



Shift4[®]

Secure Payment Processing

Storing Credit Card Data

A Look at the Business Needs, Regulations and Solutions Regarding the Issue

Authored by Dr. Heather Mark, Ph.D., CISSP

January 2006

Includes a Look at Shift4's Tokenization Technology

Executive summary

Over the past several years, the card associations, as well as both state and federal governments, have increased their focus on the security of sensitive customer information. In January 2005, the four major card associations jointly released the Payment Card Industry Data Security Standards, commonly referred to as PCI. Among its many requirements is the mandate that cardholder information be rendered unreadable and protected from unauthorized access and use. In fact, the card associations have adopted a “don’t store what you don’t need” philosophy, requiring that businesses store only the barest minimum of cardholder information.

Despite the legitimate business needs that may drive a business to retain sensitive data, the storage and protection of such information has recently come under fire. Several high-profile security breaches in 2005 have brought the issue under the microscope of congressional hearings and Federal Trade Commission scrutiny. Recognizing the incompatibility of the responsibilities inherent in storing cardholder data and the reasons that some businesses may have to retain that data, Shift4 has developed a technology, known as Tokenization, that enables compliance with the data security standards, while still facilitating the needs of the merchants.

In order to help its customers comply with relevant industry regulations, Shift4 has developed a process that will ease the compliance process while simultaneously increasing the level of security surrounding the stored credit card account number. Using Tokenization, the merchant is able to send the pre-authorization or authorization request to Shift4, which then returns a response. Rather than using the card number as the reference, however, a Token, or representation of the card number, will be used. This drastically reduces the amount of cardholder information being retained by the merchant. Since the Token contains only the last four numbers of the account number, Tokenization renders the card number unreadable.

If a data security compromise should occur, there is no danger that the Tokens stored by the merchant could be connected to a viable account number. A reduction in stored cardholder data can translate into reduced compliance efforts and costs.

The following paper includes a discussion of the particular security issues surrounding the practices of incremental authorization and recurring payments that are common in today’s business environment. It will provide a discussion of the card associations’ focus on data security, the traditional methods used to store and secure cardholder information, and the difficulties faced in complying with PCI standards. Following that, the Tokenization technology and the ways in which it impacts compliance will be examined.

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.

Introduction

Since 2001, issues of data security in the Payment Services Industry have garnered ever-increasing attention. Among the reasons for this attention is the focus of card associations on the protection of cardholder data in response to the increasingly frequent compromise of sensitive data. The Payment Card Industry (PCI) Data Security Standards set forth a number of requirements with which members of the industry must comply. PCI requires that companies “keep cardholder information storage to a minimum¹.” Additionally, PCI requires that all sensitive cardholder data be rendered unreadable anywhere it is stored, including within system and application log files. In order to comply with PCI, it is required that all account numbers be encrypted, truncated, or otherwise rendered ‘unreadable’. Clearly, the hardships imposed to adequately protect cardholder data can be onerous.

In the hospitality industry, or in any environment that necessitates recurring payments or incremental authorizations, such a requirement can be extremely troublesome. For example, merchants have historically held this data to process tips and tabs in a restaurant environment, enable recurring billing for retail and e-commerce transactions, and to enable lodging and auto rental merchants to charge multiple items, nights, and similar charges to a single invoice. In addition to storage for incremental authorizations and recurring payments, cardholder data is often written and stored in log files to enable issue investigation and resolution. Irrespective of the business need, in all cases, the accountability for protecting the data, whether it is retained in log files or is being stored in a database for incremental charges, now lies with the merchant.

The recent focus on the storage of sensitive information by

the card associations magnifies the requirements for protecting such data. In the April 11, 2005 edition of the Green Sheet, John Shaughnessy, Senior Vice-President of Visa USA Risk Management, stated that the issue of magnetic stripe data was of paramount importance to Visa USA. In fact, Mr. Shaughnessy stated that the association is focused on this issue “like a laser².” The challenge with eliminating the storage of such data is that it is not always the merchant that knowingly or intentionally makes the decision to store the data. It is not uncommon for software applications and Point-of-Sale (POS) solutions or card-swipe terminals to store sensitive data unbeknownst to the merchant.

In addition to the card associations, the U.S. government has now begun to focus its attention on the retention of cardholder information. Recent incidents such as the Card Systems Solutions (CSSI) breach have made magnetic stripe data a focus of congressional hearings. Card Systems Services suffered perhaps the most publicized security breach in which at least 40 million credit card account numbers were compromised. In the aftermath of the breach, the forensic investigation found that CSSI had been storing full magnetic stripe data, in direct violation of PCI requirements.

