



# Shift4<sup>®</sup>

## Secure Payment Processing

---

### **Tokenization**

The Best Way to Secure Data is to Not Store Data

Authored by Dr. Heather Mark, Ph.D., CISSP and J.D. Oder II

August 2007

## Executive summary

Credit card data theft is a threat to any business regardless of its size or industry focus. Should a credit card security breach occur, the affected company can suffer irreparable damage to its brand image and bottom line. Credit card data theft is also a domestic security threat. The Department of Homeland Security, the FBI, and other agencies report that data theft is a growing source of revenue for global terrorist organizations.

The growth in the number of compromises has been accompanied by a corresponding shift in breaches that target away from payment processors with large amounts of credit card data to more traditional retail merchants and especially hotels, restaurants, and other companies in the hospitality, travel and entertainment industries. The reason for this change has to do with the thief's ultimate objective. While the credit card account number alone has limited value to a data thief, the data found on the magnetic stripe of the card is the focus of card thieves today. Obtaining only the second track of the magnetic stripe on the back of a credit card will enable the criminal to create counterfeit cards that can either be used as a traditional swipe card by the criminal or sold on the black market to other criminals. In short, obtaining the magnetic stripe data allows for a greater return with less risk for the criminal.

The end result is that brick and mortar businesses, as a general rule, are at greater risk of compromise than e-commerce merchants. Restaurants, hotels and other companies in the travel and entertainment segment are even more attractive targets. Because the primary goal of data thieves today is to counterfeit cards to be resold, they are seeking cards with high credit limits and a low likelihood of fraud being reported by the user. Cards issued to frequent business travelers fit this description. Additionally, hotels and restaurants tend to store more

information in order to facilitate tips, late fees and similar associated charges.

### Disclaimer

The information provided herein is for informational purposes only. This paper is not meant as compliance advice. Prior to taking any steps that may affect your compliance status with industry or government mandates always seek advice from your compliance auditor and/or legal counsel.

## Tokenization and PCI compliance **Traditional encryption**

The Payment Card Industry (PCI) Data Security Standards sets forth a number of requirements with which members of the industry must comply. PCI requires that companies “keep cardholder information storage to a minimum.” In order to comply with PCI, it is required that all account numbers be encrypted, truncated, or otherwise rendered unreadable. Additionally, PCI requires that all sensitive cardholder data be rendered unreadable anywhere it is stored, including within system and application log files.

In this environment, securing credit card data and preventing its unauthorized use, while also preserving the payment processing systems now in use by millions of merchants, is a vital concern for consumers, government and businesses. Shift4 Corporation ([www.shift4.com](http://www.shift4.com)) developed a technology known as Tokenization that safeguards credit card data. The primary objective of Tokenization is to enable businesses to operate normally while not storing sensitive data that is the target of data hackers. Payment applications built on Tokenization can be used on existing systems, so merchants need not buy new equipment or retrain personnel.

Tokenization is different from encryption, the traditional method for protecting data. The term “encryption” applies to the use of cryptographic algorithms to render data unreadable unless the user possesses the appropriate cryptographic ‘keys’ to decrypt the data. Generally, there are two basic methods of encrypting data: symmetric and asymmetric cryptography. In symmetric encryption, also known as private-key cryptography, the same cryptographic key is used to encrypt and decrypt the data. Symmetric encryption is generally used between two parties that are known to each other and trusted. Symmetric encryption is commonly used in database and system file encryption. In contrast, in asymmetric encryption, also known as public-key cryptography, one cryptographic key is used to encrypt the data, while another, mathematically related key is used to decrypt it. Asymmetric cryptography is commonly used in email encryption programs where two unknown or untrusted parties are exchanging data. While the use of encryption does render data unreadable, it does come with its own set of issues and challenges.

