First Data™

A First Data White Paper

September 2009

Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance

Contents

Executive Summary

More than 280 million payment card records were breached in 2008 alone,[1] and a large percentage of those stolen records were used fraudulently. In fact, the underground economy is teeming with stolen payment card data.

Some controls are in place to help card payment processors prevent credit card fraud through increased controls around data and by limiting potential exposure to compromised information records. The Payment Card Industry Data Security Standards (PCI DSS), for example, are widely considered to be a worldwide set of best practices for securing sensitive data. PCI DSS procedures are an essential component in any merchant's holistic risk management program—but they are not without their burdens and limitations.

More than a billion dollars. That's how much money merchants have collectively spent on PCI DSS compliance as part of their security systems.[2] Indeed, PCI DSS compliance is a resource-intensive challenge to businesses of all sizes. According to the analyst firm Gartner, a Level 1 merchant (generally defined as a merchant that annually processes 6 million or more Visa® or MasterCard® transactions) might spend millions of dollars to initially meet the security requirements prescribed by the PCI Security Standards Council (PCI SSC). Even a Level 4 merchant (commonly defined as a merchant that annually processes less than 20,000 eCommerce or 1 million Visa or MasterCard transactions) might have to spend several thousand dollars on the initial security assessment and new technology and security measures.[3] And meeting the security requirements is just the start; maintaining PCI DSS compliance is a continuous process that requires constant vigilance and incurs ongoing costs.

Despite enormous efforts and vast expenditures since December 2004 when the security standards were first released, hundreds of millions of records with sensitive information have been breached. This clearly indicates that many merchants still have work to do to fully implement standard security procedures and technologies to thwart theft of cardholder data.

Data Encryption:

Algorithmic methods that encode plain text (such as a cardholder number) into a non-readable form called ciphertext.

In recent years, larger merchants have begun implementing data encryption as a way to protect cardholder data. Now there is a new component to data security beyond encryption that holds the promise of diminishing both a merchant's risk of a data breach and burden of PCI DSS compliance—and it's a viable solution for merchants of any size.

[1] Verizon, 2009 Data Breach Investigations Report, Verizon Business RISK Team, March 2009.
[2] Letter to Bob Russo of the PCI Security Standards Council from the National Retail Federation, et. al., June 9, 2009.
[3] Gartner, Inc., PCI Compliance Remains Challenging and Expensive, Avivah Litan, May 16, 2008.

This new element, called tokenization, replaces sensitive cardholder data with a randomized token that represents the cardholder data. Tokenization eliminates a merchant's storage of actual cardholder data. From a merchant's perspective, if the cardholder data is never stored, it's far less likely to be stolen. What's more, a large portion of a merchant's computer systems are removed from the scope of a PCI DSS compliance audit since those systems no longer process or store cardholder data.

Data encryption, when combined with tokenization, greatly improves cardholder data security. This paper describes these security techniques and helps merchants understand how and when they can be used to implement secure transaction management and reduce the burden of PCI DSS compliance.

For more detailed information about PCI DSS and protecting data, see First Data's white paper *PCI DSS and Handling Sensitive Cardholder Data—Why You Care* on the First Data Web site at www.FirstData.com. Additionally, the full PCI DSS specifications can be found at www.PCISecurityStandards.org.

A Daunting Challenge: Protecting Cardholder Data While Maintaining PCI DSS Compliance and Minimizing Expenses

Data breaches are reaching epidemic proportions

The company that ignores industry best practices for data security is putting itself at risk of a costly data breach that, among other consequences, can greatly harm its brand. For example, the IT Compliance Group reports that companies that suffered the loss or theft of sensitive data have financial outcomes that include an average of 8.1 percent customer defections, 8.0 percent revenue decline, and 8.0 percent decline in stock price.[4] Research conducted on behalf of Visa reveals that three out of four consumers won't shop again at a compromised merchant.[5]

From 2002 through 2008, the forensic investigators of the Verizon Business RISK Team conducted more than 600 investigations of breaches or suspected breaches of all types of data in all types of industries. The team's 2009 Data Breach Investigations Report reveals the following:[6]

- → 2008 was a record year for number of records compromised: 285 million. Just three industries—Retail, Financial Services, and Food and Beverage—accounted for three-quarters of the 2008 breaches. Most of the records, 99.9 percent, were compromised from servers and applications.
- → As a percentage of caseload for the Verizon Business RISK Team, payment card breaches remain near the 80 percent mark and far outnumber the other data types. They consume 98 percent of all records compromised in 2008.

[4] IT Policy Compliance Group, *Core Competencies for Protecting Sensitive Data*, October 2007.
[5] PCI-portal.com, *Why is the PCI DSS important?*, http://www.pci-portal.com/lang-en/pci-knowledge/pci-dss-overview/importance-of-pci-dss.
[6] Verizon, *2009 Data Breach Investigations Report*, Verizon Business RISK Team, March 2009.

- → Fraudulent use of stolen card data was confirmed in 83 percent of Verizon's cases. Ninety-one percent of all compromised records were linked to organized criminal groups.
- → Eighty-one percent of organizations suffering payment card breaches within the Verizon caseload were found not compliant with PCI DSS or had never been audited. This status was determined by the victims' attestations or Qualified Security Assessors (QSAs).
- → In 66 percent of the cases, the breach involved data that the organization didn't even know was on the system.

Clearly, serious threats from data breaches still exist, despite the billions of dollars that merchants have already spent toward improving cardholder data security. Why is protecting data so difficult? This is more than a rhetorical question; companies ask this question every day and find there are numerous answers.

One reason cardholder data is hard to protect is that it is so desirable to criminals; they will do almost anything to get this data, and for good reason. Security vendor Symantec's research reveals that cardholder information can be easily sold in the underground economy, sometimes for as much as $25 per record. In fact, credit card information represents the highest percentage of goods available for sale in the black market, as well as the top category of "product" requested by buyers in this illicit economy.

