Draft Specification Bulletin No. 165
First Edition May 2015

AES in CPA

This specification update introduces the Advanced Encryption Standard (AES) into CPA.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Common Payment Application Specifications*

Related Documents

- None

Description

This Specification Bulletin introduces an option to support the Advanced Encryption Standard (AES) in CPA.

In particular it introduces support for the AES option defined for CCD in EMV Books 2 and 3 and identified by Cryptogram Version '6'. In addition, it introduces the use of AES for the encryption of the offline counters when Cryptogram Version '6' is used.

Implementations of CPA that support only Cryptogram Version '5' (Triple DES) remain allowed. Implementations of CPA that support only Cryptogram Version '6' (AES) are allowed. Implementations of CPA that support both Cryptogram Version '5' (Triple DES) and '6' (AES) are allowed.

Note that the Cryptogram Version is identified in the Profile CCI (Common Core Identifier) which will be either 'A5' indicating Triple DES or 'A6' indicating AES; this data is contained in the Issuer Application Data provided in the response to the GENERATE AC command.

Background

CPA is an EMV card specification published in 2005 that complies with the EMV Common Core Definitions (CCD) published in 2004 and that initially supported only Triple DES for securing communications between card and issuer.

In 2010 Specification Update No. 74 provided the specification for the optional use of the AES block cipher algorithm in EMV for securing communications between issuers and their IC cards. This option was not introduced on account of any security concerns with the current symmetric cryptography but rather was introduced for those issuers wishing to migrate to the new AES standard.

In 2011 Specification Bulletin 91 added an option to CCD for the use of AES as the algorithm for online cryptography. SB91 noted that until then only Triple DES had been supported for CCD applications and that AES support was being defined only so that issuers who wished to implement AES to satisfy local requirements could do so in a consistent manner.

Although CCD now supports block ciphers Triple DES and AES, CPA supported only Triple DES. This specification update introduces AES into CPA.

Note that although this is a security maintenance activity for the CPA specifications it is not because EMV has security concerns with Triple DES, but rather to ensure that CPA can use the AES block cipher. Use of AES will be optional; CPA issuers may continue to use Triple DES.

In section 1.3 Contents

Make the following change to the section describing Section 20, Security and Key Management:

Section 20, Security and Key Management – Provides requirements related to security and key management for a CPA implementation that are in addition to the specifications for CCD-compliant applications, as specified in EMV ~~4.1~~4.3.

In section 2.1 EMV Documents

Make the following changes to the EMV books titles:

EMV Book 1 *EMV Integrated Circuit Card Specifications for Payment Systems*, version ~~4.1~~4.3, Book 1, Application Independent ICC to Terminal Interface Requirements, ~~May 2004~~November 2011.

EMV Book 2 *EMV Integrated Circuit Card Specifications for Payment Systems*, version ~~4.1~~4.3, Book 2, Security and Key Management, ~~May 2004~~November 2011.

EMV Book 3 *EMV Integrated Circuit Card Specifications for Payment Systems*, version ~~4.1~~4.3, Book 3, Application Specification, ~~May 2004~~November 2011.

EMV Book 4 *EMV Integrated Circuit Card Specifications for Payment Systems*, version ~~4.1~~4.3, Book 4, Cardholder, Attendant, and Acquirer Interface Requirements, ~~May 2004~~November 2011.

EMV CPS *EMV Card Personalization Specification*, version ~~1.0~~ 1.1, ~~June 2003~~ July 2007.

In section 3 Definitions

Add the following:

Advanced Encryption Standard (AES) 16-byte block cipher standardized in ISO/IEC 18033-3.

AES key A 128, 192 or 256-bit secret parameter of the Advanced Encryption Standard.

In section 4.1 Abbreviations

Add the following:

AES Advanced Encryption Standard

In section 5.1 Implementer-Options
Add the following options to Table 5-1:

Implementer-option	Description
Cryptogram Version '5' -only	A card that supports this implementer-option only supports the DES block cipher as the symmetric algorithm used to compute MACs or encrypt/decrypt data.
Cryptogram Version '6' -only	A card that supports this implementer-option only supports the AES block cipher as the symmetric algorithm used to compute MACs or encrypt/decrypt data.
Cryptogram Version '5' and '6'	A card that supports this implementer-option supports both the DES and AES block ciphers as the symmetric algorithms used to compute MACs or encrypt/decrypt data, with which version to be used by the application indicated in the Profile CCI in the Issuer Options Profile Control x used for the transaction. Note that support for different cryptographic algorithms in different profiles is out of scope.