The most critical issue with the use of encryption is the management and protection of the cryptographic keys. The importance of proper key management cannot be overstated, as the disclosure of cryptographic keys to unauthorized personnel could result in the compromise of encrypted data. If sensitive data is encrypted and the keys are compromised, this data can be viewed as easily as data that has not been encrypted. The cryptographic keys must be secured at all times to prevent their misuse and the unauthorized access to sensitive, encrypted data. In order to ensure the protection of the keys, a strict set of key management procedures must be established and followed. Key management entails the proper storage, use, destruction, creation and dissemination of the cryptographic keys. In addition, sufficient technological, administrative and logistical controls must be put in place around the keys to ensure that unauthorized individuals do

not have access to them.

In short, although encryption does enable companies to comply with PCI while allowing the storage of sensitive data, using encryption alone is not sufficient to protect data. The cryptographic keys must be treated with the same care as the data, as a compromise of the keys will result in a compromise of the encrypted data. It is simply a case of switching protection from the data, in instances where it is unencrypted, to the cryptographic keys in instances where the data is encrypted. In addition to key management, companies must ensure that the encryption method selected is of sufficient strength.

## Tokenization

In 2005, Shift4 created a new technology known as Tokenization, and released to the public, free of charge and without patent. Tokenization was designed to provide even greater protection to merchants by removing the storage of all cardholder data while enabling the customer to operate in a normal capacity. The theory behind Tokenization is simple: *The best way to secure data is to not store data at all.*

The basics of Tokenization are also straightforward. A transaction is swiped as usual at a point-of-sale (POS) terminal. Once transmitted to Shift4 for authorization, the information is converted into a representation of the data using a proprietary technology developed by Shift4. This data representation is known as a “Token” and is a globally unique, randomized representation of credit card data that is the same length as the original card number. After Shift4 receives the authorization response from the processor, the Token is then transmitted to the customer while the sensitive authorization response, containing the actual card number, remains with Shift4 and is securely stored. This means that the merchant does not have to store the cardholder number.

The Token spans the lifetime of the transaction, so it provides all of the same support for tips, tabs, incremental authorizations and chargebacks as a stored card number would. Essentially, the Token is stored on the POS system, as the cardholder number would be in a traditional setup. When an incremental authorization is required on the card, the Token is sent to Shift4. Shift4 then translates that Token into the card data for transmission to the processor. The processor returns the authorization response and Shift4 converts the data into a new, unique Token, representing a new transaction. This new Token is then sent along with the approval code to the merchant. The authorization is completed and again no credit card data is stored on the

merchant system.

In comparison with other Tokenization-type services offered by competing companies, Shift4's Tokenization offers a greater level of protection against compromise of cardholder data. Some providers allow their merchants to collect the card number along with the card identifier (similar to Shift4's Token). Still others may require the merchant to manually register each card identifier. Both of these practices undermine the primary objective of Tokenization; namely to enable merchants to operate as normally as possible while not storing the sensitive data that is the target of data thieves.

Additionally, some service providers offering Tokenization-like services do not have adequate applications or application layer support to enable merchants to operate in a normal fashion while using a representation of data. This means that these service providers can not offer the necessary transaction reporting unless they allow the merchants to import the card numbers back into their systems and thereby defeating the purpose of their own solutions. Each of these competing methods undermines the purpose and goal of Tokenization: reducing the likelihood of a data compromise or other serious event.

## Implementing Tokenization

Implementing Tokenization requires some small changes on the POS or PMS side. For example, an addendum must be added asking for the Token information instead of the cardholder account number. The Token can be stored in the now empty card number field, which is already set up to receive this type of data. Because the Token includes the last four digits of the credit card number, all of the POS and PMS system reports will still be fully functional. The Token must also be stored, but this is easily accomplished, as well. From a merchant's point of view, the implementation is seamless. In fact, it can be implemented even when there are pending sales or open tickets remaining.

Tokenization reinforces the overall objectives of PCI standards, as well as specific requirements. First and foremost, it addresses PCI requirement 3: "Protect Stored Data." By returning only Tokens in response to merchant requests, cardholder information need not be stored on the merchant system. Nor do merchants have the added concern of ensuring that the method of encryption used is of adequate strength and complexity. And, since the merchant is not required to encrypt the Token, there are no encryption keys to manage.

