



delivering comprehensive
payment security experience

End-to-End Encryption Security Requirements

Executive Summary

The SPVA defines end-to-end encryption as follows, “The transmission of cardholder data in an encrypted form, from its point of presentment, such that it prevents this data from being known in plaintext until the point of decryption.” In other words, end-to-end encryption refers to a system in which sensitive cardholder data is encrypted upon entry into the POS device and transmitted encrypted to the payment processor.

The *End-to-End Encryption Security Requirements* is a set of industry guidelines for implementing end-to-end encryption in payment devices. The requirements defined in this document are based on existing standards, such as those in use for debit card transactions. Using existing standards provides two significant benefits: first, the requirements are based on tried-and-true best practices that have been tested in production environments; second, the time and cost required to implement these requirements are minimized as stakeholders are already familiar with the standards.

The *End-to-End Encryption Security Requirements* are auditable, so that the proper implementation of end-to-end encryption can be consistently verified from implementation to implementation.

The document defines the following requirements:

- Data required to be encrypted – Defines the sensitive cardholder data that must be encrypted, including card numbers, track data, and security codes taking into consideration all forms of card holder data including Magnetic stripe, Smartcard, Contactless and manual entry.
- Key management requirements – Provides general key management guidelines and refers to existing standards upon which the requirements are based.
- Encryption requirements – Defines the permitted cryptographic algorithms.
- Physical security requirements – Defines the requirements for the physical security of the cryptographic keys and cryptographic devices.
- Logical security requirements – Defines the logical security requirements regarding operators in the key management process and applications accessing sensitive data on secured devices.
- Encryption monitoring and management system requirements – Defines the logging requirements for the terminating systems in an end-to-end encryption environment. This provides for the detection mechanisms and auditing information which improves the overall security and compliance of the solution.

End-to-end encryption systems will improve security for all stakeholders in the realm of electronic payments. By introducing the *End-to-End Encryption Security Requirements*, the SPVA expects to facilitate the implementation of these highly secure systems throughout the industry.

STATEMENT CONCERNING
END-TO-END ENCRYPTION SECURITY REQUIREMENTS

The End-to-End Encryption Security Requirements (“E³ Requirements”) are a work product developed by the Secure POS Vendor Alliance (“SPVA”) through the collaborative efforts of its members, and does not represent the work product or position of any individual member or group of members of SPVA. While every effort has been made to ensure that the E³ Requirements reflect “best practices” as determined by SPVA, no guarantee can be made by SPVA or its members in any manner with respect to the E³ Requirements; accordingly, use of, reference to and/or reliance upon the E³ Requirements by third parties is without warranty from or recourse against SPVA or its members.