In section 5.1 Implementer-Options

Add the following below Table 5-1:

Req 5.4 (AES key lengths):
If the Cryptogram Version '6'–only or the Cryptogram Version '5' and '6' implementer-option is supported, then the application shall support AES key lengths of 128, 192 and 256 bits for the Master Key for AC, the Master Key for SMC and the Master Key for SMI. The length of the AES key used is determined at personalisation when the AES key is personalised.

It is not required that the application support different key lengths for the Master Key for AC, the Master Key for SMC and the Master Key for SMI (i.e. it is required that the three of them can have a common key length of 128, 192 or 256. Support of mixed key lengths is out of scope).

In section 5.4.1 Card Functional Requirements

Make the following change:

First Card Action Analysis	*Mandatory*
▪ *Online/offline decision*	*Mandatory*
▪ *Card Risk Management*	*Mandatory*
▪ *Application Cryptogram*	*Mandatory, algorithm specified by CCD for Cryptogram Version '5' or '6'*~~*, algorithm specified by CCD for Cryptogram Version '5'*~~
▪ *Transaction Logging*	*Mandatory*

In section 14.5.2 Request Cryptogram Processing

Replace the first sentence as follows:

In the Request Cryptogram Processing step of Terminal Action Analysis, the terminal formats the first GENERATE APPLICATION CRYPTOGRAM (GENERATE AC) command and issues it to the card requesting generation of an Application Cryptogram.

In section 15.5.8.1 Build Issuer Application Data

Replace Req 15.80 as follows:

Req 15.80 (Build Issuer Application Data for Token Authentication profile):
If the Profile ID has the value '7E' (Token Authentication Profile – see Annex H10.2), then the application shall build the Issuer Application Data (IAD) to be sent in the response, coded as specified in the CCD Part of EMV Book 3, Annex C.7, for a CCD-compliant application with a Format Code of 'A' ~~with Cryptogram Version of '5'~~; with the profile specific requirements shown in Table 15-9.

IAD Byte	Description	Value
1	*Length*	*'0F'*
2	*CCI*	*set to the value of the Profile CCI in the Issuer Options Profile Control for the transaction ('A5' or 'A6' ~~for CCD-compliant profiles~~)*
3	*DKI*	*set to the value of the Profile DKI in the Issuer Options Profile Control for the transaction (issuer-discretionary)*
4-8	*CVR*	*set to zero except for the following bits used to indicate the results of offline PIN verification:* *· 'Offline PIN Verification Performed'* *· 'Offline PIN Verification Performed and PIN Not Successfully Verified'*
9-16	*Counters*	*zero*
17	*Length*	*'0F'*
18	*Profile ID*	*'7E'*
19-32	*issuer-discretionary*	*zero*

Table 15-9: Issuer Application Data for Profile '7E' *(Authentication Token)*

In section 15.5.8.1 Build Issuer Application Data

Replace CCI value of Table 15-10 as follows:

IAD Byte	Description	Value
2	*CCI*	*set to the value of the Profile CCI in the Issuer Options Profile Control for the transaction ('A5' or 'A6' ~~for CCD-compliant profiles~~)*

In section 15.5.8.2 Generate Application Cryptogram

Change the second paragraph as follows:

Data requirements, key requirements, and the algorithms used in the cryptogram generation process are as detailed in Table CCD-3 and section 8 of the CCD part of *EMV Book 2*, for a CCD-compliant application with Cryptogram Version of '5' (which uses Triple DES) or '6' (which uses AES).

If the Cryptogram Version '5' –only implementer-option is supported:

> *the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*

If the Cryptogram Version '6' –only implementer-option is supported:

> *the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*

  the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'
- *if the application uses AES as cryptographic algorithm:*

  the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'

In section 17.5.3.1 Issuer Authentication Data Received

Replace the text for step 2 as follows:

Using the CSU recovered in step 1 and the ARQC sent in the first GENERATE AC response, generate an ARPC as specified in *EMV Book 2* for a Common Core Definitions application with the Cryptogram Version '5' (which uses Triple DES) or '6' (which uses AES).

