An Analysis of End-to-end Encryption as a Viable Solution for Securing Payment Card Data

Purpose
The purpose of this item is to examine end-to-end encryption in response to recent industry interest regarding it as a potential method to secure account number and transaction data. This discussion is limited to magnetic stripe transactions in a face-to-face environment.

MasterCard’s current position on encryption is as follows:

• MasterCard is encouraged by and supportive of the recent increased focus within the POI industry to better protect card number data from the first swipe to the next acquiring level.

• MasterCard also encourages product developers to continue to work together to develop ways of ensuring consistency in implementation.

• However, none of these solutions replace PCI compliance and they should be implemented in the context of an overall PCI program. With respect to the development of more specific standards regarding encryption, this should occur under the auspices of the Payment Card Industry (PCI) Security Standards Council.

• MasterCard considers EMV Chip & PIN and Dynamic PayPass™ as the preferred way forward for mitigating the risk of counterfeit fraud.

• Emerging point-to-point encryption solutions between the merchant and acquirer offer promising benefits for securing both magnetic stripe and Chip & PIN transactions, although currently no industry security standards exist for these solutions.

• Extending encryption beyond the initial acquirer point across the entire transaction cycle is a very complex and costly undertaking that may introduce new risks and ultimately detract from efforts to move from magnetic stripe to new payment technologies.

• As always, MasterCard is happy to speak with its customers about any specific requirements they may have to encrypt transactions leaving their host systems.
Overview

This document includes highlights and conclusions resulting from a MasterCard review of end-to-end encryption, its relative effectiveness (both benefits and flaws) and the estimated cost to the payment card industry to implement. The following additional factors have been considered in forming conclusions:

- Current industry deployments of end-to-end encryption are intended to secure data from the swipe at the POI to the acquirer and do not address the extension of encryption beyond the acquirer host system.
- The Payment Card Industry Data Security Standards (PCI DSS) offers appropriate protection for account and transaction data when those standards are appropriately followed.
- Members of the card industry on both sides of an authorization have made a significant investment in implementing Chip devices and cards in many areas of the world.
- Chip functionality is superior to current POS device read-head/OS-layer encryption at protecting account and transaction data across the entire processing chain and throughout a transaction’s life cycle.

BACKGROUND

The capture of magnetic stripe track data either at the point-of-interaction (POI) or via the breach of systems owned and managed by merchants or other stakeholders on the acquiring side of the business put over 279 million payment card numbers at risk in 2008 in the US alone. Four out of five breached entities were not certified PCI compliant prior to the compromise event, and the typical breached organization that had received a prior PCI certification met less than a third of the 12 PCI DSS requirements at the time of the breach. The mode of operation by which card and transaction data is illegally captured ranges from the downloading of improperly stored data in merchant, Third Party Processor (TPP), Data Storage Entity (DSE), and/or acquirer systems to eavesdropping the data transmitted by the point-of-sale (POS) or at another point in the transaction chain prior to it reaching the MasterCard Worldwide Network.

Acquiring-side industry stakeholders are looking at device-level encryption of the Primary Account Number (PAN) or transaction information as a method, either in lieu of or in addition to following PCI standards, to secure their data and thereby reduce or eliminate the risk of consequences of suffering a security breach.

This paper addresses the following topics:

- The true nature of current industry-available forms of encrypting authorization transaction information
- A discussion of the challenges involved in encrypting sensitive account data during transmission
- Cost components of building encryption into the authorization stream, and
- MasterCard’s present position with respect to the implementation of acquiring-side authorization transaction encryption.

In current industry discussions, encryption is commonly referred to as end-to-end encryption; however, current encryption methods focus only on the acquiring side of the authorization request transaction (vs. the full transaction cycle). The discussions gloss over important facts about transaction encryption that are critical to a full understanding of its value.

Acquiring-side authorization transaction encryption currently is offered to merchants as a service provided through POI terminal manufacturers, acquirers, TPPs, and ISOs. Most encryption solutions in the marketplace use tokenization of a portion of the PAN (typically the middle six digits) from the POI to as far as possible in the acquiring chain. For encryption to be fully effective, it should take place immediately at the magnetic stripe reader, although that will not always prevent skimming attacks while the card is being read.