PCI requirement 3.4 mandates that all cardholder data be rendered unreadable using one of several forms of strong encryption. One of the methods suggested is the use of truncation. Since only the last four digits of the card number are used in the Token, the Tokenization process meets this requirement.

Since the merchant is not using encryption to derive the Token, the Tokenization process renders requirements 3.5 and 3.6 moot. Requirement 3.5 states that all encryption keys should be protected against misuse and disclosure. The Token is sent to the merchant, rather than derived by the merchant using encryption keys.

Therefore, the merchant has no keys that must be protected. Similarly, requirement 3.6 mandates the development and implementation of key management processes and procedures. Again, since the merchant uses no encryption, there are no keys to be managed. This ultimately results in cost savings to the merchant, as well.

## Conclusion

Tokenization provides the ability to eliminate much of the sensitive data that is usually stored, thereby protecting merchants and supporting the objectives of PCI. It is important to understand that while Tokenization considerably lessens the burden of compliance, it does not completely remove the obligation to comply with relevant industry requirements.

Merchants are being targeted more frequently than ever before and with greater success for the criminal. In addition to the public fallout and brand damage that inevitably occurs as a result of a data compromise, current state and federal legislation exposes merchants to significant financial and legal liability should they be unfortunate enough to experience a data compromise. Keeping abreast of the new exploits and attack methods makes the protection of sensitive data a challenging proposition for even the most security-minded of companies. Those without the internal expertise to guard against the onslaught of data thieves are gambling with their company's assets.

## About the authors

### **Dr. Heather Mark, Ph.D., CISSP**

Sr. Vice President  
The Aegenis Group

Dr. Mark is an experienced information security and privacy professional who is both well known and respected within the Payment Services Industry. Prior to joining The Aegenis Group, Dr. Mark co-founded a Qualified Security Assessment Company and worked at various technology companies supporting PCI efforts. Her expertise helped develop a variety of assessment methods and practices that assisted companies in achieving compliance in a cost-effective, timely manner.

Dr. Mark has spoken at numerous industry events on topics of information security, privacy and the intersection between the two. In addition, she is an experienced instructor and taught for two years at Auburn University while a Doctoral Candidate. Dr. Mark writes a monthly article for Transaction World Magazine and has a PhD in Public Administration and Public Policy from Auburn University. Her knowledge of public policy and the ability to analyze the impact of that policy on day-to-day business practices gives her a unique insight into the compliance landscape. Dr. Mark holds a certificate in Marketing Research from the University of Georgia, is a Certified Information Systems Security Professional (CISSP), and a Certified Information Privacy Professional (CIPP).

### **J.D. Oder II**

Sr. Vice President of Research & Development and CTO  
Shift4 Corporation

J.D. is a founder of Shift4 Corporation, chief designer of the DOLLARS ON THE NET gateway system and leads Shift4's systems operation and development efforts. He holds degrees in Cognitive Science and Computer Science with numerous networking and information security credentials.

J.D. became an early adopter/member of the PCI Security Standards Council and was recently named as a 2006 Mover and Shaker by Transaction World Magazine. J.D. is responsible for many innovations, including Tokenization technology, which revolutionized the payments industry when it was released in 2005. Following the release of Tokenization, J.D. and his development team are very excited to exhibit 4Go SecureSuite™, which represents the final mile in Shift4's race to create "Real Security", an environment where absolutely no cardholder data exists at the POS.



1491 Center Crossing Road  
Las Vegas, NV 89144-7047  
**Office:** (702) 597-2480

1453 South Dixie Drive, Suite 250  
St. George, UT 84770-5845  
**Office:** (435) 628-5454

**Fax:** (702) 597-2499  
**Sales:** (800) 265-5795

<http://www.shift4.com>