

pci update

Tokenization Guidelines from the PCI Council: What Does it Really Mean?

by Sue Zloth

Merchants have been waiting for guidance from the PCI Council on the emerging security technologies slated to impact PCI compliance efforts. Late last year, the encryption guidelines were released, followed by virtualization guidance and most recently, the official tokenization guidelines.

The tokenization task force has been working on this guidance for a long time and is happy to see it finally released to the public. These guidelines provide much-needed direction on how to implement tokenization solutions and how they impact the scope of a merchant's compliance efforts with the PCI Data Security Standard (PCI DSS.)

There have already been a lot of questions and conversations about the guidelines. Many smaller merchants and independent sales organizations have been wading through the 23-page document to determine what the guidance means for them.

Here are some of the pressing questions that we at Merchant Link are hearing about the guidance, and some answers.

What is a token and how does tokenization work?

Let's start at the beginning and define tokenization. Tokenization is a process by which the primary account number (PAN) is replaced with a surrogate value, called a token.

So, as a merchant, if you are authorizing transactions all day long and send a settlement file at night, you have a large amount of sensitive card data sitting on your system for a period of time.

In fact, this same information may be sitting on your system for weeks, or even months, and this becomes very enticing to hackers.

A properly-implemented tokenization system can help reduce the places where merchants store data, which is known as the Cardholder Data Environment (CDE.) This means that the merchant is more secure and doesn't have to spend as much money on achieving PCI compliance.

Are there different types of tokens?

In the tokenization guidelines, the Council points out that there are various types of tokenization products on the market today. To ensure that a

merchant implements the proper solution, they must first understand which type of tokenization solution best fits their needs.

In today's market there are both single-use tokens and multi-use tokens. Single-use tokens are used to represent a specific, single transaction; whereas a multi-use token represents the PAN and can be used to track that specific PAN across multiple transactions.

Which one is right for my business?

To determine which type of token is appropriate for their business, a merchant needs to evaluate their business model. If it is necessary for the merchant to track data for analytics purposes, multi-use tokens are needed to keep their business processes functioning correctly. If that is not necessary, a single-token approach could be more beneficial.

According to the PCI guidelines for tokenization, "whichever generation method is used, the recovery of the original PAN must not be computationally feasible knowing only the token or a number of tokens. This is true for both single-use and multi-use tokens. Additionally, access to multiple token-to-PAN pairs should not allow the ability to predict or determine other PAN values from knowledge of only tokens. Tokens should have no value if compromised or stolen, and should be unusable to an attacker if a system storing only tokens is compromised." This means that it should be virtually impossible for a hacker to reverse-engineer back to the original PAN.

What should I consider before implementing tokenization?

The tokenization solution provider that a merchant selects needs to demonstrate the capability and flexibility that makes the most sense for their business. It is also critical that the provider has experience and expertise in both payments and security.

The guidelines provide some best practices that a merchant should keep in mind when searching for the right tokenization solution.

As a general principle, the Council recommends that tokenization and de-tokenization operations should occur only within a clearly defined tokenization system that includes a process for approved applications to submit tokenization and de-tokenization requests.

In addition, strong authentication and access controls must exist for all access to the tokenization system, whether for tokenizing or de-tokenizing data, and authentication credentials must be secured from unauthorized access or use.

Finally, all components within the tokenization system (for example, the token generation and mapping process, data vault and cryptographic key management) must be located in a PCI DSS compliant environment.

Will tokenization absolve a merchant of PCI requirements?

This is a misperception and is absolutely false. Merchants must understand that there is no "silver bullet" when it comes to PCI compliance. The need to meet PCI requirements will not disappear when tokenization solutions are implemented. Every merchant that accepts card payments must follow the PCI Data Security Standards.

That being said, solutions like tokenization can minimize the scope of a merchant's CDE, which reduces a merchant's PCI scope and offers a cost reduction on compliance efforts. By using a tokenization solution that removes all data from the network and stores the data in an off-site secure vault, the scope is significantly minimized. ■

Sue Zloth is product group manager at payment data security provider Merchant Link, a member of the PCI Council's tokenization task force and head of the payment security group for Hotel Technology Next Generation. She is a frequent blogger on SecurityCents where you can view her full bio and contact.

back to articles