October 2014

Heartland

The Relationship Between PCI, Encryption and Tokenization:

What you need to know

Mike English
Executive Director, Product Development
Heartland Payment Systems

There is much confusion and misinformation on the Internet and in vendor publications on the subject of encryption and the impact of tokenization on reducing Payment Card Industry (PCI) compliance scope. This white paper addresses the facts regarding PCI, encryption and tokenization, as stated by PCI, Qualified Security Assessors (QSAs) and Internal Security Assessors (ISAs). It is intended to aid merchants and those companies accepting card payments by clarifying what is and what is not in PCI scope as related to encryption and tokenization.

Summary

The PCI DSS (Data Security Standard) guidelines state that companies and merchants that process and store credit card data must comply with well-defined audit requirements in twelve areas of cardholder data management and privacy. In doing so, the following points are becoming increasingly clear to these entities:

- Achieving and maintaining PCI DSS compliance is costly, perplexing, time-intensive and troublesome as cardholder data is often stored, transmitted and used in many different applications within a company or merchant's ecosystem.
- With the heightened number of merchant breaches in the news over the past 12 months, PCI DSS compliance does not equal security and is not enough to prevent data breaches. Those companies that have been breached are finding that cyber threats are increasingly sophisticated and hackers are going after data that they can monetize. They are also finding that PCI compliance is not sufficient to guard against breaches and the resulting issues.
- Emerging new business initiatives such as mobile, e-commerce, cloud and big data are expanding the PCI scope of these companies as well as increasing their risk and compliance costs.

Encryption's Impact on PCI Scope Reduction

PCI compliance scope reduction, such as encrypting cardholder data, does not remove a merchant from the requirement to be PCI compliant. A merchant is responsible to validate compliance to their acquirer, often through a qualified QSA or ISA. It is important to note that PCI DSS always applies to any and all businesses that accept card data. All applicable PCI DSS requirements for card data in scope apply if the following is true:

- If encrypted cardholder data is stored on a system, media or environment that also contains the decryption key
- If encrypted data is accessible to an entity that also has access to the decryption key

When Is Encrypted Cardholder Data out of Scope?

Encryption of cardholder data with strong cryptography is an acceptable method of rendering the data unreadable in order to meet PCI DSS Requirement 3.4.[1] The PCI SSC states, "Encrypted data may be deemed out of scope if, and only if, it has been validated by a QSA or ISA that the entity that possesses encrypted cardholder data does not have the means to decrypt it." If a merchant encrypts cardholder data but does not possess the means to decrypt it, the cardholder data is not considered in scope once it has been encrypted.[2] The best means to encrypt cardholder data is within a terminal or PIN pad that is PCI PTS certified.

[1] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

[2] https://pcissc.secure.force.com/faq/articles/Frequently_Asked_Question/Is-encrypted-cardholder-data-in-scope-for-PCI-DSS/

"The important phrase in the aforementioned definition is 'if, and only if.' The only way encrypted cardholder data (CHD) is out of scope is if the entity being assessed for PCI compliance cannot decrypt the encrypted CHD. This is a very important concept that gets constantly misinterpreted by QSAs and their clients. However, it is up to the QSA to confirm that the organization being assessed cannot decrypt the encrypted CHD and to document the procedures conducted to prove that fact."[3]

If a merchant or business accepting credit cards outsources encryption or key management operations to a third party, the merchant or business is responsible, as part of their due diligence processes, to ensure that all applicable PCI requirements are being met by the third party, including the security of any cryptographic operations used to encrypt the data.

In summary:

- An encrypted PAN is still defined as cardholder data and in scope for PCI DSS compliance if the merchant has access to the key and the ability to decrypt data
- If a merchant has no ability to decrypt encrypted data, the encrypted data is not card data and is NOT in scope of PCI
- Systems that transmit, process and store encrypted data are not in scope
- Encryption removes clear text card data at point of entry to eliminate risk and reduce PCI scope
- By removing clear card data from the merchant's environment, the opportunity for monetization of the card data is also eliminated or greatly reduced

Tokenization's Impact on PCI Scope Reduction

Tokenization, which is a way of replacing sensitive data like credit card numbers with tokens, is one of the data protection and audit scope reduction methods that is recommended by PCI DSS.[4] The use of tokens for post-authorization operations such as returns, chargebacks, recurring payments, sales reports, analytics or marketing programs eliminates the storage of the PAN (Primary Account Number) and subsequent use of PAN. Tokenization takes applications and systems for these business processes out of PCI scope.

