Utilizing Tokenization
How to minimize the impact of the payment card industry data security standards (PCI DSS) on SAP® applications
# Table of Contents

Introduction .............................................................................................................. 3

The PCI DSS ................................................................................................................ 3

The Challenges with PCI Requirement 3 ................................................................. 4

The Challenges of Encryption ................................................................................... 5

The Mandate: Keep Cardholder Data Storage to a Minimum ............................... 6

A Best-in-Class Approach to Securing Cardholder Data for Heterogeneous SAP Environments – Remove It ................................................................. 7

Benefits of Tokenizing Cardholder Data ................................................................. 8

How A Tokenization Service Approach Compares with Traditional Encryption Approaches .......................................................... 10

An Introduction to XiSecure On-demand ................................................................. 12

Benefits of XiSecure On-demand ............................................................................ 13

Conclusion .................................................................................................................. 13

About Paymetric ....................................................................................................... 14
Introduction

Electronic payment acceptance is a mainstay of the 21st century. Even B2B companies that traditionally have extended payment terms to their customers and used paper-based invoicing methods now look to leverage electronic payments as a way to accelerate time to cash, offer their clients expanded payment options and open new channels of revenue. Adoption of electronic payment acceptance among organizations conducting B2B commerce will continue to grow exponentially and so will the responsibility and risk associated with it.

Thieves have become increasingly interested in getting their hands on sensitive information, such as cardholder data, because they can sell it for a hefty price tag. Over the past decade, the number of data security breaches has grown and identity theft and fraud have become more and more prevalent. It is for that reason that regulatory bodies, including federal and state governments, have paid increasing attention to mandating sound data security practices. Organizations that accept electronic payments are ultimately responsible for protecting their customers’ sensitive information from falling into the wrong hands.

PCI DSS

Prior to 2004, each card brand had a unique security program that merchants were required to adhere to. These included: Visa’s Card Information Security Program, MasterCard’s Site Data Protection, American Express’s Data Security Operating Policy, Discover’s Information and Compliance and the JCB Data Security Program. These five card brands realized it was confusing for merchants to comply with multiple regulations and decided to develop a uniform security standard called the Payment Card Industry Data Security Standard (PCI DSS), released in December 2004.

In 2006, the Payment Card Industry Security Standard Council (PCI SSC) was formed as a joint venture between American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa. The PCI SSC’s goal is to facilitate the broad adoption of consistent data security measures and is responsible for the development, management, education and awareness of the PCI Security Standards including the PCI DSS.

PCI DSS is a set of constantly evolving requirements intended to help organizations proactively protect customer account data. Any organization that processes, stores or transmits cardholder data is required to comply with PCI DSS. That means even if you process a single transaction, you must be PCI compliant.

The standard is organized into six governing principles that contain a total of twelve requirements. Figure 1 illustrates these requirements.
Figure 1: The Payment Card Industry Data Security Standards

<table>
<thead>
<tr>
<th>Principle</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and card data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security</td>
</tr>
</tbody>
</table>

All PCI DSS eligible organizations are required to certify their compliance on an annual basis, but that doesn’t mean merchants should think about PCI DSS simply as a point-in-time validation. Compliance with PCI DSS should become part of a company’s overall security strategy and requires constant attention. Many companies that have experienced a breach have validated compliance at an earlier point in time, but at the time of the incident were found to be out of compliance. While companies may have, in fact, been compliant during a breach, that doesn’t mean compliance guarantees protection from a breach. It is, however, in the opinion of Paymetric’s experts, a sound guideline for ensuring the security of your customer’s sensitive data and should be taken seriously.

The Challenges with PCI Requirement 3

With the advent of PCI DSS, securing stored cardholder data is no longer optional. Any company that stores, processes or transmits credit card information – regardless of the volume of transactions – must secure stored credit card data or face serious consequences for non-compliance, including fines of up to $500,000 per incident, the loss of brand integrity, erosion of market value and loss of merchant processing privileges.

