



Best Practices for Data Field Encryption to Protect Cardholder Information in Transit and Storage

Cardholder data security continues to be an important issue for all stakeholders in the payment system. While payment system participant compliance with the Payment Card Industry Data Security Standard (PCI DSS) has undoubtedly prevented many breaches of cardholder information, some entities' lack of ongoing compliance has resulted in compromises, particularly of cardholder data in transit. As a result, many merchants and service providers have recently expressed interest in pursuing data field encryption (also known as "end-to-end encryption" or "line encryption") to address PCI DSS requirements and protect cardholder information in the event of a compromise. Visa supports data field encryption as an additional tool to protect cardholder information in merchant and other stakeholder environments.

"Data field encryption" is defined as encrypting cardholder information for transmission, processing, and storage to limit the cleartext availability of cardholder data and sensitive authentication data. Typically, data field encryption solutions focus on protecting cardholder data and sensitive authentication data by encrypting it at the merchant acceptance device and decrypting it in the acquirer-processor system. While vendors may market data field encryption solutions as "end-to-end encryption" or a "silver bullet" for PCI DSS and data compromises, the challenges of data field encryption must not be underestimated.

Data field encryption will require significant investment, the execution of proper key management, and reengineering of processes and systems with varied deployment scenarios to support the diversity of merchant environments. In an effort to enhance overall data security in the payment industry and to further the development of data field encryption, Visa has developed best practices to help merchants evaluate the new encryption solutions emerging in the marketplace.

Payment industry participants are encouraged to provide Visa with feedback on these best practices by writing to ais@visa.com.

Visa Best Practices for Data Field Encryption

To help vendors and early adopters determine what criteria must be met to properly secure cardholder data and sensitive authentication data, Visa has developed best practices based on the following five security goals:

1. Limit cleartext availability of cardholder data and sensitive authentication data to the point of encryption and the point of decryption.
2. Use robust key management solutions consistent with international and/or regional standards.
3. Use key-lengths and cryptographic algorithms consistent with international and/or regional standards.
4. Protect devices used to perform cryptographic operations against physical/logical compromises.
5. For business processes, use an alternate account or transaction identifier that requires the primary account number to be utilized after authorization, such as processing of recurring payments, customer loyalty programs or fraud management.

Please refer to the *Visa Best Practices for Data Field Encryption* for a detailed set of practices.

NOTE: Per PCI DSS, sensitive authentication data must not be stored after authorization (even if encrypted). The implementation of data field encryption solutions for the protection of card data **will not** supersede or replace any Visa-established global Triple Data Encryption Standard (TDES) mandates.

PCI DSS Impact

Data field encryption, when implemented in accordance with these best practices, may simplify PCI DSS compliance. Merchants should work with a qualified security assessor or internal subject matter expert to determine the impact of a data field encryption solution.

These best practices represent the first step in an ongoing communication from Visa, which will include a more detailed set of requirements for the validation of the secure implementation of data field encryption solutions.

Industry Efforts

The PCI Security Standards Council is currently completing a review of data security solutions, including data field encryption. *Visa Best Practices for Data Field Encryption* are designed to further the industry's efforts in developing a common standard that is open and interoperable, while also providing guidance to encryption vendors and organizations currently contemplating data field encryption solutions.

Visa is also working with industry stakeholders to explore options for data field encryption through the ANSI X9F6 Standards Working Group. As chair of this group, Visa is leading efforts to develop industry-wide standards to help ensure that solutions are open, consistent and enable choice.

Related Documents

[Visa Best Practices for Data Field Encryption](#)
