EMV® Specification Bulletin No. 281
First Edition, May 2023

EMV® CPS DGIs for AES Key Personalisation

Applicability

This Specification Bulletin applies to:

- *EMV Card Personalisation Specification (EMV CPS), v2.0, August 2021*

Related Documents

- *EMV Specification Bulletin No. 165 - AES in CPA, May 2015*

Effective Date

- *Immediate*

Description

This Specification Bulletin introduces in the EMV CPS new DGIs specifically for personalising AES based CAM/Issuer Auth Issuer Script UDKs and the Key Check Values for those AES keys. The DGIs introduced are aligned with the DGIs introduced for AES UDKs and AES Key Check Values in *EMV Specification Bulletin No. 165 – AES in CPA*. The Specification Bulletin also clarifies Requirement 14 in section 3.2 as regards the padding to be applied if the data grouping to be encrypted is one or more symmetric keys.

Specification Changes

In section 3.2 replace Requirement 14 with the following:

14 a) If the data grouping is to be encrypted and it contains data that is not a symmetric block cipher key or a PIN block, it must always be padded. Padding is accomplished by appending an '80', followed by 0-7/0-15 bytes of '00' depending on the block size of the cipher (DES/AES). The length of the data part of the data grouping must be a multiple of 8 bytes/16 bytes for DES/AES respectively.

b) If the data is one or more symmetric keys and a multiple of 16 bytes in length no padding is required. If AES is used and the data to be protected is a multiple of 8 bytes but not 16 bytes, then 8 bytes of random padding shall be appended to form a sequence of 16-byte blocks.

c) If the data is an 8-byte PIN block and the block cipher is DES, no padding is required. If AES is used, then an 8-byte PIN block is padded with 8 bytes of random data to form a 16-byte block. N.B. this is not to be confused with the RANDOM field mechanism for blinding low entropy data.

In Table A-1 in Annex A2, insert the rows listed below (additions are identified using red text):

Table A-1 Data Grouping Identifiers for Payment Applications

DGI	Data Content	Function	Encrypt	External Access
'8000'	Block cipher (DES/AES) keys – Table A-2	CAM* / Issuer Auth/ Issuer Script	Yes	None
'8002'	Block cipher (AES) keys – Table A-2a	CAM* / Issuer Auth/ Issuer Script	Yes	None
'9000'	Block cipher (DES/AES) Key Check Values – Table A-3		No	None
'9002'	Block cipher (AES) Key Check Values – Table A-3a		No	None

After Table A-2, add the following new table:

Table A-2a Data Content for DGI '8002'

Req.	Tag	Data Element	Length[12]	Encrypt
C	N/A	Unique Derivation Key (UDK) AES Key Message Authentication (MAC UDK) AES Key Data Encipherment (ENC UDK) AES Key	16, 24 or 32 16, 24 or 32 16, 24 or 32	K_{DEK} (SCP03)

Update Table A-3 as follows:

Table A-3 Data Content for DGI '9000'

Req.	Tag	Data Element	Length	Encrypt
O	N/A	Key Check Values for card keys UDK, MAC UDK and ENC UDK stored in DGI '8000'	3, 6 or 9	N/A

[12] It should be noted that CPA requires the personalisation of all 3 keys, other applications may require alternative mechanisms to determine how many keys are personalised so that the encryption padding can be removed appropriately.

After Table A-3, add the following new table:

Table A-3a Data Content for DGI '9002'

Req.	Tag	Data Element	Length	Encrypt
O	N/A	Key Check Values for card keys UDK, MAC UDK and ENC UDK stored in DGI '8002'	3, 6 or 9	N/A

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