While the PCI standard offers broad guidance – featuring rules on the proper use of firewalls, computer access controls, antivirus software and more – it is the requirement for securing stored cardholder data that is proving to be one of the more difficult for organizations to address. “18.2% of organizations suffering a breach had Requirement 3 in place and 32.7% of companies passed Requirement 3. This suggests some correlation between not having strong data protection methods in place and suffering a data breach.”

1http://www.verizonenterprise.com/pcireport/2014/
What does Requirement 3 state, and why is it so challenging? Titled “Protect Stored Cardholder Data,” this requirement focuses on all the aspects essential to ensuring that stored payment data remains secure. PCI DSS Requirement 3 applies to any system in which cardholder data is stored, including applications, databases, backup tapes and portable digital media.

**Requirement 3 includes these mandates:**
- Minimize the amount of credit card information stored
- Encrypt credit card data that remains stored
- Protect encryption keys against both disclosure and misuse
- Implement sound key management processes
- Rotate encryption keys annually

### The Challenges of Encryption

While most security professionals recognize the merits of encrypting credit card data, they may struggle with limitations in SAP. The SAP Cryptographic Library (SAPCRYPTOLIB) functionality offers a starting point for native encryption logic in SAP. Basis administrators can download the library relevant to their operating system and configure SAP to encrypt credit card data. SAP notes 766703 and 1032588 answer frequently asked questions about credit card number encryption logic in SAP. Security professionals must address the encryption limitations in native SAP as enumerated below.

**Tables:** Encryption functionality in SAP ERP secures payment card number data a limited number of tables, notably: two tables related to storage of card numbers on customer master records, VCKUN and VCNUM; a third table related to storage of card numbers on sales orders and invoices, FPLTC; and a fourth table related to storage of card numbers on accounting documents, BSEGC. This targeted coverage in these four tables, as well as several others, leaves card number data in other standard SAP tables and in custom tables unencrypted and exposed.

**Algorithms:** Three encryption algorithms are made available by SAP and they may not meet the PCI DSS definition of strong cryptography due to the inability to verify the actual algorithm being utilized.

**Flexibility:** SAP’s offering supports only a software-based cryptography, leaving no possibility to use hardware-based cryptography components that are fast becoming the standard because of their additional security benefits.

**No Pre-defined Integration Point:** For organizations interested in integration of best-of-breed, third-party encryption solutions, SAP provides no single, predefined point of integration. The CCNUM domain is not the only domain with which credit card numbers will be associated, so multiple integration points will be required.

---

**Figure 2:** Selected Section 3 Requirements Addressable by Tokenization

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.0</td>
<td>Encryption is a critical component of cardholder data protection</td>
</tr>
<tr>
<td>3.1</td>
<td>Keep cardholder data storage to a minimum</td>
</tr>
<tr>
<td>3.4</td>
<td>Render account number unreadable through strong cryptography and associated key management</td>
</tr>
<tr>
<td>3.5</td>
<td>Restrict access to keys to the fewest number of custodians necessary</td>
</tr>
<tr>
<td>3.5.2</td>
<td>Store keys securely in the fewest possible locations and forms</td>
</tr>
<tr>
<td>3.6</td>
<td>Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data</td>
</tr>
<tr>
<td>3.6.4</td>
<td>Periodic changing of keys, at least annually</td>
</tr>
</tbody>
</table>
Downtime for Key Rotation: SAP stores encryption keys locally in .pse files. This presents a significant challenge to meeting the annual key rotation requirement found in PCI Section 3.6.4. Until the release of enhancement package 4, in order to rotate encryption keys, SAP must be taken offline so each credit card number can be manually unencrypted with the old key and re-encrypted with the new key. Order-entry and billing processes must be discontinued during this time to avoid storing credit card numbers in clear text, or to avoid failed authorization and settlement requests resulting from mismatched keys.

