Specification Bulletin No. 162
First Edition April 2015

AES Key Derivation Erratum

This Specification Bulletin corrects an error in the specification of AES key derivation described in Annex A1.4 of EMV Book 2.

Effective Date

Changes specified in this bulletin are effective immediately.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 2 Security and Key Management*

Related Documents

- *None*

Description

The current specification for AES key derivation in Annex A1.4 states that a 24-byte AES key is derived as the leftmost 24-bytes of AES(IMK)[Y] || AES(IMK)[Y*] and that a 32-byte AES key is derived as AES(IMK)[Y] || AES(IMK)[Y*], where Y is a 16-byte string (based on the PAN and PAN Sequence Number) and where

$$Y^* = Y \oplus (\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}).$$

However the construction of Y* is poorly formulated because Y is 16-bytes and the string ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF') is only 8-bytes. Thus although the intention had been that Y* would be formed by flipping all the bits of Y, the strict interpretation of the stated construction, according to the definition of ⊕ in section 4.2 of Book 2, is that

$$Y^* = Y \oplus (\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'00'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}).$$

As this was not the intention, this bulletin corrects the construction of Y* as

$$Y^* = Y \oplus (\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}||\text{'FF'}).$$

Specification Change Notice

Please correct the specification in Annex A1.4 of *EMV Book 2 Security and Key Management as follows:*

A4.1.1 Option C

Option C is only applicable when the n-byte block cipher is AES.

Concatenate from left to right the decimal digits of the Application PAN with the PAN Sequence Number (if the PAN Sequence Number is not present, then it is replaced by a '00' byte). Pad it to the left with hexadecimal zeros in order to obtain a 16-byte number Y in numeric format.

The k-bit ICC Master Key MK is then equal to

- In the case $k = 8n$:

  MK := AES(IMK)[Y]

- In the case $16n \geq k > 8n$:

  MK := Leftmost k bits of {AES(IMK)[Y] || AES(IMK)[Y*]}

, where ~~Y*= Y ⊕ ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF')~~

Y* = Y ⊕ ('FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF'||'FF')

In other words Y* is a bit-wise inversion of Y.

.