With so much money at stake, cybercriminals are devising ever more sophisticated methods to access the data they desire. Bryan Sartin, managing principal of Verizon Business Investigative Response, says the nature of the criminal attacks he has investigated over the years is changing. "Cybercriminals have become much more sophisticated in the last decade," according to Sartin. "At first we saw directed attacks against specific companies that processed lots of sensitive data—banks, ATM operators, data processing companies. Then we observed a shift toward fully random attacks using botnets, SQL injections, authentication bypass and scans for vulnerabilities. Just recently, the criminals have shifted techniques again to pursue softer targets, like data in transit or in the computer's running memory because it's not encrypted."

A high level of sophistication isn't always required, however. Sometimes all it takes is a simple vulnerability to create the opportunity a cyberthief needs. A review of two of the most damaging data breaches ever in the retail space shows that simple exploits worked effectively to let the thieves siphon nearly 100 million payment card records from just two companies:

[7] Symantec, Report on the Underground Economy July 07–June 08, Fossi, et. al., November 2008
[8] Network World, *Don't Be a Data Loss Victim*, Linda Musthaler, February 9, 2009

Breach/Date Reported	Known or Suspected Contributing Factors
International Discount Retailer January 2007	The company had an outdated wireless security encryption system and failed to install firewalls and data encryption on the computers using the wireless network. Thieves accessed the streaming data between hand-held price-checking devices, cash registers and the stores' computers. All told, approximately 94 million credit and debit accounts were compromised.
U.S. Supermarket Chain March 2008	Malware[9] was surreptitiously installed on the servers of almost 300 stores. When customers swiped their cards, the malware intercepted the data as it was being transmitted from the stores' POS systems to authorize transactions. The malware then forwarded the stolen card numbers and their expiration dates to an overseas destination. As many as 4.2 million credit and debit card numbers were stolen.

Figure 1: Contributing factors to recent major breaches
Sources: DataLoss DB – http://datalossdb.org and Privacy Rights Clearinghouse – http://www.privacyrights.org

PCI DSS compliance is a stringent and expensive process—but necessary

The very reason that PCI DSS exists is to provide detailed guidance to merchants on how best to protect cardholder data. The goal is to prevent breaches of cardholder data that can have far-reaching ramifications not only for the merchant, but also for the cardholders whose data was compromised; for the card issuers, banks and financial institutions that may be required to absorb losses from the incident; and for shareholders affected by a drop in stock value.

Nevertheless, protecting cardholder data proves to be the biggest challenge for many merchants. One of the top reasons a merchant is most likely to fail a PCI DSS audit—and a leading factor in data theft—is the failure to adequately protect stored data. VeriSign Global Security Consulting Services, a division of security services vendor VeriSign, has conducted hundreds of PCI DSS assessments in recent years. Of the merchant companies assessed by VeriSign, 79 percent were cited for the failure to protect stored data—and thus failed their assessments.[10]

The PCI DSS requirements have a tremendous impact on the information technology systems utilized by every company in the card processing ecosystem. Compliance efforts have forced merchants to update existing systems and implement new hardware and software in order to segment networks, install firewalls, deploy data encryption technologies, implement data access controls, track and monitor access to data and networks, and much more.

[9] The use of malware such as keystroke loggers and "phone home" applications increased by 400 percent in 2008, according to security technology firm McAfee, Inc.
[10] VeriSign Global Security Consulting Services, *Lessons Learned: Top Reasons for PCI Audit Failure and How To Avoid Them*, 2007, p. 4.

The implementation and ongoing maintenance of the needed technology measures is expensive, and it continues to grow more expensive with time. According to a 2008 survey by Gartner Inc., Level 1 retailers reported spending an average of $2.7 million on PCI DSS compliance, excluding the costs of PCI DSS assessment services. That number compares with an average of $568,000 reported by Level 1 merchants in a fall 2006 Gartner survey. Also, Level 2 merchants (those that annually process from 1 million to 6 million Visa or MasterCard transactions) reported spending $1.1 million on PCI DSS compliance, as opposed to an average spending of $267,000 reported in the fall of 2006. Altogether, Level 1 and Level 2 U.S. merchants' spending to protect cardholder data and become PCI DSS compliant increased nearly fivefold during the past 18 months, according to the Gartner report.[11]

Further complicating the matter, merchants are required to demonstrate on an ongoing basis that they have the proper controls in place to protect the data. The demonstrations—whose costs are borne by the merchants—are done through self-assessments, network scans and/or regular audits performed by third-party assessors. For Level 1 and Level 2 merchants, the scope and cost of an audit can be huge. Even many Level 3 and Level 4 merchants find the time and financial commitments to their PCI DSS assessments to be onerous for the size of their businesses.

Despite the expenditures to date, as well as the implementation of many beneficial security technologies, many merchants are still struggling with PCI DSS and are coming to realize that the cost of PCI DSS compliance is vastly underestimated.

> The PCI DSS requirements have a tremendous impact on the information technology systems utilized by every company in the card processing ecosystem.

Given the cost and difficulties of attaining and maintaining PCI DSS compliance, the obvious question is, "Why bother?" After all, PCI DSS compliance is not mandated by any law or government regulation (with the exception of the new PCI DSS requirement in the State of Nevada). Rather, compliance is a contractual obligation. Nevertheless, a merchant's failure to comply with PCI DSS—in other words, a breach of contract—can result in monetary fines and/or the loss of the privilege to accept payment cards. Since few merchants are willing to forgo accepting customer-preferred third-party payment cards, there seems to be little choice but to make a serious commitment to comply with the PCI DSS standard.

The Aberdeen Group reports the companies that are rated as "best in class" in PCI DSS compliance follow the security standards in order to protect the organization and its brand.[12] These progressive companies view PCI DSS not merely as an obligation but as an opportunity to develop processes and capabilities that improve their business performance in multiple areas; for example, a holistic view of risk management.

