

What Does Tokenization Mean To You?

Choose banking relationships wisely when weighing the value of your tokenization solution.

by J. David Oder

Over the past few months leading up to and following a recent Payment Card Industry Security conference, there has been a veritable plethora of announcements about “emerging” payment security technologies, including end-to-end encryption and tokenization. Players in the payment security industry have made an announcement of their new tokenization or end-to-end solution. Some have even announced combinations of tokenization and end-to-end solutions.

Speaking as someone in the middle of the payment industry and one of the guys who coined the term “tokenization,” these announcements are overwhelming and confusing. I wonder how a retail merchant views them. All I hear is, “Me, too,” “I’ve got that, too,” or “Look at mine; it’s really cool.” But, what I don’t hear is how it works, what it does, how much it costs, when it is available, and how long it has been available to merchants.

While there are a number of things being called tokenization, the term was defined for the first time in the payment industry in 2005 at a security conference in Las Vegas. Many “tokenization-in-name-only” adaptations exist, but they are in fact various encryption keys handlers, hashing schemes, and “at-once” transaction schemes.

Tokenization replaces the card number with a randomly generated, unique, alphanumeric value representing the card information for a particular transaction and merchant, used mostly, but not exclusively, for postauthorization data retention. That is, the token can only be used by the merchant referencing a particular transaction. A token is not a key, a partial key, a hash, or any one-to-one relationship with a card number.

True tokenization can be used for processing, transmitting, and storing credit card numbers in a secure manner. Make sure that if you are offered a tokenization solution, it closely matches this definition, and it gives you the ability to use it for everything for which you could use the actual card data. Furthermore, ask how long the particular tokenization solution has been working, and make sure that millions, if not billions, of successful tokenized transactions are already in use.

The nature of tokenization means that in order to simplify your PCI DSS (Payment Card Industry Data Security Standard) compliance, a third party holds the actual card data for you, and you are given a token in its place. They



should allow you to use the token for future transactions, if necessary, for credits, layaways, or payment plans. Because of the close relationship you will have with your tokenization provider, you need to make sure they can give you the flexibility you require for the future.

Does Tokenization Tie You To A Merchant Bank?

Many of the recent announcements have come from merchant banks, merchant services providers, and processors. The problem with using tokenization from merchant banks’ merchant services providers is that you are tied to that merchant bank, etc. for as long as you need to use your tokens. Depending on your business and your need for future use of tokens, you could be tied to that bank forever. Therefore, you might think that you would be tied to anyone supplying you with tokens. That is true, but if the firm you use is independent from any bank or financial institution, you will not be tied to a merchant bank. You will be able to change banks to pursue lower discount rates or other needs. While this article predominantly covers tokenization, the advice is applicable to end-to-end providers, too. If the bank holds the keys to the encryption, it holds you captive.

With all the news about bank failures, you are reminded of the importance of choosing banking relationships wisely and the unmitigated value of a bank-independent company supplying your tokenization solution. Declare your independence. ■



J. David Oder is president, CEO, and founder of Shift4 Corporation. He can be reached at dave@shift4.com.