If the Cryptogram Version '5' –only implementer-option is supported:

> *the ARPC generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*

If the Cryptogram Version '6' –only implementer-option is supported:

> *the ARPC generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*
  > *the ARPC generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*
- *if the application uses AES as cryptographic algorithm:*
  > *the ARPC generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

In section 17.5.3.1.3 CSU Processing

Change the first sentence as follows:

After successful Issuer Authentication, the card has verified that the CSU received in Issuer Authentication Data is valid. The CSU for the Common Payment Application shall be coded as specified in the Common Core Definitions part of *EMV Book 3*, for a Cryptogram Version of '5' or '6'.

In section 17.5.8.1 Build Issuer Application Data

Replace CCI value of Table 17-13 as follows:

IAD Byte	Description	Value
2	*CCI*	*set to the value of the Profile CCI in the Issuer Options Profile Control for the transaction ('A5' or 'A6' ~~for CCD-compliant profiles~~)*

In section 17.5.8.2 Generate Application Cryptogram

Change the second paragraph as follows:

Data requirements, key requirements, and the algorithms used in the cryptogram generation process are as detailed in Table CCD-3 and section 8 of the CCD part of *EMV Book 2*, for a CCD-compliant application with Cryptogram Version of '5' (which uses Triple DES) or '6' (which uses AES).

If the Cryptogram Version '5' –only implementer-option is supported:
the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'

If the Cryptogram Version '6' –only implementer-option is supported:
the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*
  the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '5'
- *if the application uses AES as cryptographic algorithm:*
  the cryptogram generation process is as detailed for a CCD-compliant application with Cryptogram Version of '6'

In section 18. 1 Purpose

Add the following paragraph after the second paragraph:

If the Cryptogram Version '5' –only implementer-option is supported:
the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '5'

If the Cryptogram Version '6' –only implementer-option is supported:
the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '6'

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*
  the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '5'
- *if the application uses AES as cryptographic algorithm:*
  the secure messaging is as detailed for a CCD-compliant application with Cryptogram Version of '6'

In section 18.5.3 Card Secure Messaging

Add the following paragraph before section 18.5.3.1:

If the Cryptogram Version '5' –only implementer-option is supported:

> *the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*

If the Cryptogram Version '6' –only implementer-option is supported:

> *the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*

  > *the secure messaging process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*
- *if the application uses AES as cryptographic algorithm:*

  > *the secure messaging is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

In section 18.7.2.2 Change PIN

Replace the second paragraph with the following:

The plaintext PIN Block before encipherment for confidentiality is coded as shown in *EMV Book 3*, Table 24. It is padded with '80 00 00 00 00 00 00 00' and then enciphered as specified for a CCD-compliant application in *EMV Book 2*, section 9.3 to form a 16-byte enciphered PIN block.

If the Cryptogram Version '5' –only implementer-option is supported:

> *the encipherment process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*

If the Cryptogram Version '6' –only implementer-option is supported:

> *the encipherment process is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

If the Cryptogram Version '5' and '6' implementer-option is supported:

- *if the application uses Triple DES as cryptographic algorithm:*

  > *the encipherment process is as detailed for a CCD-compliant application with Cryptogram Version of '5'*
- *if the application uses AES as cryptographic algorithm:*

  > *the encipherment is as detailed for a CCD-compliant application with Cryptogram Version of '6'*

For an illustration of the process for recovering the New PIN Block, see Figure 18-3.

In section 18.8.1 PUT DATA Command Coding

Add the following to the note below Req 18.32:

For the 3 implementation options (Cryptogram Version '5' –only implementer-option, Cryptogram Version '6' –only or Cryptogram Version '5' and '6' implementer-option), support for updating the CCI with a PUT DATA is out of scope.