[11] Gartner, Inc., *PCI Compliance Remains Challenging and Expensive*, Avivah Litan, May 16, 2008.
[12] Aberdeen Group, *PCI DSS and Protecting Cardholder Data: Year-over-Year Progress in Achieving, and Sustaining, Compliance*, June 2008.

Data is vulnerable at all points in card processing

The PCI Security Standards Council points out that merchant-based vulnerabilities may appear almost anywhere in the card processing ecosystem. This includes point-of-sale (POS) devices, PCs or servers, wireless hot spots, Web-based shopping applications, paper-based storage systems and the unsecured transmission of cardholder data to service providers. Vulnerabilities also can extend to outside systems operated by service providers. These vulnerabilities can, and often do, lead to the exposure or theft of sensitive cardholder data, especially at the merchant level.

Sensitive data is vulnerable

In transit – When data is moving from one device, application or system to another—such as when cardholder data is being sent from the POS endpoint device to the POS server—it can be surreptitiously copied and sent to a computer controlled by a thief. This is precisely what happened in the U.S. supermarket chain data breach noted previously in this paper. Millions of cardholder data records were siphoned off before anyone noticed the problem.

- **At rest** – Data often must be stored somewhere for later use, or for archival purposes. Whether the storage medium is online (such as a file server) or offline (such as a file cabinet), the data is vulnerable to accidental exposure or loss and to intentional theft. For example, in September 2007, a U.S. sporting goods retailer reported that a computer containing the credit card information for customers who shopped at a specific store between July 2002 and June 2007 was lost or stolen. On the computer were 112,000 credit card numbers and 10,000 transaction records.[13]
- **In use** – Many organizations use cardholder data for purposes other than simply authorizing a transaction. For instance, the marketing department may use the data to create or support marketing programs, such as loyalty rewards. Or the data may be analyzed for loss-prevention purposes. In some instances, the data may be replicated or used in ways in which the company isn't even aware. Unfortunately, when sensitive data is used in multiple applications, it is especially vulnerable to loss or theft.

These three states—in transit, at rest and in use—cover the full spectrum of the life of sensitive data. PCI DSS provides guidelines to help merchants understand how to protect or limit the exposure of the data in all of these states.

Every part of the computer network that touches or uses cardholder data in these three states is known as the "cardholder data environment" (CDE). This includes the POS devices and applications; storage devices where the data is stored, temporarily or permanently; applications that use the data, as well as the servers that process those applications; the network components like routers and switches that help transmit and route the data; backup media such as tapes; and any other parts of the network that allow access to the aforementioned resources. It's easy to see how the CDE can grow to be quite extensive, especially if a merchant uses cardholder data for purposes beyond simply authorizing transactions.

One of the biggest challenges organizations face is reducing the size of their CDE (cardholder data environment) and isolating it from the larger corporate network. Effectively doing so significantly minimizes data breach opportunities and streamlines the annual PCI DSS assessment process.

[13] Source: The Breach Blog, www.breachblog.com.

The entire CDE is subject to fraud and data breaches. For this reason, the entire CDE is subject to PCI DSS compliance. This is why the requirements are so costly for merchants; and it's not a one-time revamp. First, merchants need to implement and maintain the security measures to come into compliance with PCI DSS. Then the merchants must submit to quarterly and annual assessments to substantiate compliance. A Level 1 merchant can easily spend millions of dollars on both efforts with little return on the investment. Even a small retail establishment with only a few thousand card transactions a year is forced to spend thousands of dollars on security measures and validation.

Merchants of all sizes are looking for ways to reduce the risks of data violation, along with the time and financial burdens of PCI DSS compliance. Reducing the scope of the CDE is a prime way to do so. By allowing fewer computing resources to have access to real cardholder data, merchants can minimize the opportunities for fraud and limit spend on both security and annual PCI DSS assessments. The rest of this document explains how emerging technologies can address this issue.

Emerging Solutions for Improving Cardholder Data Security

Protecting stored cardholder data is essential for businesses, and PCI DSS compliance will continue to be a challenge for many retailers in 2010. Now, two important security methods are coming to market to help secure sensitive cardholder data from thieves as close to the initiation of the transaction as possible. Both methods specifically address the complex requirement to secure in-transit data and stored data; one of the methods even addresses the concerns of using sensitive data in business applications. Here's an overview of the two methods, including how they might be used, along with their benefits and drawbacks.

Encryption of sensitive data

Probably the single most important measure that merchants can take to protect cardholder information is to encrypt it as soon as the data, including the primary account data (PAN) and all track data, is captured and leave it in an encrypted state while it is transmitted to the payment processor. This is sometimes referred to as end-to-end encryption. This step means the transaction is never transmitted in plain text in the frame relay, dial-up or Internet connection, where the potential exists for interception by fraudsters. If the data does get siphoned off once it is encrypted, it is virtually useless to thieves.

> "End-to-end encryption may well be the end-game recommendation of PCI and, if data breaches continue to plague the payments industry and occupy headlines, that recommendation may become a mandate within two years."
>
> George Peabody,
> Principal Analyst,
> Mercator Advisory Group

Encryption refers to algorithmic schemes that encode plain text (such as a cardholder number) into a non-readable form called ciphertext, thus providing privacy for the encrypted data. One or more "keys" are required to decrypt the data and return it to its original plain text format. The key—which thieves would not possess—is the trigger mechanism to the algorithm.

To be most effective, data encryption should take place at the POS terminal application, immediately after the magnetic-stripe reader (MSR) obtains the card data track. While numerous Level 1 merchants have already enabled this capability, most other merchants have not. If data is not encrypted at the point of capture, it is vulnerable as it is transmitted in plain text to the POS server or the merchant's central server. (This is what is believed to have happened in the highly publicized data breaches involving a U.S. supermarket chain, an international discount retailer and a U.S. restaurant chain.)

Getting even closer to the origination of the data, there are proponents in the industry for encrypting sensitive data at the MSR rather than in the POS application. This can be accomplished through the use of specific hardware within the POS. However, detractors feel that the incremental benefit of replacing POS hardware to enable encryption at the time of MSR does not offset the added expense of replacing hardware. To date, few merchants have implemented this solution.

