EMV® Specification Bulletin No. 304
First Edition May 2024

EMV® Secure Messaging PIN Change with AES

Applicability

This Specification Bulletin applies to:

- *EMV® Integrated Circuit Card Specifications for Payment Systems, Book 3 – Application Specification, Version 4.4, October 2022.*

Related Documents

- *EMV Integrated Circuit Card Specifications for Payment Systems, Book 2 – Security and Key Management, Version 4.4, October 2022.*

Effective Date

- *Immediate*

Description

This Specification Bulletin introduces wording into the EMV Specifications to allow for the use of ISO 9564-1 Format 4 PIN Blocks during PIN Change. ISO Format 4 PIN blocks have a structure whereby the PIN is encrypted using a 16-byte block cipher such as AES into an integral 16-byte PIN block and therefore such PIN blocks do not need the encryption component of EMV secure messaging.

The proposed changes to the EMV specifications for the PIN CHANGE command support encrypted PIN blocks such as ISO Format 4 PIN blocks. Key derivation is addressed by section 9.4 of Book 2.

Specification Changes

In section 6.5.10 of Book 3, replace the third paragraph of section 6.5.10.1 with:

If PIN data is transmitted in the command, it shall be enciphered for confidentiality, unless in a format that is already enciphered (e.g. an ISO 9564-1 Format 4 PIN Block).

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