



Passing the PCI Audit:

Best Practices for Securing Payment
Card Data in SAP® Environments

February 2012

The Payment Card Industry now requires onsite security audits for all large companies and many medium-sized ones.

Executive Summary

To combat the growing problem of payment card fraud, the major payment card brands worldwide established a standard for protecting cardholder data from theft: the Payment Card Industry (PCI) Data Security Standard (DSS). The DSS outlines best practices that merchant companies must employ if they store, process, or transmit sensitive payment card information such as the card number. Companies who fail to meet these standards face potential fines of \$50,000, \$100,000, or more.

To enforce these best practices, the Payment Card Industry Security Standards Council (PCI-SSC) requires onsite security audits for all large companies and many medium-sized ones. Smaller companies that process fewer than 20,000 e-commerce transactions a year) can validate compliance with the standard using a detailed self-assessment questionnaire, though they must still adhere to best practices. Unfortunately, a large number of companies are failing their audits. The most common reason: the failure to properly encrypt stored data.

Many companies who rely solely on their business solution's native encryption for compliance do not realize that their approach may not satisfy current PCI requirements. This white paper helps companies who use SAP solutions understand where an external encryption solution may be necessary to protect cardholder data, and *required* in order to satisfy the mandatory PCI security audits. The paper also addresses certain other key components of the PCI directive, common issues that lead to audit problems, and the strengths and weaknesses of three types of encryption methods available: SAP native encryption; external encryption which uses the SAP environment for data storage (here called "*encryption in SAP*"); and external encryption using tokens stored in SAP (here called "*tokens in SAP*").

Introduction

It's no secret that payment card theft worldwide is prevalent, expensive, and growing.

The Identity Theft Resource Center (<http://www.idtheftcenter.org/>) compiled reports of more than 22.8 million records compromised in the United States in 2011. This number is 28% higher than the approximately 16.1 million records reported compromised in 2010... and these are only the *reported* breaches. According to Network World (<http://www.networkworld.com/>) the cost of a corporate data breach is now \$7.2 million in 2011 which is an increase from \$6.8 million reported in 2010.

The Payment Card Industry brands foresaw the need to protect cardholder data from the growing threat of theft and began taking decisive action. Visa pioneered the way with its Cardholder Information Security Program (CISP) in September 2000, initially chartered to help build customer confidence in the e-commerce channel. Subsequently, Visa, Mastercard, American Express, Discover, and JCB joined forces to organize the PCI Security Standards Council. The Council is responsible for the development, management, education, and awareness of the PCI Security Standards, a set of best practices to secure cardholder data and unite the card brands' requirements into a consistent standard.

All companies that store, transmit, or process credit card data are responsible for securing the data, and the penalties for failure to do so are high... starting at \$50,000 for the first offense and rising from there.

The group's latest update, the PCI Data Security Standard (DSS) 2.0, published in October 2010, outlines the latest thinking in best practices for security management, policies, procedures, network architecture, software design and other critical protective measures. All bank members and clearing houses for all of the major credit cards must adhere to the DSS, which offers a unified approach to safeguarding sensitive payment card data. Merchant companies must also comply with the DSS, which ensures that all participants in the payment chain are on the same security protocol.

To ensure that the best practices in the Data Security Standard are followed, the acquiring banks require mandatory onsite security audits by a PCI-SSC Qualified Security Assessor (QSA) for companies who store cardholder data and process large volumes of transactions. Failure to satisfy an audit carries potentially heavy penalties. For example, Visa's CISP program, which enforces the requirements outlined in the unified PCI DSS, assesses substantial fees for failure to comply: \$50,000 for the first violation, \$100,000 for the second violation, and third violation fees levied by management discretion. MasterCard has also toughened its stance on PCI compliance, updating merchant compliance plans and penalties for Level 1 and Level 2 merchants.

As the Payment Card Industry continues to shift the obligation of data protection from banks to the merchants who store the data, the costs of an onsite QSA audit are increasing. According to Network World (<http://www.networkworld.com/>) merchants that undergo audits are paying an average of \$225,000 – \$500,000 annually to the QSA to ensure compliance with the PCI DSS. These estimates do not include operating expenses, or the cost of the technology and staff required to address audit issues. And while requirements for onsite audits are less strict for smaller companies, they too must validate adherence to the DSS by completing a detailed self-assessment questionnaire.