Encryption can also safeguard data in a card-not-present (CNP) scenario. The data can be encrypted as soon as it is entered into the payment application and prior to being submitted for approval of the transaction. This can be further enhanced by leveraging third-party-hosted payment pages, eliminating the need for the CNP merchant to touch the card data at all.

Taking the value of encryption a step further, a merchant should send its transactions to the payment processor for approval in an encrypted form using industry standard, laboratory-tested algorithms. Using a key, the processor can decrypt the transaction and continue to process it as usual with the bank associations and networks. It is important to note that many encryption algorithms exist that are public or proprietary, and the resulting encryption will be only as effective as the industry testing and validation of such algorithms. Proprietary algorithms do not go through necessary crypto-analysis scrutiny from industry experts, and one should be cautious when these untested algorithms are the basis of the encryption method used.

Once encrypted, the data can be safely stored on a merchant's POS server or host computer for the purpose of end-of-day reconciliation and other internal uses if needed.

The processes of encrypting data immediately after capture and transmitting it to the payment processor in encrypted form provide great risk reduction. Even if a thief is able to intercept the data in transit, it will be in a format that is both unreadable and unusable to him. George Peabody, principal analyst with the Mercator Advisory Group, says it's all about the money. "Remove the economic benefit of hacking into a merchant or processing network and financially motivated criminals will move onto something else. Make PANning for gold a fruitless exercise and you will minimize the damage when a breach does occur. By making the card data on the merchant network unusable and keeping all stored data on a third-party's systems, the merchant is able to protect its customers' data, ensure its reputation for proper care and control of that data, and reduce PCI scope."[14]

End-to-end encryption is not currently a requirement in PCI DSS. However, according to Peabody, "End-to-end encryption may well be the end-game recommendation of PCI and, if data breaches continue to plague the payments industry and occupy headlines, that recommendation may become a mandate within two years." [15]

[14] Mercator Advisory Group, *End-to-End Encryption: The Acquiring Side Responds to Data Loss and PCI Compliance*, George Peabody, June 2009, p. 11.
[15] Mercator Advisory Group, *Merchant Security, Tokenization and the Fairy Tale of Outsourcing PCI*, George Peabody, March 2009, p. 4.

The advantages and disadvantages of encryption

As with any security solution, there are advantages and disadvantages to the approach. On the positive side, encryption is a common technique that has proven to be very reliable over many years. That's not to say that encryption can't be broken; however, it takes a sophisticated thief to know how to penetrate an encryption algorithm to defeat it. What's more, encryption technology continues to advance, making it far harder for someone to "crack the code."

Data encryption satisfies the PCI DSS requirement of protecting stored data. As deemed in a PCI DSS assessment, a merchant whose data at rest or in transit is adequately protected via encryption can feel confident in meeting those particular PCI DSS compliance requirements. What's more, end-to-end encryption offers the benefit of limiting the scope of PCI DSS compliance and shifting more responsibility to the processing community, thus lowering the cost of compliance for the merchant. The chart below looks at three scenarios in which Level I merchants have the potential to save money through PCI DSS compliance scope reduction using encryption. The "scope reduction" percentages are estimates provided by the Mercator Advisory Group.

Scenario	Cost	Scope Reduction	Savings
Scenario 1 – Low			
Annual compliance assessment by QSA (qualified security assessor)	$250,000	25%	$62,500
Compliance maintenance	$1,000,000	20%	$200,000
		Annual Savings	***$262,500***
Scenario 2 – Moderate			
Annual compliance assessment by QSA	$1,500,000	25%	$375,000
Compliance maintenance	$3,000,000	20%	$600,000
		Annual Savings	***$975,000***
Scenario 1 – High			
Annual compliance assessment by QSA	$3,000,000	25%	$750,000
Compliance maintenance	$5,000,000	20%	$1,000,000
		Annual Savings	***$1,750,000***

Figure 2: Sample PCI DSS compliance savings through use of end-to-end encryption[16]

Encryption is a technology that can be utilized by an individual merchant; it doesn't require sweeping changes in the payment processing ecosystem that would take years and cost billions to bring about. The technology is available today, it is proven to be effective, and many merchants already use it to protect customer data.

On the negative side, data encryption can be an expensive and resource-intensive proposition. For Level 1 and Level 2 merchants, deploying encryption accounts for a significant portion of the hardware and software costs needed to be initially compliant with PCI DSS. Level 3 and Level 4 merchants left to implement encryption on their own may simply find encryption too expensive and difficult. Deployment may require the upgrade or replacement of POS terminal devices and changes to the POS application. Merchants may find it necessary to hire a consultant to help with the implementation. Moreover, since there are numerous encryption techniques and technologies, merchants may be forced to adopt a specific implementation based on what their payment processor accepts. This situation could create a feeling of "vendor lock-in" and make it difficult to switch payment processors in the future.

[16] Mercator Advisory Group, *End-to-End Encryption: The Acquiring Side Responds to Data Loss and PCI Compliance*, George Peabody, June 2009.

One of the other aspects of an encryption solution that is often overlooked is that of key management. With an encryption solution, card data is still present within a merchant's system, protected by encryption. The security of the keys used to perform that encryption is just as vital as securing the data itself. The use of symmetric encryption algorithms (where the same key can be used to encrypt and decrypt data) by most solutions requires vigilant protection of keys, lest they be compromised. "Identity based" key derivation may remove some of the manual management of keys, but does not remove the risk of key theft or compromise. Poor key management practices risk the compromise of the data, or potential data loss if keys are "lost."