There is a lack of consensus among encryption providers about where encryption should commence in the POI environment, either in the terminal read head or within the terminal operating system. Some solutions are based on encryption outside of the POS device, which allows potential data compromise by eavesdropping the clear text data exchanged between the terminal and the encryption module. Encryption in the terminal increases transaction security at the edge of the transaction message in the systems that inherently have the least security oversight and management, but the transaction message is still vulnerable to data capture before it is encrypted, possibly by corruption of the operating system and/or through the injection of malware. MasterCard therefore encourages the industry players to continue collaborating with respect to creating a common approach to minimizing these issues.

Some new terminals are being shipped with encryption software installed. Most existing terminals in the marketplace would require upgrades to be able to partially encrypt a portion of the PAN. Some newer devices are able to be upgraded remotely, while others require software or hardware upgrades completed in person at a cost of approximately USD11/device. Key-entered transactions are not able to be encrypted by most of the current encryption solutions.

While encrypting a portion of the PAN provides protection of sensitive account data, the encryption can actually never be end-to-end, as all encrypted data must be decrypted and re-encrypted as the transaction record moves from one system to another (e.g., from the merchant’s host system to the acquirer’s host system or from the acquirer’s host system to the MasterCard acquiring MasterCard Interface Processor-MIP). The points of decryption and the systems handling the PANs in the clear would remain unprotected by end-to-end encryption for even brief periods of time, sufficient to expose those systems to sophisticated attacks; therefore, all acquiring-side entities would need to maintain complete, constant compliance with the PCI Standards. A partially encrypted PAN remains potentially vulnerable to fraudsters who have the resources and time to attempt to decode the encryption method and match it to other unencrypted transaction data elements (i.e., the full magnetic stripe data and PIN), which may have been captured.

As an authorization transaction message is decrypted and re-encrypted, multiple new encryption keys are necessary and would require proper operator management, introducing additional complexity and risk into the authorization life cycle. Improper key management could become a new source of data compromise.

Tokenization inherently requires the merchant to rely upon its TPP or acquirer to decrypt and/or store data on its behalf so that some functions, which require the full PAN in the clear, may take place. The use of full PANs by acquirers and others include:

- Subscriptions, recurring billing and cards on file
- Initiating/processing returns, refunds and credits
- Chargeback processing
- Loyalty programs
- Fraud monitoring
- Clearing and settlement

Many TPP systems would require upgrades to be able to decrypt transaction data coming from the merchant.
EMV specifications (and resulting MasterCard M/Chip specifications) were developed to provide a secure alternative to magnetic stripe card functionality. EMV Chip security features include:

- Card validation of the PIN before an authorization request moves beyond the POS terminal
- Offline card authentication, by which the terminal can authenticate the card at the beginning of the transaction
- On-line card authentication, by which the card generates an unpredictable cryptogram (the Authorization Request Cryptogram or ARQC). The ARQC is generated using the account data, the transaction data and dynamic elements from the card and terminal.

The great strength of properly implemented EMV Chip technology, when compared to magnetic stripe, rests in the unpredictability of the ARQC. The ARQC can only be generated by the genuine card during a specific transaction, rendering the capture of account data and the ARQCs from previous transactions useless in the attempt to counterfeit cards. The dynamic ARQC is superior to the magnetic stripe CVC1, which is static and therefore can be copied and used to create counterfeit cards with the other account data. PayPass cards can also use the ARQC method or another similar dynamic cryptogram method known as CVC3.

CONCLUSIONS

Acquiring-side encryption, as defined above, can potentially improve the security of authorization transaction data for face-to-face swiped magnetic stripe transactions in the merchants’ environment, and may be an appropriate method of simplifying PCI compliance implementation plans for those merchants. Potential points of compromise remain, starting from the point of interaction to the various points in the chain, where it is necessary to decrypt and re-encrypt the PAN after it has left the merchants’ systems and use it in the clear for various purposes. Also, currently there are no industry standards for acquirer-side encryption. The risk of counterfeit fraud is greatly reduced once dynamic cryptographic techniques are used such as ARQC for EMV Chip and dynamic PayPass.

Encryption solutions that focus on securing data at the POI to the acquiring host system can provide additional security for merchants. However the extension of end-to-end encryption across the entire transaction cycle is not a short-term prospect and probably not a strategically sound alternative to the full implementation of EMV Chip technology in the long term. We would therefore view front-end encryption solutions as being a viable stop gap for merchants, however plans should always take into consideration the increasing role of EMV in the electronic payment environment and not distract from its broad adoption and use.