Increased SAP Exposure: When utilizing native SAP encryption, the SAP system will always be in scope for a PCI audit because the encrypted cardholder data is stored in the SAP database.

The Mandate: Keep Cardholder Data Storage to a Minimum

The challenges presented in the prior section are significant for SAP organizations. For those that also store credit card numbers in other systems outside of SAP, the challenge to securely storing sensitive data grows exponentially more imposing.

Requirement 3.1 of the PCI standard advises that organizations, “Keep cardholder data storage to a minimum.” To do so, organizations must first identify precisely where all payment data is stored. While this may seem simple, for many large enterprises it is anything but. In fact, for a large enterprise the data discovery process can take months of staff time to complete.

While Requirement 3.1 of PCI speaks to common sense – that is, don’t keep sensitive data where it’s not required – the reality for many organizations is that retention of cardholder data in multiple locations is critical to a host of business processes. For most business-to-business transactions, payment card numbers are required throughout the entire order-to-cash process. In addition, most retailers require the data for returns, disputes and fraud protection.

For these organizations the reality is that credit card data must be stored in many separate and distributed systems, making the encryption requirements of PCI Requirement 3.1 onerous and expensive. It’s a simple equation: the more repositories that house payment card information, the more points of exposure and the higher the cost of encryption and PCI compliance.

But what if there was an alternative for these organizations? What if there was a way to take PCI Requirement 3.1 a step further, and remove credit card numbers from all of an organization’s systems, while at the same time enabling all essential business processes to continue as needed? Some organizations have done this very thing – by adopting a best-in-class approach to cardholder data security called tokenization. The following section offers an overview of this approach, outlining how it works, some of its benefits, how it compares to traditional encryption methods and more.
A Best-in-Class Approach to Securing Cardholder Data for Heterogeneous SAP Environments – Remove It

Today, there’s a new approach to securing cardholder data that offers an array of benefits, both in terms of security and ease of administration. Tokenization is a solution that affords organizations the opportunity to eliminate the storage and/or transmission of cardholder data in enterprise systems and applications. Implementing tokenization can make achieving PCI compliance much easier than replacing an existing application with a PA-DSS-compliant one, according to a Verizon Business Report.²

When tokenization is delivered on-demand, it is extremely affordable when compared to the investment businesses would have to make in costly encryption solutions. According to a Gartner research study, more than 25 percent of Gartner clients have already adopted payment card tokenization to reduce the scope of their PCI assessments, and three out of four clients calling about PCI inquire about tokenization.³

Tokenization works by taking cardholder data entered into enterprise systems or applications and replacing it with a surrogate value known as a token. A token is a unique ID created to reference the original data. The original data is encrypted and stored off-site in a secure data vault with reference to the token. The merchant no longer possesses sensitive cardholder data and the token can be passed throughout the enterprise to meet the demands of customer interactions and support analytics without disruption of day-to-day business activities. In the event of a data security breach, tokens can’t be reverse engineered to retrieve the original number, and are thus useless to thieves.

²Verizon 2014 PCI Compliance Report
³“Choosing a Tokenization Vendor for PCI Compliance,” Gartner—Avivah Litan

---

Figure 3: Before Tokenization
If a tokenization solution is not utilized, merchants are forced to deploy costly encryption solutions to protect stored cardholder data. Encryption and key management technology must be implemented on each internal system where the card numbers are stored. As the data passes between system components, it must go through the dreaded, encrypt, de-crypt, re-encrypt process because keys cannot be shared between systems. This method exposes the raw card number in transit, thereby increasing risk. When companies utilize encryption, their systems remain in scope for PCI Requirement 3, which is a more costly and time-consuming scenario. This also means that the company is still storing cardholder data even though it is encrypted. Because encryption technology is key-based, if a breach were to occur it is feasible that the attacker could get access to each and every payment card number stored in that system. Not only would that be costly to deal with, but also it would be extremely damaging to an organization’s brand. The bottom line is encryption solutions still leave systems vulnerable to attack.