Despite the cost and complexity of encryption, it's a valuable tool for merchants of all sizes. Dennis Fisher is the executive editor of the security information Web site SearchSecurity.com. In a column where he discusses the data breach of a specific international discount retailer, Fisher justifies the expense of data encryption technologies and the time spent managing them. He writes, "Companies complain that database encryption products are cumbersome, expensive and difficult to manage. Really? You know what else is expensive and difficult to manage? A data theft. It's bad enough that attackers are able to get inside the perimeters of the companies, but they certainly shouldn't be able to find any unencrypted customer records once they get there. The same goes for government agencies. Just do it."[17]

Tokenization of sensitive data

An increasingly popular approach for the protection of sensitive data is the use of a token (or alias) as a substitute for a real credit card number. In the process of tokenization, a payment card is used in a transaction and, once authorized, the cardholder data is sent to a centralized and highly secure server called a "vault," where it is stored securely. Immediately after, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The end result is that the token can be used in various business applications as a reliable substitute for the real card data.

Tokenization has the ability to enhance the protection of sensitive data by offering a token-based data substitution value for plain-text-sensitive data elements. In other words, instead of maintaining ciphertext and an associated key (ID) within the merchant's data stores, a single token is stored and used as a pointer to the encrypted value in the vault. A credit card number, for example, is replaced within the merchant's storage environment by a token value generated in such a way that it cannot be linked back to the original data element. A secure cross-reference table is established to allow authorized lookup of the original value, using the token as the index. Encryption tools and secure key management complements this approach by protecting the original value within this environment. To anyone who doesn't have authorization to access the vault, the token value is totally meaningless; it's just random characters.

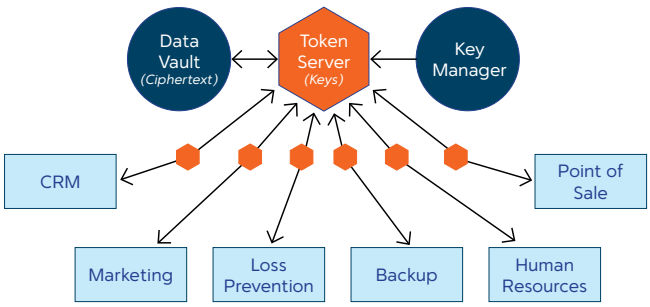


Figure 3: How tokenization data security works

[17] SearchSecurity.com, *TJX breach: There's no excuse to skip data encryption*, Dennis Fisher, January 2007.

From a security perspective, tokenization significantly reduces risk based on the fact that sensitive data can't be breached if it's not there in the first place. At a time when cardholder data loss is at an all-time high, this is an extremely interesting prospect for many organizations. Tokenization is even appealing to Level 1 merchants who have previously passed their PCI DSS audits. Those merchants who have full encryption solutions are investigating how the addition of tokenization can benefit them, as well.

A handful of Level 1 merchants have already adopted tokenization. However, the concept is fairly new, so a more detailed discussion of how it works in a typical payment transaction environment is warranted. Here's a simplified step-by-step view of how the transaction authorization process works, incorporating a token solution. In this scenario, the payment processor is also the token service provider. However, the token service can be implemented in-house or delivered by a neutral third-party provider.

Step	Transaction Authorization Process with Tokenization
1	A customer initiates a transaction by providing his cardholder number. This can be via a swipe of the card, a contactless reading of the card or a CNP data entry.
2	The merchant captures and encrypts the card data. The card data needs to be encrypted only at the POS for the point in time where it can be transmitted to the payment processor.
3	The merchant transmits the encrypted card data to the payment processor.
4	The processor decrypts the data and sends it via a secure channel to the appropriate network or association for authorization. As a function of the authorization process, the payment processor generates a new token or retrieves an existing token that matches this card data.
5	When the transaction is authorized for payment, it gets sent back to the payment processor.
6	The payment processor replaces the card number with the token and sends the outbound transaction response to the merchant. There is no sensitive data going back to the merchant.
7	The merchant receives the transaction authorization, permanently deletes the encrypted card number and retains the token in its place. The merchant can store the token for settlement, reconciliation, chargebacks and other purposes. If the tokens are intercepted or stolen, they have no value to the thief, since they cannot be used to initiate a financial transaction at the point of sale.

Figure 4: How tokenization fits into transaction processing

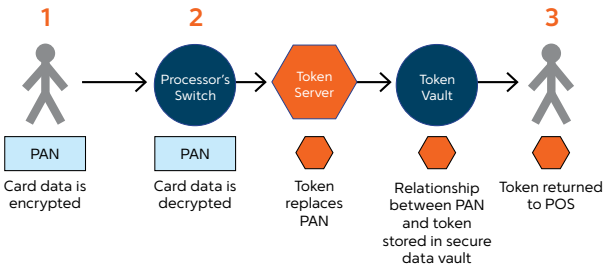


Figure 5: Integrated encryption and tokenization process

1 The full customer data, including the primary account number (PAN) and all track data, is entered into the POS system, where it is encrypted.

2 The encrypted data is sent to the processor's switch and decrypted. The decrypted PAN is then sent to a token server, where the token replaces the PAN and the relationship of PAN to token is stored in a secure token data vault.

3 The token is returned to the point of sale and all of the customer data, with the token replacing the PAN, is sent to other systems, such as settlement applications, as needed.

The processes of encrypting data immediately after capture and transmitting it to the payment processor in encrypted form provide great risk reduction. Even if a thief is able to intercept the data in transit, it will be in a format that is both unreadable and unusable to him. The merchant applications no longer require the real PANs, but the processor retains the data in the secure token vault storing the relationship of PAN to token in the event it is needed in the future.

Tokens can be reused for recurring payments, too, making them ideal for "payment wallet" scenarios. For example, suppose a customer gives his credit card information to an online merchant for a purchase today and the customer also chooses to allow the merchant to store the card for the customer's future purchases (i.e., the payment wallet). The merchant replaces the customer's credit card number with a token. The next time the customer makes a purchase, the token stored in the wallet acts as an index pointer to the actual credit card number, which the merchant's token service provider would keep on file. If someone hacks the merchant's servers and steals the wallet data, the thief would simply get a bunch of tokens that have no meaning to him, since a token can be used only to initiate a financial transaction through an authorized merchant account.

