Specification Bulletin No. 147
First Edition September 2014

Clarification on the Format of Exponent Data Elements

This Specification Bulletin clarifies the format, specifically the length, of the public key exponent data elements.

Applicability

This Specification Bulletin applies to:

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 3*

Related Documents

- *EMV Integrated Circuit Card Specifications for Payment Systems Version 4.3 Book 2*

Description

It has been noted that there is an inconsistency between EMV Book 2 and Book 3 in the description of the length of the public key exponents, i.e. the Issuer Public Key Exponent (tag '9F32') and the ICC Public Key Exponent (tag '9F47'). This bulletin removes the inconsistency between Book 2 and Book 3 by updating the data element descriptions in Book 3.

Note: The updated description of the public key exponent length, "1 or 3", technically allows for e=3 to be coded on 3 bytes. However, it is recommended that issuers code e=3 on 1 byte (and e=2^{16}+1 on 3 bytes).

© 1994-2014 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of the EMV Specifications ("Materials") shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at http://www.emvco.com/specifications.cfm.

Specification Change

In EMV Book 3, Annex A, Table 33, update the following data element entries as shown:

Name	Description	Source	Format	Template	Tag	Length
Integrated Circuit Card (ICC) Public Key Exponent	ICC Public Key Exponent used for the verification of the Signed Dynamic Application Data	ICC	b	'70' or '77'	'9F47'	1 ~~to~~ or 3
Issuer Public Key Exponent	Issuer public key exponent used for the verification of the Signed Static Application Data and the ICC Public Key Certificate	ICC	b	'70' or '77'	'9F32'	1 ~~to~~ or 3

© 1994-2014 EMVCo, LLC ("EMVCo"). All rights reserved. Any and all uses of the EMV Specifications ("Materials") shall be permitted only pursuant to the terms and conditions of the license agreement between the user and EMVCo found at http://www.emvco.com/specifications.cfm.