Compounding the issue was the fact that the information that CSSI was authorized to store was not encrypted. Both Visa USA and MasterCard International cited CSSI’s improper retention of magnetic stripe and transaction data during their respective testimony before Congress. Given the focus on the retention of sensitive data, and of full magnetic stripe data in particular, it is only reasonable to assume a continued focus on the issue from both the card associations and the government.

¹ PCI Requirement 3.1

² Campeau, Juliet. Green Sheet Issue 5:04:01 (April 11, 2005) “All Together Now: Don’t Store What you Don’t Need.” Available on the World Wide Web at: <http://www.greensheet.com/PriorIssues-/050401-/050401.html>

Traditional methods of securing sensitive data

Traditionally, the primary method of securing stored sensitive data has been through the use of encryption technologies. 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 logical controls must be put in place around the keys to ensure that unauthorized individuals do not have access to them. This endeavor can necessitate significant resources. As an example of the complexity of key management, the National Institute for Standards and Technology (NIST) has published an 80-page guide just on best practices surrounding cryptographic key-management procedures³.

While many POS systems do not encrypt data, the ones that do bring their own set of challenges. It is often the case that the merchant using the POS system is not the party managing the cryptographic keys, although it is the merchant responsible for the security of the data.

In many systems, the POS vendor manages the POS solution, including the cryptographic keys. In these cases, the merchant has little control over the management and protection of the keys. It is an unfortunate fact that in some cases, the vendor may utilize a limited number of cryptographic keys for all of their merchants. As such, no merchant is using a unique key. Should the shared keys be compromised on the POS vendor’s side, or on one of the other merchants’ systems, it is conceivable that the encryption keys of all of the other merchants would be vulnerable, putting all the cardholder data held by the merchants at risk. PCI requires that merchants partner only with service providers (processors, POS vendors, etc.) that have been validated as compliant with PCI. Unfortunately, if the POS vendor fails to live up to those requirements, it is the merchants and acquiring banks that are held accountable. The card associations do not have authority to hold the POS vendor accountable for a breach that results in the loss of merchant data. The unfortunate

³ Barker, Elaine et al. “Recommendation for Key Management – Part 2: Best Practices for Key Management,” NIST Special Publication 800-57. Available on the World Wide Web at <http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf>

STORING CREDIT CARD DATA

result is that POS vendors do not necessarily have the same focus on compliance and security that the rest of the industry does.

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. Commonly, transactions are protected using 3DES 128-bit encryption. There are a number of additional, stronger encryption methods available for use as well, such as the Advanced Encryption Standard (AES), Blowfish or Two-Fish. Unfortunately, encryption technology can best be described as an ongoing arms race. As computing power increases, it becomes inevitable that someone will break the encryption, given enough time. To date, 56-bit DES has already been broken, as well as several cryptographic hash functions. Therefore, the encryption method must be continuously updated to ensure that it is still appropriately strong to protect data.

Another challenge with the use of encryption technology that is rarely discussed is that of optical recognition or pattern determination. PCI requires that all cardholder data be encrypted using at least 3DES 128-bit encryption. This is generally considered a best practice in information security. However, if the data is misappropriated, it may be possible for an individual or program to recognize a pattern in the encrypted data. In essence, this results in exposure of the

encrypted data without breaking the actual encryption. For example, when cardholder data is stored in a database it is usually stored in a sequential pattern.

When the data is encrypted using 3DES 128-bit encryption, the resulting ciphered text is also stored in a sequential fashion. If the pattern were recognized, the mal-intentioned individual could focus efforts on breaking just one portion of the encrypted information, which would thereby unzip the entire encrypted database. This method is commonly used to 'crack' Windows passwords that are 'hashed' using the MD-5 algorithm. In theory, with a large enough population of encrypted data and known variables, this process can be used to determine any pattern of data.

Given the above issues, it is clear that, while certainly still a very good practice for protecting stored data, encryption alone is not sufficient to ensure the security of personally identifiable information.

Compliance difficulties

Understanding the issues addressed above, the difficulties in achieving compliance with PCI begin to emerge. While PCI does provide companies with an excellent guideline for securing data, it is sometimes difficult to reconcile PCI requirements with the realities of the business environment in which many companies operate. Following is a brief discussion of some of the more onerous requirements and the difficulties found in complying with them.