However, per a PCI Information Supplement: PCI DSS Tokenization Guideline that was published by PCI in August 2011, "Tokenization solutions do not eliminate the need to maintain and validate PCI DSS compliance, but they may simplify a merchant's validation efforts by reducing the number of system components for which PCI DSS requirements apply."[5]

[3] http://pciguru.wordpress.com/2013/03/07/encrypted-cardholder-data-out-of-scope/
[4] https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf
[5] https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

Per the PCI DSS Tokenization Guidelines, PCI Data Security Standard (PCI DSS), Version 2, published August 2011:

In PCI scope:

- All elements of the tokenization system and tokenization process, including de-tokenization and PAN storage, are considered part of the cardholder data environment (CDE) and are in scope for PCI DSS.
- Any system component or process with access to the tokenization system or the tokenization/de-tokenization process is considered in scope.

Out of PCI scope:

- System components that:
  - are adequately isolated from the tokenization system and the CDE
  - that store, process or transmit only tokens
  - that do not store, process, or transmit any cardholder data or sensitive authentication data
  - may be considered outside of the CDE and possibly out of scope for PCI DSS

Tokenization Scoping Principles

When scoping a tokenization environment for PCI DSS, the following general principles apply:

- All components of a tokenization system are considered part of the CDE and are always in scope since they store, process, and/or transmit cardholder data
- System components that provide the ability to perform either of the following functions are in scope:
  - Generate a token in exchange for a PAN
  - Redeem a PAN in exchange for a token
- Any system component or process with access to the tokenization system or tokenization/de-tokenization processes is considered in scope as it is connected to the CDE
- Any other system component located within or connected to the CDE, even if it does not perform tokenization or de-tokenization operations, is in scope

Out-of-Scope Considerations for Tokenization

To be considered out of scope for PCI DSS, tokens and the system components that store, process and/or transmit tokens need to meet the following points:

- Recovery of the PAN value associated with a token must not be possible through knowledge of the token, multiple tokens, or other combinations
- PAN cannot be retrieved even if the token and the systems it resides on are compromised
  - System components are isolated from any application, system, process or user with the ability to submit a de-tokenization request for that token and retrieve the PAN:
    - Access to the tokenization system, data vault, or cryptographic keys for that token
    - Access to token input data or other information that can be used to de-tokenize or derive the PAN value from the token
  - System components are not connected to the tokenization system or processes, including the data vault, or cryptographic key storage
  - System components are not located within or connected to the CDE, nor do they have access to any authentication credentials that can be used to authenticate to any part of the CDE
  - System components do not store, process, or transmit cardholder data or sensitive authentication data through any other channel
  - System components that previously stored, processed or transmitted cardholder data prior to implementation of the tokenization solution have been examined to ensure that all traces of cardholder data have been securely deleted

Additionally, the *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures*, Version 3.0, November 2013 states the following:[6]

- Render PAN unreadable anywhere it is stored including on portable digital media, backup media, and in logs by using any of the following approaches:
  - One-way hashes based on strong cryptography, (hash must be of the entire PAN)
  - Truncation (hashing cannot be used to replace the truncated segment of PAN)
  - Index tokens and pads (pads must be securely stored)
  - Strong cryptography with associated key-management processes and procedures

In summary, to be considered out of scope for PCI DSS, tokens and the system components that store, process and/or transmit tokens need to replace the PAN with a token, PAN cannot be retrieved, and tokenization is isolated.

It's Really About Risk Management

PCI DSS compliance does not provide optimal security and is not enough to prevent data breaches. Companies that have been breached are finding that cyber threats are increasingly sophisticated and hackers are going after data they can monetize. Simply stated, both encryption and tokenization would have not prevented the breaches that occurred at these merchants, but would have stopped the monetization of the card data by making the card data unusable.

Encryption and tokenization complement PCI by removing card data from the merchant's environment. Encryption at swipe, tap, card insert or key entry immediately removes card data from the merchant's environment. Tokenization eliminates the need to access and reuse customer card data for further transactions or analysis, and also removes card data from the merchant's environment.

[6] https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Heartland Secure

Heartland Secure™ is a comprehensive card data security solution that combines three powerful technologies, working in tandem, to provide merchants with the highest level of security available to protect against card-present data fraud. Featuring the only warranty of its kind in the payments industry, this exclusive solution is designed to provide businesses with security against point-of-sale (POS) intrusions, insider misuse, and other common sources of data fraud, by eliminating the opportunity for criminals to monetize card data.

Offered to Heartland customers for no extra service fees, Heartland Secure combines:

- EMV electronic chip card technology to authenticate that a consumer's card is genuine;
- Heartland's E3™ end-to-end encryption technology, which immediately encrypts card data as it is entered so that no one else can read it; and
- Tokenization technology, which replaces card data with "tokens" that can be used for returns and repeat purchases, but are unusable by outsiders and have no value.

Heartland SECURE

Questions?

If you have questions about EMV, lowering your cost of payments, how to better manage your store network, improving transaction security, payroll management or anything related to payment processing, please reach out to us at heartlandpaymentsystems.com/about/contact us.