitted
EA	4.1.3	Para 10	te	Length GetLength(T) Returns NULL if the TLV Database does not include a data object with tag T. NULL cannot be returned since it is not return type of the function.	In this condition the function should return Zero.	Reject	The function returns zero when the data object isEmpty. GetLength(T), when there is no data object in the TLV Database with tag T, should not return zero. We use NULL to signify there is no database entry, and zero to signify there is a database entry, but its length is zero. Note that this is a behavioral specification and does not follow strict source code-like syntax such as function prototypes or data type checking. The implementer may use any value that does not represent a valid length, like -1 for example.
EA	3.9	Table 3.3	ed	Certificates is miss spelled as cerificates	Fix the miss-spelling	Accept	The correction will be made.
EA	Annex E	Table E.1	ed	DS is missing in abbreviation table	Add DS in abbreviations table	Accept	The change will be made.

1 **EA/Sub** = EMVCo Associate or Subscriber company (enter a 2-3 letter abbreviation for commenting)
2 **Type of comment:** **ge** = general **te** = technical **ed** = editorial – For technical comments, please indicate whether your comment is a MAJOR or MINOR technical comment.