The requirement at the heart of the PCI program is Requirement 3, which states that companies must “Protect Stored Data.” Specifically, Requirement 3.1 states:

“Keep cardholder information storage to a minimum. Develop a data retention and disposal policy. Limit your storage amount and retention time to that which is required for business, legal and/or regulatory purposes, as documented by the data retention policy.”

This seems very straightforward. In essence, the card associations are saying, “don’t store what you don’t need.” Storage of cardholder data is not necessarily a convenience, but is often a necessity. Often the card data is used to perform incremental authorizations or delayed settlements that are integral to the way the merchant does business. For example, in the restaurant environment, the card is first authorized for the amount of the bill. However, it is frequently necessary to add incremental charges, such as tips and tabs to the bill after the cardholder has left. In order to complete the transaction process with the additional charges, the merchant has to retain card information.

The lodging and car rental industries are environments in which incremental authorization is a necessity. Both hotels and car rental businesses require a credit card authorization in order to make reservations. Storing the cardholder Information enables hotels and auto rental businesses to

charge multiple items to a single invoice.

Consumers want and expect the ability to charge items to their room from the gift shop, restaurant, spa, etc. In some cases, it may not always be possible to ask the customer to present a card to cover the cost of incidentals. The customer may have already checked out, for instance, prior to the discovery of a depleted honor bar, or they may have said they would return the car with a full tank of gas, but in fact did not.

Mail order, telephone order and online businesses are required to operate using a “book and ship” model. In the “book and ship” model, the order is placed, but the credit card is not charged until the order is actually shipped. In these cases, cardholder information must be retained until the order is shipped and the card is charged for the amount of the order. In each of these cases, the merchant is subject to great risk between the time that the pre-authorization or authorization is requested and the time that the transaction is completed. Merchants who charge monthly memberships, such as spa, clubs, and gyms, also store the credit card data in order to process these monthly charges.

The “don’t store what you don’t need theme” is reinforced by Requirement 3.2-3.2.3, which prohibits the storage of any authentication data subsequent to the transaction. This prohibition applies even to data that is encrypted. Authentication data includes CVV2/CVC2, full magnetic stripe data (CVC1 & service code), and the PIN Verification Value (PVV).

The constraints placed on the storage of cardholder data create difficulties for those offering recurring payments. According to an industry survey, most customers that have recurring bills would switch to a merchant that offers a recurring payment solution⁴. While both the merchant and the customer benefit from the use of recurring payment

STORING CREDIT CARD DATA

solutions, in practice, the authorization of recurring payments may put some merchants in violation of the PCI standards. In order to process a recurring payment, the merchant will need to retain at least the cardholder name and account number, expiration date, transaction amount and billing address. While it is allowable to retain this information, if properly secured, as indicated previously, the protection of this data can be arduous.

To illustrate the difficulty associated with the implementation of encryption, according to the 2005 CSI/FBI Computer Crime and Security Survey⁵, only 46% of the surveyed companies employed encryption for sensitive files. In many cases, companies are deterred from employing an encryption solution by the cost of implementation and the substantial increase in resources consumption (processing resources, bandwidth). By the time these costs are aggregated, companies are seemingly more willing to chance the security breach than to sustain such a large capital outlay. In the absence of encryption as a security measure, companies are left to implement compensating controls to protect sensitive cardholder data. Compensating controls are those procedures that are used when the ideal or prescribed technologies are impractical to implement. In these cases, the company may choose to implement a number of additional technical, logical and administrative controls in an attempt to afford the data as much protection as it would have if it were encrypted. The use of compensating controls, however, is generally accompanied by greater scrutiny during the course of any compliance assessment or audit and often does not result in a significant cost savings. Greater scrutiny can mean additional challenges convincing the certifying entity to approve the compensating controls and greater cost for the overall compliance project.

Requirement 3.3 requires merchants to mask the card when displayed and show only the first six or last four number of the account. This requirement is consistent with the Fair and Accurate Credit Transaction Act (FACT Act). The FACT Act was passed by the U.S. Congress in 2003 to address the need to ensure that credit reporting agencies “adopt reasonable procedures” to meet the needs of consumers with regard to the confidentiality and accuracy of their credit information. Section 113 of the FACT Act requires that no more than the last five digits of the account number be printed or displayed. Similarly, Requirement 3.4 requires that all cardholder data be rendered unreadable using one-way hashes, truncation, index tokens and PADs, or strong cryptography such as 3DES 128-bit or AES 256 bit.