In section 20.5 Other Data Requirements

Replace Req 20.14 as follows:

Req 20.14 (Enciphering counters in Issuer Application Data):

*If the (8-byte) Counters portion of the Issuer Application Data is to be enciphered **and Triple DES is used**,*
then the Counters portion of the Issuer Application Data shall be enciphered as follows:

- *The eight-byte Counters block shall be enciphered using Triple DES in ECB Mode as defined in Appendix A1.1 of EMV Book 2, with no additional padding applied (thus the ciphertext is eight bytes long).*
- *The encipherment key (ECK) used shall be a variant of the AC session key (SK_{AC}) computed as follows:*
  - SK_L *= the left-most bytes of* SK_{AC}
  - SK_R *= the right-most bytes of* SK_{AC}
  - $ECK_L := SK_L \oplus (\text{'59'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'})$
  - $ECK_R := SK_R \oplus (\text{'95'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'})$
  - $ECK = ECK_L \,||\, ECK_R$

*If the (8-byte) Counters portion of the Issuer Application Data is to be enciphered **and AES is used**,*
then the Counters portion of the Issuer Application Data shall be enciphered as follows:

- *The eight-byte Counters block shall be XORed with the leftmost 8 bytes of a 16-byte mask R.*
- *The mask R is a ciphertext computed as the encipherment of a 16-byte value '00..0X' (15 bytes '00' followed by one byte '0X' with 'X' = '1' for IAD returned by the first GENERATE AC command and 'X' = '2' for IAD returned by the second GENERATE AC command) using AES in ECB Mode as defined in Appendix A1.1 of EMV Book 2, with no additional padding applied (thus the ciphertext R is 16 bytes long).*
- *The k-bit encipherment key (ECK) used shall be a variant of the k-bit AC session key (SK_{AC}) computed as follows:*
  - $ECK := SK_{AC} \oplus (\text{'59'}||\text{'00'}||\text{'00'}|| \ldots ||\text{'00'}||\text{'00'}||\text{'00'})$

  with (k-8)/8 bytes of '00'.

In section 21.1.2 CPA Data Elements Requiring Personalisation

Make the following changes to Table 21-2:

Tag	Data Element Name	Size (bytes)	Format
'C1'	*Application Control*	4	*binary*
'C8'	*Application Issuer Life Cycle Data*	20	*binary*
'9F10'	*Issuer Application Data*[6]	32	*binary*
'5F28'	*Issuer Country Code*	2	*n3*
-	*Master Key for SMC (Triple DES)*	16	*binary*
-	*Master Key for SMI (Triple DES)*	16	*binary*
-	*Master Key for AC (Triple DES)*	16	*binary*
-	*Master Key for SMC (AES)*	16, 24, 32	*binary*
-	*Master Key for SMI (AES)*	16, 24, 32	*binary*
-	*Master Key for AC (AES)*	16, 24, 32	*binary*

Add the following below the table:

If the Cryptogram Version '5' -only implementer-option is supported, only the Triple DES versions of the master keys are personalised.
If the Cryptogram Version '6' -only implementer-option is supported, only the AES versions of the master keys are personalised.
If the Cryptogram Version '5' or '6' implementer-option is supported, either the Triple DES or the AES versions of the master keys are personalised as stated in **Req 21.74 (CV in Profile CCI of Issuer Options Profile Control x)**.

In section 21.1.2 CPA Data Elements Requiring Personalisation

Add the following note below Table 21-2

NOTE: If the Cryptogram Version '6' -only or the Cryptogram Version '5' or '6' implementer-option is supported, then the length of the AES key is determined at personalisation, as stated in **Req 5.4 (AES key lengths).**

In section 21.2.11 DGIs for PIN and Key Related Data

Add the following after Table 21-29:

If the Cryptogram Version '5' -only implementer-option is supported, DGIs '8000' and '9000' as defined in EMV CPS are used to personalise the Triple DES master keys.

If the Cryptogram Version '6' -only implementer-option is supported, DGIs '8000' and '9000' are not used. Instead, DGIs '8002' (AES keys) and '9002' (AES Key Check Values) are used to personalise the AES master keys.

If the Cryptogram Version '5' or '6' implementer-option is supported and if the application uses Triple DES as cryptographic algorithm, DGIs '8000' and '9000' as defined in EMV CPS are used to personalise the Triple DES master keys.

If the Cryptogram Version '5' or '6' implementer-option is supported and if the application uses AES as cryptographic algorithm, DGIs '8002' (AES keys) and '9002' (AES Key Check Values) are used to personalise the AES master keys.

