Data Field Encryption Version 1.0

Introduction

The marketplace has expressed a growing interest in pursuing data field encryption (also known as end-to-end encryption) of card data. Data field encryption protects card information from the swipe to the acquirer processor with no need for the merchant to process or transmit card data in the "clear." Importantly, data field encryption renders cardholder data useless to criminals in the event of a merchant data breach.

The implementation of any data field encryption solution must be done in a strong and secure way to prevent the compromise of card data. With industry standards still in the development phase, that goal can be particularly challenging. 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 assist merchants in evaluating the new encryption solutions emerging in the marketplace.

However, no single technology can completely solve for fraud. Accordingly, Visa views data field encryption as a complement to, rather than a substitute for PCI DSS compliance requirements.

The best practices are designed to achieve five implementation objectives:

- Limit cleartext availability of cardholder data and sensitive authentication data to the point of encryption and the point of decryption.

- Use robust key management solutions consistent with international and/or regional standards.

- Use key-lengths and cryptographic algorithms consistent with international and/or regional standards.

- Protect devices used to perform cryptographic operations against physical/logical compromises.

- Use an alternate account or transaction identifier for business processes that requires the primary account number to be utilized after authorization, such as processing of recurring payments, customer loyalty programs or fraud management.

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. Use an alternate account or transaction identifier for business processes that requires the primary account number to be utilized after authorization, such as processing of recurring payments, customer loyalty programs or fraud management.

Environment

- Visa Best Practices for Data Field Encryption pertain to systems used to acquire payment transactions in physical locations such as:
    - Payment terminals
    - Merchant point-of-sale systems
    - In-store controllers
    - Corporate transaction aggregation systems
    - Payment gateways
    - Core processing systems
    - Acquirers or Acquirer-processors
- Cardholder data includes Primary Account Number (PAN), cardholder name and expiration date.
- Sensitive authentication data includes but is not limited to full contents of the magnetic-stripe data, track 1, track 2, Card Verification Value (CVV), CVV2, PIN Verification Value (PVV), and PIN/PIN block. Additionally, sensitive authentication data shall not be used for any purpose other than payment authorization.

Best Practices

The following are best practices for data field encryption to protect cardholder data and sensitive authentication data:

Security Goal	Best Practice
Limit cleartext availability of cardholder data and sensitive authentication data to the point of encryption and the point of decryption.	1. Cleartext cardholder data and sensitive authentication data shall only be available at the point of encryption and at the point of decryption. 2. All cardholder data and sensitive authentication data shall be encrypted using only ANSI X9 or ISO approved encryption algorithms (e.g. AES, TDES). 3. All cardholder data and sensitive authentication data shall be encrypted with the following exceptions: • The first six digits of the PAN, may be left in the clear for routing purposes in authorization processing. • The first six and last four digits of the PAN may be displayed by the payment terminal and/or printed on the transaction receipt, in settlement reports, used for selection of account on file, etc. (This does not supersede stricter laws or regulations in place for displays of cardholder data.). 4. Sensitive authentication data must not be stored after authorization even if encrypted (per PCI DSS).
Use robust key management solutions consistent with international and/or regional standards.	5. Keys shall be managed per ANS X9.24 (all parts) /ISO 11568 (all parts) or its equivalent within Secure Cryptographic Devices (SCD) such as a PED, HSM, etc., as defined in ANS X9.97 (all parts) /ISO 13491 (all parts) or its equivalent. 6. All keys and key components shall be generated using an approved random or pseudo-random process such as NIST SP 800-22. 7. Documentation describing the set-up and operation of the key management solution must be made available upon request for evaluation purposes. 8. Keys shall be conveyed or transmitted in a secure manner. For example, the key distribution method described in X9/TR-34 Interoperable Method for Distribution of Symmetric Keys using Asymmetric Techniques, *Part 1–Using Factoring-Based Public Key Cryptography Unilateral Key Transport (to be published)* or equivalent should be used. • If remote key distribution is used, mutual authentication of the sending and receiving devices shall be performed. 9. Keys used in the data field encryption process: • Must be unique per device. • Must only be used to encrypt cardholder data and sensitive authentication data and cannot be used for any other purpose. • Keys used for PIN encryption must never be used for data field encryption (per PCI PIN Security Requirements).

Security Goal	Best Practice
Use key-lengths and cryptographic algorithms consistent with international and/or regional standards.	10. Encryption keys shall have strength of at least 112 equivalent bit strength. The following table summarizes equivalent bit strengths for commonly used approved algorithms | Algorithm	Bit Length
TDES	112[1]
AES	128[2]
RSA	2048
ECC	224
SHA	224 | For details on equivalent bit strengths, see *ISO TR-14742 Recommendations on Cryptographic Algorithms and their Use – Technical Report (to be published 2009).* 11. Any methods used to produce encrypted text of the same length and data type as the original cleartext shall be evaluated by at least one independent security evaluation organization and subjected to a peer review; such methods shall also be implemented following all guidelines of said evaluation and peer review including any recommendations for associated key management.
Protect devices used to perform cryptographic operations against physical/logical compromises.	12. Devices used to perform cryptographic operations should undergo independent assessment to ensure that the hardware and software they are using is resilient to attack. 13. Symmetric and private keys shall be protected against physical and logical compromise. Public keys shall be protected from substitution and their integrity and authenticity shall be ensured.

---

[1] For the purposes of these Best Practices, two key TDES (112-bits) should not process more than 1 million transactions. In cases where the number of transactions potentially processed through the system using a single 112-bits TDES key greatly exceeds 1 million, three key TDES (168-bits) or AES should be used. Note that key management schemes that greatly limit the number of transaction processed by a single key, such as Derived Unique Key Per Transaction (DUKPT) can be used to ensure that any individual key is used only a limited number of times.

[2] The smallest key size usable with AES is 128 bits. This key size is stronger than needed, but if AES is to be used, it is the smallest available. (Longer keys may of course be used if so desired.)

Security Goal	Best Practice

Use an alternate account or transaction identifier for business processes that requires the primary account number to be utilized after authorization, such as processing of recurring payments, customer loyalty programs or fraud management.	14. If any cardholder data (e.g. the PAN) is needed after authorization, a single-use or multi-use transaction ID or token should be used instead.
	• A single-use transaction ID is preferred.
	   o Acceptable methods for producing a single-use transaction ID include hashing of the PAN with a transaction-unique salt value, encrypting the PAN with an approved algorithm using a transaction-unique key, or equivalent. The single-use transaction ID can be produced by other methods provided that the resulting reference data is unique per transaction and the original cardholder data (e.g. the PAN) cannot be reproduced.
	• A multi-use transaction ID may be used if there is the need to maintain correlation (of the account) across multiple transactions.
	   o Acceptable methods for producing a multi-use transaction ID include hashing of the cardholder data using a fixed (but unique per merchant) salt value, or equivalent.
	
	NOTE: Irrespective of whether the transaction ID is a single use or multi-use, if a salt is used, the salt must be kept secret and appropriately protected. Salt should be a minimum length of 32-bits.

Conclusion

The payment industry, vendors and early adopters of field data encryption technologies should consider these best practices when evaluating or implementing data field encryption technology.