Faced with all these challenges, the merchant is required to devote an enormous amount of resources to the protection of data, detracting attention from the business’ core competency. Shift4 has recognized this dilemma and has developed a solution that can address the need to retain cardholder data while simultaneously lightening the burden of PCI compliance.

⁴ MasterCard International. “Service Industry Incentive Program for Recurring Payments.” http://www.mastercardmerchant.com/build_business/incentive_program.html

⁵ Computer Security Institute. (2005) CSI/FBI Computer Crime and Security Survey. Available online at (http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml)

Tokenization

In light of the aforementioned difficulties in complying with industry and government regulations while storing sensitive data, companies are rightly concerned about the proper implementation of security controls. Of primary concern is the diversion of scarce resources from the company's core competency to the implementation and maintenance of complex security measures and maintaining compliance with varied legal and industry requirements. Ideally, companies would be able to retain the data they need for incremental authorizations without jeopardizing their compliant status or expending unnecessary resources on the protection of such data. In order to address the issues posed by the storage of sensitive data, Shift4 has developed a Tokenization process that will allow merchants to store the data that they need for incremental authorizations, reporting and reconciliation while easing the challenge of compliance.

Tokenization is a term used to describe the replacement of the card number used in transactions processing with a Token. The Token is a unique identifier comprised of a 16-character, alphanumeric code that is used to reference sensitive cardholder data. In keeping with PCI, as well as the legal requirements of the FACT Act, the Token contains only the last four digits of the card number. The last four digits of the account number become the first four in the Token. Spaces 5-16 are random characters that are globally unique to that transaction.

Much of the process of authorization and settlement remains unchanged. The only difference is that the response to the authorization request will return the described Token instead of the credit card number along with the approval, referral or decline. For example, the merchant will swipe the credit card and transmit the authorization request over Shift4's fully encrypted communication lines. Shift4 sends the request to the processor and receives the authorization

response. When the response is communicated back to the merchant, however, the card number is replaced with the Token. Minimal card information is included in the response; only the last four numbers of the credit card number.

For payment applications and merchants that use Shift4, only the Token has to be stored in the POS system. Each time a new transaction is sent concerning that invoice or card number, the Token will be updated. For example, a communication cycle might resemble the following:

Invoice/Folio 1: Authorization	
Request	Merchant Sends Card Data
Response	Shift4 Returns Token A
Invoice/Folio 1: Sale	
Request	Merchant Sends Token A
Response	Shift4 Returns Token A
Invoice/Folio 1: Return Credit	
Request	Merchant Sends Token A
Response	Shift4 Returns Token B

Tokenization and compliance

The only time the card number is used is in the initial authorization request. In all subsequent communications, the card is referenced using the Token. At the merchant level, the Token is stored in the POS terminal in place of the card number. If the merchant needs to communicate further regarding an invoice or folio, then any of the Tokens, Token A or B, could be used. When the merchant sends a request to Shift4, the Token is translated into the card number and sent to the processor. When the processor sends the response back to Shift4, the card number is converted into a new Token and then sent to the merchant. This allows the merchant to conduct incremental authorizations or recurring payments while keeping the storage of sensitive data to a minimum.

Tokenization is also easily implemented on the merchant system. There are some minor changes that must be implemented by the POS/PMS. For example, an addendum must be added asking for the Token information instead of the cardholder account number. The Token must also be stored, but this is easily accomplished, as well. Because the Token consists of 16 characters, it can be stored easily in the field that used to hold the cardholder number. The ease of implementation is further demonstrated by the fact that the change can be implemented even while there are open tickets and pending sales.

Shift4's Tokenization also addresses a major concern that faces most POS users when implementing any change to the system: the continuing functionality of reporting functions. The Token still contains the last four digits of the card number. The retention of that information means that most POS and PMS reports will remain fully functional. The implementation is entirely seamless to the merchant.