Benefits of Tokenizing Cardholder Data

By implementing this tokenization approach, companies can realize a range of benefits, including a reduced impact of PCI on SAP systems, improved security, optimized application integration and performance and also simplified administration.

Reduced Impact of PCI Compliance

By removing stored credit card numbers from enterprise systems and storing them in an off-site data vault, your company no longer bears the full weight of the PCI requirements. In particular, with the proper implementation of tokenization and data intercept technologies, the SAP system may be out of scope for PCI Requirement 3 and could reduce the burden of a PCI audit.

Figure 4: After Tokenization

With tokenization deployed, sensitive cardholder data is neither transmitted nor stored. Tokens can be easily passed from one system to another, never exposing raw card numbers in transit. Because you only store tokens, the risk of a data security breach is greatly reduced, saving you time and money.
Improved Security
By tokenizing data, organizations gain these security benefits:

- **Minimized exposure of data**: As mentioned above, PCI Requirement 3.1 requires that organizations keep payment data in a minimum number of locations. This approach addresses the requirement fully. Eliminating potential targets for hackers immediately strengthens security. Thieves can’t steal what a company doesn’t have.

- **Segregation of card data from applications**: Unsecured data never resides in SAP or other applications. SAP users never see payment data in clear text; they will only be able to see the token.

- **Impact of breach limited**: With this approach, if an attacker somehow bypasses both the token and encryption, they will have access to only one card number. In contrast, with many encryption solutions, if an attacker gains access to one cryptographic key, they can potentially decrypt thousands or even hundreds of thousands of records.

Optimized SAP Performance and Availability
Through employing an tokenization solution, organizations can enjoy a range of advantages in integration and performance:

- **Improved application processing**: Tokens can be passed between SAP and other applications without requiring any encryption or decryption, thus securing the data “on-the-wire” at system integration points. Further, SAP is freed from having to do resource-intensive cryptographic processing. This can significantly streamline transactions across the enterprise.

- **Optimized application availability**: Full key rotation is handled externally, which will eliminate any SAP downtime otherwise required.

- **Static tokens**: Tokens maintain a one-to-one relationship with the original card number and can be used for reporting and analytics. Multi-use tokens will not be affected if there are any changes to the source system.

Simplified Administration
Tokenization significantly eases the administrative burden of securing cardholder data, offering a range of advantages:

- **Minimized compliance requirements**: By removing payment data from disparate repositories or multiple application databases and storing that data outside of the SAP system, the cost of certifying PCI compliance is drastically reduced. It is no longer necessary to worry about implementing encryption, managing keys and implementing policies on multiple systems.

- **Elimination of key management**: All encryption keys and policies are managed off-site, as opposed to having keys in multiple, distributed locations. This takes the burden of key rotation off the merchant and removes the burden of PCI-required tasks, such as key revocation and rotation, and shifts that burden to the tokenization service provider.

- **Centralized log management**: With a tokenization solution, administrators gain one centralized location that contains information on all decryption requests, which significantly eases compliance audits as well as surveillance and remediation efforts.

> “From the world’s largest corporations to small Internet stores, compliance with the PCI DSS is vital for all merchants who accept credit cards, online or offline, because nothing is more important than keeping your customers’ payment card data secure.”
> – PCI Security Standards Council
How A Tokenization Service Approach Compares with Traditional Encryption Approaches

Many security professionals have either deployed or are familiar with such traditional approaches as application encryption and database encryption. How does tokenization compare to these traditional approaches? The following is an overview of the differences, and how these solutions can work in concert together.

Application Encryption

Application encryption is an approach in which encryption and decryption of the data takes place within the SAP application. The data is encrypted or decrypted by SAP every time it is written to or retrieved from the database. As a result, the data residing on the database is always encrypted.

Once an organization has deployed a tokenization service, however, SAP no longer directly participates in any cryptographic operations. The SAP application relies on the external token server to manage cryptographic operations and key management processes. This means the SAP application does not require local cryptographic technology and so is spared the management and performance issues associated with encryption.