The advantages and disadvantages of tokenization

From a PCI DSS compliance perspective, tokenization has powerful implications for merchants, banks and service providers. As discussed at length by organizations attending the 2008 PCI Community meetings, one of the biggest challenges organizations face is reducing the size of their cardholder data environment (CDE) and isolating it from the larger corporate network. Effectively doing so significantly streamlines the annual assessment process. By ensuring that business applications, systems and infrastructure are processing randomly generated numbers instead of regulated cardholder information, organizations can drastically reduce the controls, processes and procedures needed to comply with PCI DSS. This is particularly true if tokenization is provided to merchants as a service from a third party that maintains ownership of the secure cross-reference table.

For example, consider PCI DSS compliance as a spectrum. On one end, there are more than 200 detailed requirements with which merchants must comply. On the other end, there are far fewer requirements, mostly because the specifications for the PCI DSS requirement to protect stored data have been removed. The number of PCI DSS requirements merchants must contend with is predicated as to whether and how each merchant processes, transmits and stores the cardholder data. By using tokenization to replace sensitive stored data, merchants move their businesses toward the "fewer requirements" end of the PCI DSS spectrum. Merchants eliminate a large technology and administrative burden, saving money in the long run.

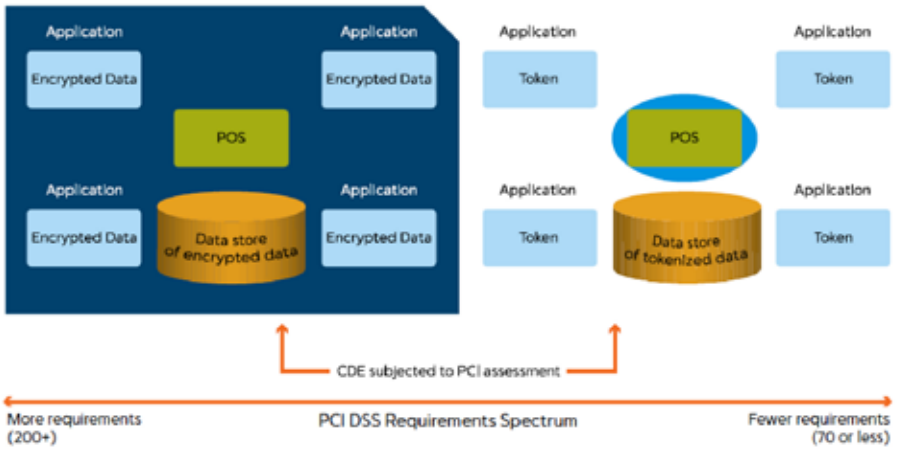


Figure 6: CDE scope reduction through the use of tokenization

In shifting the data breach risk from merchants to a third-party token provider, merchants don't need to spend unnecessary time and money building extra security into their transaction systems. Some security measures will still be needed, of course, such as in the POS device and application. However, merchants can focus on growing the business instead of worrying about stored cardholder data because there is none on the merchants' systems.

Meanwhile, the token provider now is the keeper of the cardholder data for many merchants. Some critics of tokenization say the token provider represents a single point of failure; if this company is breached, the cardholder data from hundreds or thousands of merchants can be compromised. True, but a trusted and reputable token provider should have sufficient resources and expertise to build and maintain strong security in its systems—just as major payment processors do today. What's more, if the token service provider is breached, this company generally assumes liability for the problem.

One more merchant benefit is protection of the merchant brand in the market. If internal risk of data exposure is significantly reduced, and most of the liability for safeguarding cardholder data has shifted to a third party, the organization has taken great strides to protect its brand. It will not become the next company in the headlines accused of carelessly handling its customers' sensitive data.

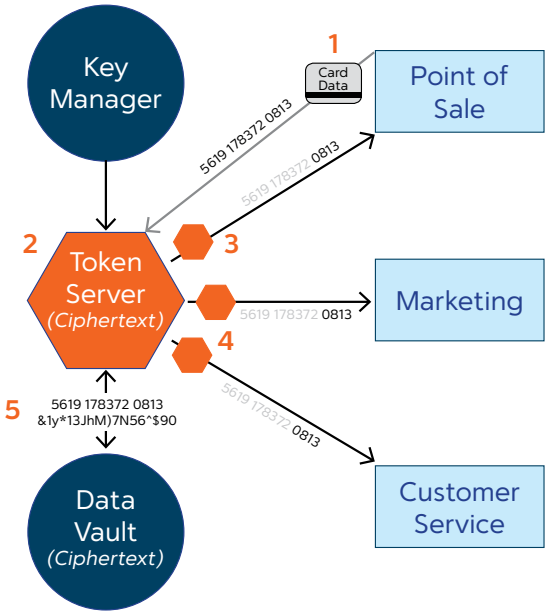
There are some drawbacks to tokenization. For instance, it is a relatively new application of technology. While there are successes in the marketplace, there are no long-term implementations that provide a sufficient history of how well the technique performs. Furthermore, there's a lack of trust in the various small, independent vendors who have brought tokenization solutions to market. It's not that their solutions aren't good; it's simply that they are unproven over time. Many organizations feel the stakes are too high to trust their most sensitive data to a newcomer in the data security or payment processing market.

Some larger merchants have a resistance to outsourcing data security to a third party. They believe there is an increased business risk in giving access to the organization's most sensitive data to an outside company. Of course, outsourcing a data security measure such as tokenization is a catch-22 situation. A company can forgo tokenization altogether or implement it completely in-house with an in-sourced solution. In this case, the company assumes all responsibility (and liability) for data security. Or, the organization can outsource the measure to a third-party provider, thus trusting the outsourcer with the sensitive data while also lessening the liability burden. The company must decide for itself which risk is more acceptable.