The implications and benefits of Tokenization on PCI compliance are myriad. First and foremost, the Tokenization

process addresses PCI Requirement 3: Protect Stored Data. In using the Tokenization process, the duty of protecting cardholder data is largely shifted from the merchant to the gateway. By returning only Tokens in response to merchant requests, Shift4 dramatically reduces the number of places in which cardholder information is stored on the merchant system. While some card information may still be stored in logs, the majority of the card data is stored on Shift4's systems, rather than on the merchant's system. Nor do merchants have the added concern of ensuring that the method of encryption used is of adequate strength and complexity. Additionally, since the merchant is not required to encrypt the Token, there are no encryption keys to manage. Following is a brief discussion of the ways in which Tokenization can minimize the challenges of compliance.

As stated earlier, PCI Requirement 3.1 requires businesses to keep storage of cardholder data to a minimum, limiting the type of information stored and the amount of time that it is retained. By using Tokenization, merchants are in fact reducing the amount of cardholder information they are retaining on their systems. Since the Tokens are viable for up to two years after its inception, merchants have no need to store the cardholder data for reporting or reconciliation purposes.

Requirement 3.4 mandates that all cardholder data is rendered unreadable using one of several forms of strong encryption. One of the methods suggested was 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. Further, by using the Token the merchant is not storing the card number. This lessens considerably the merchant's obligations under PCI requirements.

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 from Shift4, 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.

Tokenization also assists in complying with the notification laws of several states, including California and New York. The California law, also known as the Security Breach Notification Law, states that any company that loses unencrypted personal information must notify all individuals that may have been affected by the breach. New York has passed a similar law, and thirty-three other states are now considering such laws. If a merchant system is compromised and a Token disclosed, there is no way to link that Token to a particular individual. Following that logic, the unauthorized disclosure of the Token does not enable identity theft or financial fraud, which means that notification of the loss need not be made. It should be noted, however, that if the merchant is storing any unencrypted identifiable personal information (this may include social security number, drivers license number, account numbers and similar information) that is compromised, then notification is still required.

Tokenization can accomplish the same ends as encryption without the cost or work factor usually associated with the solution. Since the process is not encryption, there is no need to securely manage any encryption keys. The merchant also can rest assured that the cardholder data

is stored in Shift4's PCI compliant data center. Shift4, as a registered third party of the card associations, is required to validate compliance with PCI requirements on an annual basis.

It is important to understand, however, that while Tokenization considerably lessens the burden of compliance, it does not completely remove the obligation to comply with relevant industry requirements. Though Tokenization will make complying with PCI less complicated, its use is not a replacement for validating compliance. PCI compliance must still be validated to ensure that all information security practices are adhering to the requirements of the program. For example, Tokenization does not reduce the liability surrounding the protection of logs that may contain cardholder data. Logging is an essential part of maintaining network systems. Through logging, problems can be tracked and identified. The amount of data that is stored in the logs, however, can be problematic in relation to compliance. By turning on verbose logging, the logs capture an extreme amount of data, including sensitive information that must be protected. It is imperative that a great deal of thought is devoted to exactly the type of information that is captured by the logs. The merchant must work closely with the POS vendor to understand exactly what information is captured in the logs. If they capture sensitive data, then that must be afforded protections that are commensurate with the risk posed and with industry and government requirements.

Additionally, the use of Tokenization does not diminish the need to create and implement a robust information security program. The information security program, as required by PCI, must contain a plan to constantly identify new threats and vulnerabilities and to address those newly identified risks. Additionally, an important component

(both of PCI requirements and of an information security program) that is often overlooked is the education of employees. Security is a responsibility that falls to everyone within the organization. The implementation of Tokenization does not diminish the importance of security education for employees.

Conclusion

Compliance with information security regulations, both industry mandated and government imposed, has taken on ever-increasing importance in the daily business of companies in all industries. Through the implementation of Tokenization, merchants can ease their compliance process while taking proactive steps to protect the sensitive information with which their customers have entrusted them. Tokenization not only protects the customers' information; it removes liability from the merchant and places it on the gateway.

The elimination of magnetic stripe and authentication data from merchant systems will require the cooperation of all stakeholders in the industry, from the software developer to the merchant to the POS device manufacturer. Tokenization provides the ability to eliminate much of the sensitive data that is usually stored, thereby protecting customers and lessening the burden of compliance on both merchants and payment applications.

About the author

Dr. Heather Mark, Ph.D., CISSP specializes in regulatory compliance, privacy, and data security issues. She received her doctorate in Public Administration and Public Policy from Auburn University and is a Certified Information System Security Professional who frequently consults with companies within the payment services industry. Dr. Mark also writes a monthly article for Transaction World magazine on the topic of information security in the payments space.



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>