With this approach, an external server issues a token to replace the credit card number in SAP. A benefit of this approach is that there is no need to encrypt or decrypt at every step in the SAP workflow, such as for payment processing or researching disputed transactions. The token becomes a surrogate for the credit card number itself and may even be exchanged with other applications in the enterprise as if it was a real credit card number – without the overhead of decryption and re-encryption, or the risk of exposure. Also, by replacing the card number with a token into the standard SAP Credit Card Number Database Table field, there is no additional database space required.

Database Encryption

Database encryption is an approach to encrypting data at rest in which encryption and decryption is handled at the SAP database server level, rather than at the application level. The data to be protected is encrypted every time it passes from the application to the database. Likewise, as data is requested from the SAP database, it is decrypted before being returned to the application. The data is only in an encrypted state when it's at rest in the database. Application processing happens independently of encryption and decryption, with all data stored unencrypted in the SAP application's memory.

When a tokenization service is deployed, however, SAP interfaces it as described in the previous section. The SAP database no longer requires local cryptography and key management, with all intelligence for encryption outsourced and contained within the off-site tokenization server. Again, this centralized tokenization server interfaces with other databases and applications by issuing a token to be used in place of the credit card number.

This approach offers significant benefits over traditional database encryption. First, exposure to unencrypted credit card numbers is removed from the SAP application and database at all times, which boosts security. Secondly, cryptographic processing is completely removed from SAP servers, which enhances application and database performance.
Implementation Requirements
To implement this new tokenization service approach for heterogeneous SAP environments, an organization must be able to build integration utilizing one of two methods depending on the source application.

SAP interface: A tokenization server must have the capability to extract the credit card number when it enters SAP in the normal business workflow and then replace it with a token. This will require a custom remote function call (RFC) that enables an interface between SAP and the tokenization service when the credit card number is entered in SAP. Integration can be enabled without any changes to standard SAP code and objects via the use of several userexits for securing specific table fields or a Domain or Search Help object can be enhanced to provide a more ubiquitous integration across multiple tables.

Non-SAP interface: For most other applications, a Web Services interface will be required that provides a similar integration as the SAP RFC.

Hurdles to Developing Your Own Tokenization Management Server
Developing all the capabilities outlined above can present significant challenges if a security team seeks to build a solution in-house. The following are a few of the biggest hurdles an internal team could face in this endeavor:

Developing application interfaces: Developing a custom RFC for SAP or a Web Services interface may require unique expertise and consume significant internal time and resources. Consideration must be made for how this interface will affect business workflow, SAP tables and overall application performance.

Developing token applications: Writing an application that is capable of issuing and managing tokens in heterogeneous environments and that can support multiple field-length requirements is complex and challenging. Further, ongoing support of this application could be time consuming and difficult.

Development time: Allocating dedicated resources to this large undertaking and covering for responsibilities this staff would otherwise be fulfilling could present logistical, tactical and budgetary challenges.

Development expertise: For many organizations, locating the in-house expertise to develop and maintain such complex capabilities as key management, token management, policy controls and heterogeneous application integration can be very difficult.

Accommodating new algorithms: Over time, an organization’s security needs change. Likewise, the cryptographic algorithms or encryption mechanisms in use may also require changes. Once initial development has been done, the development team may need to add capabilities for integration with a new protocol or encryption solution, which may entail a substantial rewrite of the application in use.

According to Gartner Group, the cost to roll out encryption solutions is $6 per customer record. For a company with 100,000 records, that means they would spend $600,000.
Minimizing impact on application performance: Writing code that interferes with multiple interfaces and multiple applications, while minimizing the performance impact on those applications, presents an array of challenges.

Maintaining software upgrades and updates: The overhead of maintaining and enhancing a security product of this complexity can ultimately represent a major resource investment and a distraction from an organization’s core focus and expertise. These challenges are significant and can severely undermine the value of an encryption management server. For security administrators looking to gain the benefits of tokenization, without having to develop and support their own tokenization server, Paymetric offers an off-the-shelf solution called XiSecure® On-demand.