DGIs 8002 and 9002 are defined as follows:

DGI '8002'

Tag	Data Element	Length	Encrypt
N/A	*Master Key for AC (AES)* *Master Key for SMI (AES)* *Master Key for SMC (AES)*	16, 24, 32 16, 24, 32 16, 24, 32	SKU_{DEK}

All keys are of the same length.

DGI '9002'

Tag	Data Element	Length	Encrypt
N/A	Key Check Values for the card keys *Master Key for AC (AES), Master Key for SMI (AES), Master Key for SMC (AES)*	9	N/A

The Key Check Value for any AES key is computed by encrypting 16 bytes of '01' using ECB AES with the key concerned. The Key Check Value is the three leftmost bytes of the result.

Add the following new section 21.3.14:

21.3.14 Profile CCI in Issuer Options Profile Control x

Req 21.74 (CV in Profile CCI of Issuer Options Profile Control x):
The Profile CCI of every Issuer Options Profile Control x personalized in the application should be personalised to the same value[11]*:*

- *If the Cryptogram Version '5' –only implementer-option is supported, then the Profile CCI of every Issuer Options Profile Control x personalized in the application shall be personalised to the value 'A5'.*
- *If the Cryptogram Version '6' –only implementer-option is supported, then the Profile CCI of every Issuer Options Profile Control x personalized in the application shall be personalised to the value 'A6'.*
- *If the Cryptogram Version '5' and '6' implementer-option is supported, then the Profile CCI of every Issuer Options Profile Control x personalized in the application shall be personalised to either 'A5' or 'A6'.*

Footnote 11:

Support for different cryptographic algorithms in different profiles is out of scope.

In Annex L Data Dictionary

Make the following change to the last sentence in the description of the Common Core Identifier:

Set to the value 'A5' or 'A6' for CCD-compliant profiles.

In Annex L Data Dictionary

Make the following change Table L-51: Issuer Application Data:

2	CCI	'A5' or 'A6' for CCD-compliant profiles

In Annex L Data Dictionary

Make the following change to:

- *Master Key for AC*
- *Master Key for SMC*
- *Master Key for SMI*
- *Session Key for AC*
- *Session Key for SMC*
- *Session Key for SMI*

Master Key for AC

Tag: -	Master Key used for Application Cryptogram Generation. If the Cryptogram Version '5' -only implementer-option is supported, the Master Key for AC is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Master Key for AC is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Master Key for AC is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

Master Key for SMC

Tag: -	Master Key used for Secure Messaging for Confidentiality. If the Cryptogram Version '5' -only implementer-option is supported, the Master Key for SMC is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Master Key for SMC is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Master Key for SMC is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

Master Key for SMI

Tag: -	Master Key used for Secure Messaging for Integrity. If the Cryptogram Version '5' -only implementer-option is supported, the Master Key for SMI is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Master Key for SMI is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Master Key for SMI is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

Session Key for AC

Tag: -	Session Key used for Application Cryptogram Generation. If the Cryptogram Version '5' -only implementer-option is supported, the Session Key for AC is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Session Key for AC is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Session Key for AC is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

Session Key for SMC

Tag: -	Session Key used for Secure Messaging for Confidentiality. If the Cryptogram Version '5' -only implementer-option is supported, the Session Key for SMC is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Session Key for SMC is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Session Key for SMC is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

Session Key for SMI

Tag: -	Session Key used for Secure Messaging for Integrity. If the Cryptogram Version '5' -only implementer-option is supported, the Session Key for SMI is a Triple DES key (length 16). If the Cryptogram Version '6' –only is supported, the Session Key for SMI is an AES key (length 16, 24 or 32). If the Cryptogram Version '5' or '6' implementer-option is supported, the Session Key for SMI is either a Triple DES key (length 16) or an AES key (length 16, 24 or 32).
Length: 16, 24 or 32	
Format: b	

In H11.1 Coding of Profile-Related Data Elements

Make the following change in the 8th bullet describing the content of the Issuer Options Profile Control:

- the Common Core Identifier is 'A5' (that is, Profile '01' is CCD-compliant and the symmetric crytographic algorithms is Triple DES)