> "By making the card data on the merchant network unusable and keeping all stored data on a third-party's systems, the merchant is able to protect its customers' data, ensure its reputation for proper care and control of that data and reduce PCI scope."
>
> George Peabody,
> Principal Analyst,
> Mercator Advisory Group

Many merchants have already made significant investments in data encryption for their cardholder data. This begs the question, "If we encrypt our data, why would we also need to tokenize it?" The primary answer here is to reduce the scope of the PCI DSS requirements the organization must satisfy. Remember the spectrum discussed earlier. While encrypting data is a valid security measure, it doesn't significantly reduce the requirements the company must meet because the cardholder data is still present—albeit encrypted, but it's still there. By complementing data encryption with tokenization, merchants remove sensitive card data from their applications and storage systems. This effectively reduces the cardholder data environment and subsequently reduces the cost and extent of the quarterly scans and the annual PCI DSS assessments.

Large organizations may use cardholder information in business applications such as MIS reporting, marketing, return processing, sales auditing, loss prevention and loyalty programs. They may be concerned about replacing the actual card data with a representative token for these applications. As long as the token is format-preserving—in other words, it uses the same number and format of characters as the original cardholder data—the token can be safely used by any application throughout the organization without extensive modification to those applications. Any further concerns can be overcome by how tokenization is implemented. There are two different models of tokenization: dynamic and static. The dynamic model creates a new token for a card transaction every time the card is used to make a purchase. The static model reuses an existing token that has been assigned to the card every time the card is used. If the static model is implemented, the merchant can maintain the functions supported by storing cardholder data. The static model represents a one-to-one relationship for life between the token and the PAN. Both models achieve the goal of reducing the burden placed on the merchant through the PCI DSS requirement to "protect stored data."



1 A purchase is made and the card data is sent to token server

2 The card number is tokenized, preserving the last four digits

3 The token is returned to the POS for storage with other transactional information (i.e., items, name)

4 The token is sent to other business systems

5 The card information is encrypted when tokenized, and ciphertext is stored in the data vault

Figure 7: How tokenized data can be used in other applications

The cost equation of tokenization

Since tokenization is such a new method for protecting cardholder data, a brief discussion about the cost equation is warranted. Proponents of the solution assert that tokenization is a means for merchants to reduce overall costs associated with cardholder security and PCI DSS compliance. How can this be, if new processes and technology must be implemented? How can adding more security end up costing less?

Merchants will find there are new costs associated with implementing a tokenization solution. Depending on the solution chosen, there may be application integration work to ensure that tokens work with their POS and their internal systems. For example, the token will only slightly resemble a cardholder number—perhaps maintaining only the last four characters of the real cardholder number in the last four characters of the token. Modifying the number returned to the POS in the authorized response may require new edits within the POS. Additionally, a company that currently stores cardholder data in a database will need to reprogram the database to store tokens instead. The impacts will vary by merchant depending on the uses of their databases.

The merchant's token service provider will have a fee for its service. Since tokenization is a relatively new service, the providers are still assessing their cost models. At the time of this writing, many service providers seem to charge a small fee per transaction, with the fee being on a sliding scale based on the volume of transactions from a specific merchant.

Offsetting these new charges, however, is the reduction in costs to implement, verify and sustain PCI DSS compliance measures—in other words, shifting on the compliance spectrum toward fewer requirements and a smaller audit/assessment scope. The Mercator Advisory Group reports that a large merchant can spend upward of $100,000 per application or process to make an application or a process PCI DSS compliant. The annual PCI DSS audit costs for such a merchant can range from $20,000 to hundreds of thousands of dollars, depending on the merchant size, POS terminal estate size and the range of applications using cardholder data.[18]

With tokenization, some of these applications are removed from the scope of PCI DSS compliance and the ensuing annual audits. Mercator states that one large merchant reported $2 million annual savings by moving to an outsourced tokenization solution after it had already become PCI DSS compliant.[19]

The Mercator report concludes, "The truth is that tokenization's short-term benefits accrue to the merchant and its PCI compliance burden. The reduction in scope of the audit and the security-monitoring posture taken by the merchant are welcome improvement and the results are worthwhile."[20]

[18] Mercator Advisory Group, Merchant Security, *Tokenization and the Fairy Tale of Outsourcing PCI*, George Peabody, March 2009.
[19] Ibid.
[20] Ibid.

Considerations for Enhancing Your Transaction Security Strategy

Both encryption and tokenization offer the means to vastly improve merchants' cardholder data security and their PCI DSS compliance posture. Merchants can view these two technologies as a two-level approach to increasing security for payment transaction processing.

Start with encryption

For all merchants, data encryption is the minimum base level of recommended security. The data should be encrypted as soon as it is captured and left in an encrypted state for transmission to the payment processor to minimize the likelihood that useful data can be intercepted when it is in transit between the POS terminal and POS server, or the POS dial-up terminal and the acquirer or payment processor.

This level of encryption should not require the complex management of keys. However, merchants should coordinate the encryption strategy with their acquirer or payment processor to ensure the encrypted data sent from the merchant can be decrypted properly by the payment processor in order to complete the authorization process.

Data encryption alone (i.e., without tokenization) may be sufficient for those merchants whose POS does not store the card data after submission of the authorization, or who don't have external data stores of transaction data.

Bolster encryption with tokenization

Merchants whose POS does hold onto or store the card number after the submission of the authorization, or who do have data stores of transaction data for MIS and/or return processing, should implement both encryption and tokenization. The data should be encrypted as soon as it is captured and left in an encrypted state for transmission to the payment processor. In this scenario, too, merchants should coordinate the encryption strategy and security keys with their payment processor to ensure that the encrypted data can be decrypted properly in order to complete the authorization process.

When merchants receive the token in the authorization response from the payment processor, they should delete all instances of the cardholder data and store the token instead. Business applications throughout the organization can safely use the token without fear of data exposure and without expanding the cardholder data environment and the scope of the PCI DSS assessment. In fact, the very act of replacing cardholder data—encrypted or not—with tokens shrinks the CDE and greatly eases the burden of the PCI DSS assessment.