An Introduction to XiSecure On-demand

XiSecure On-demand is Paymetric’s breakthrough solution for tokenizing credit card data across an enterprise. XiSecure On-demand works exactly as described in this document: it removes credit card numbers from distributed business applications, replaces them with tokens and stores the encrypted card numbers in an off-site, highly secure data vault in the cloud.

XiSecure On-demand Offers All the Following Critical Capabilities:

- Pre-built interfaces to SAP products
- Native Web Service interface
- Removes stored credit card numbers from enterprise application databases
- Replaces credit card numbers in enterprise applications with tokens
- Stores encrypted card numbers in an off-site, secure data vault in the cloud
- Provides key management processes outside of enterprise applications, thus eliminating system and application downtime
- Provides key rotation capabilities outside of enterprise payment acceptance systems eliminating maintenance downtime
- Provides access logging for decryption requests
- Provides monitoring of decryption requests
- 24X7 operation is supported via high availability mechanisms such as load balancing and database clustering
- Integrated back-up included in the service
- A disaster recovery site provides recovery from total-site outages
Benefits of XiSecure On-Demand

Reduced Scope and Cost of a PCI DSS Audit
All systems, applications and processes that have access to raw or encrypted credit card numbers are considered “in scope” for a PCI DSS audit. However, substituting tokens for credit card numbers within the systems, applications and processes will render the data useless and will eliminate the need to access to the token’s underlying value internally. The credit card numbers are not stored on-site and those merchant systems (where raw card numbers are never entered or displayed) may be considered “out of scope” for PCI audits.

Accelerate Time to PCI Compliance
With Paymetric’s SaaS (Software-as-a-Service) platform, organizations can quickly and easily deploy the XiSecure On-demand solution, resulting in a decrease in time spent to achieve and maintain compliance with the PCI DSS requirements.

Increase Security and Protect Your brand
With Paymetric’s tokenization solution, XiSecure On-demand, card numbers are never stored anywhere in internal systems, making it impossible for hackers to reassemble them through decryption or reverse engineering. This increased security allows companies to preserve their brand without the worry of unexpected fees, fines or legal costs associated with a data breach.

Works in Any Enterprise Payment Acceptance System
With XiSecure On-demand, cardholder data can be tokenized from anywhere payments originate within enterprise systems such as SAP or other ERP and CRM systems, legacy application, POS, order entry systems, web stores and call centers. With Paymetric’s XiSecure On-demand solution, you can take comfort in the fact that all of your systems are safe.

Conclusion
Securing cardholder data is one of the most important components of the PCI DSS, but it is also one of the more difficult requirements to successfully comply with. Traditional encryption can be used to address PCI Requirement 3, but it is costly and can still leave your systems vulnerable during an attack. Tokenization is a best-in-class security solution that removes cardholder data from your enterprise systems and applications. Since sensitive data is no longer stored in these systems, the cost and scope of PCI compliance is greatly reduced and the risk of a data security breach is drastically minimized. Hundreds of SAP customers have implemented Paymetric’s XiSecure On-demand solution and are experiencing all of these great benefits today.
About Paymetric

Paymetric, Inc. is the standard in secure, integrated payments. Our innovative payment acceptance solutions expedite and secure the order-to-cash process, improve ePayment acceptance rates, and reduce the scope and financial burden of PCI compliance. Leading global brands rely on Paymetric for the only fully integrated, processor-agnostic tokenization solution, supported by dedicated customer service. Paymetric is a nationally award-winning industry leader recognized for continual innovation, SAP partnership and world-class support since 1998. For more information, visit paymetric.com.

©2014 Paymetric, Inc. All rights reserved. The names of third parties and their products referred to herein may be trademarks or registered trademarks of such third parties. All information provided herein is provided "AS-IS" without any warranty.