Key considerations when selecting a solution provider

The technologies and processes for secure transactions discussed above require a partnership with one or more solutions providers. For example, the way to reap the main benefits of tokenization—the reduced scope of the PCI DSS implementation, assessment and maintenance—is to outsource the token service to a third party, thus relinquishing the responsibility of storing and securing sensitive data. Here are some key considerations when selecting a solution provider.

- → **Uptime/reliability of the service** – Merchants shouldn't risk their business with a service that isn't available when they need it. Even a few minutes of service downtime make it impossible for merchants to transact sales. A reputable solution provider should guarantee uptime with a Service Level Agreement contract and back up the agreement with proof of redundant systems. That is, if any part of the solution fails for any reason, there is an immediate (and unnoticeable to the merchants) cutover to a secondary computer component, system or facility. This ensures no disruption to the merchants' businesses.
- → **National Institute of Standards and Technology (NIST)**-certified forms of encryption – It is critical to use an algorithm that has been certified through industry testing and validation. Vetting of encryption algorithms is a process that normally takes years, and the skills required are generally found only in academic or governmental settings. Note that many public or proprietary encryption algorithms have not been through the necessary crypto-analysis scrutiny from industry experts, and the resulting encryption will be only as effective as the encryption algorithm.
- → **Token creation through strong random number generation** – Predicting tokens produced from strong random number generators is nearly impossible. These secure, non-reproducible sources of true random numbers are designed to generate a sequence of numbers that lack any pattern, virtually ensuring that each token is sufficiently spontaneous and not projectable by fraudsters.
- → **Technical specifications of the solution** – Any solution for encryption and/or tokenization is going to be sophisticated. However, some technologies are far superior to others. For example, there are numerous types of encryption. Some require only one key to encrypt and decrypt the data, while others require two keys, one to encrypt and one to decrypt. Some keys are dynamic (constantly changing) while others are static. Any encrypted data that is stolen is better protected if the keys are dynamic or if separate keys are required to unlock it. In selecting a solution provider for security services, it's important to get the details about the technical specifications and compare them to other solutions on the market.
- → **Seamless integration with existing POS system** – Merchants already have a significant investment in their POS systems. "Rip and replace" is not an attractive option. Therefore, any new data security measures will need to integrate with what is already in place. Still, there are differing definitions of "integration." When selecting a solution provider, merchants should feel comfortable that the vendor can orchestrate a seamless integration between the POS and the security systems, with no disruption to business.
- → **Pricing model** – Merchants already spend a lot of money on data security. It's an unavoidable expense to reduce business risk. Additional security measures such as encryption and tokenization aren't free; however, they can offset other costs such as the dollars spent on lengthy PCI DSS assessments and remediation efforts, or worse yet, a breach. A security solution provider's pricing model should be compatible with a merchant's business; for example, a minimal upfront outlay to implement the new solution, with reasonable per-use service fees over time.

- → **Track record** – There is a reason many merchants are hesitant to outsource security: it's hard to let go of something that can make or break a business. That's why a service provider's track record of avoiding system failures, data breaches and other lapses in delivery of the contracted service is a critical selection criterion.
- → **Level of risk/responsibility assumed by the solution provider** – Hand in hand with the service provider's track record is the company's willingness to assume certain business risks and responsibilities if a failure should occur. If the service provider truly is at fault for an incident, the merchant should not be held accountable for the results of the breach; for example, fraud due to stolen cardholder data.

The above criteria may actually be a "wish list," but the issues are certainly worth bringing up for discussion with any potential solution provider.

Conclusion

PCI DSS compliance is growing more burdensome every year. As new threats to data security emerge, businesses are forced to apply more security techniques to attempt to stay a step ahead of cybercriminals and to plug newly identified vulnerabilities. The cost to attain, maintain and verify PCI DSS compliance is skyrocketing. Thus, all businesses in the card payments ecosystem have a vested interest in implementing long-term enhancements to data security and reducing the scope of the cardholder data environment.

Data encryption and data tokenization are two emerging technologies that show great promise in the race to secure transaction processing systems and applications. Many Level 1 merchants are already enjoying the benefits of encrypting their cardholder data, and a few merchants have initiated data tokenization projects. Used as a one-two punch complement to each other, these two technologies can be especially effective at lowering the cost of PCI DSS compliance and validation by reducing the scope of the cardholder data environment.

Merchants aren't expected to do this alone. The end-to-end card payment process includes many players—acquirers, ISOs, payment processors, card networks, etc. Merchants can look to these players to assist with cardholder data security, and in the process, help reduce the burden of PCI DSS compliance.

First Data brings a wealth of PCI DSS knowledge to the table, along with a range of solutions that help keep data safe, meet the requirements of PCI DSS, help save money and support merchants' critical business processes. First Data encourages all merchants to learn more about PCI DSS compliance, and to develop and implement a strategy to reduce and protect the cardholder data environment—or the ramifications of a breach could become a reality.

A Powerful Combination: First Data and RSA and Encryption and Tokenization

They are leaders in their respective industries: First Data—a global leader in electronic commerce and payment processing services—and RSA, the Security Division of EMC—the premier provider of information-centric security solutions to guard the integrity and confidentiality of information.

And they've teamed up to provide a layered data security solution. The new First Data® Secure Transaction Management℠ service leverages encryption and tokenization technology from EMC's security division to reduce risk and cost associated with card data and PCI DSS compliance. The solution enables merchants to secure payment card data and remove it from their environment while allowing access when needed. The First Data® Secure Transaction Management℠ service, offered exclusively by First Data and powered by RSA SafeProxy™, helps to reduce organizational risk and ease the process of complying with the PCI DSS.

For more information about the First Data® Secure Transaction Management℠ solution, please see your First Data Sales Representative or visit FirstData.com.

First Data™

The Global Leader in Electronic Commerce

First Data powers the global economy by making it easy, fast and secure for people and businesses around the world to buy goods and services using virtually any form of payment. Serving millions of merchant locations and thousands of card issuers, we have the expertise and insight to help you accelerate your business. Put our intelligence to work for you.

For more information, contact your
First Data Sales Representative
or visit firstdata.com.