Unfortunately, many organizations are unaware of the necessity of passing the PCI audits, much less the scope of the requirements that must be fulfilled to comply with the PCI DSS.

Summary of PCI DSS Requirements

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications

Implement Strong Access Control Measures

7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data

Regularly Monitor and Test Networks

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Read the full standard at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

Unfortunately, many organizations are unaware of the necessity of passing the PCI audits, much less the requirements that must be fulfilled.

PCI DSS and SAP Environments: The Key Issues

The PCI Data Security Standard applies to every company that stores, processes, or transmits payment card numbers. The DSS outlines a holistic set of requirements designed to protect data against threats of all kinds. Companies must demonstrate that they have secure firewalls, anti-virus protection, access control for systems that house or process sensitive data, and finally, protection for the card data itself.

Complying with some of these requirements can be challenging, particularly requirement 3: *Protect stored cardholder data*. Auditors report that this requirement is the one most frequently failed.

So what does protecting stored cardholder data really mean for companies? First and foremost, your business applications are not permitted to store cardholder data “in the clear.” *The card number must be strongly encrypted in mass storage, in databases, on hard drives and on backup media*. In cases where the database is considered vulnerable, a token strategy of card number replacements must be implemented. For either encrypted values or token values, at least parts of the card number must be hidden, or masked, so that the actual card number is not displayed. With these security measures in place, even if unauthorized or malicious parties gain access to the data, the format makes it unusable.

Several solutions have arisen to provide basic encryption for SAP environments, but *many fall short in other areas*. Thus, companies fail the QSA audits. The following crucial encryption steps frequently present compliance issues for enterprise solutions:

- The encryption must use a recognized industrial-level algorithm such as AES or Triple DES.
- Encryption capability must be separate from the enterprise application. Personnel with business application access should be different than those with access to the encryption system.
- Generation and management of the keys used in encryption must also be separate from the business application.
- A demonstrable and practical key rollover strategy is required to ensure timely and secure updates of encryption keys.
- If data is to be stored in an unsecured database, tokens must replace encrypted values in the database.

Companies that want unqualified, clean security audits must find a proven solution that addresses all of the PCI requirements for encryption. The next section talks about various types of encryption available for SAP environments and how they hold up under the scrutiny of a PCI-DSS QSA audit.

An Auditor's Advice

Visa has stated that the primary source of data breaches in the retail sector is non-compliant card processing software, a truth that applies to B2B and e-commerce transactions as well. To ignore PCI best practices is to open your company up to serious risk and potential card theft!

We look for software that properly encrypts cardholder data, protects the key management process and rolls the keys over without card data in the clear. Make sure your card-processing software meets PCI standards for Payment Application Best Practices (PABP), and beware any application that does not offer strong cardholder encryption!

— Greg Johnson,
SecurityMetrics

Types of Encryption to Secure Data in SAP Environments

Several different types of encryption are currently available to secure data in SAP environments:

- SAP native encryption
- Use an external encryption server that encrypts the data outside of SAP and stores data in the SAP database (*encryption in SAP*)
- Use an external encryption server that replaces card data in SAP with tokens that reference encrypted values stored in an external database (*tokens in SAP*)

To provide additional security, specialized hardware encryption modules are often used in conjunction with the latter two methods. The rest of this section describes each of these encryption types in more detail. Once companies understand the structure of each method, they should choose the one that best fits their goals and budget.

SAP Native Encryption

In 2005, SAP introduced native capability to encrypt payment card numbers. This native encryption is the simplest way to encrypt the card number, because it's built-in and no external systems need to be installed. The encryption itself is reasonably strong and well-designed. However, because the encryption remains within SAP, it creates *scope* problems during a QSA audit, meaning that more SAP functions need to satisfy the security standards. More functions being audited means a more expensive audit, and more resources devoted to security issues on a daily basis.

To meet PCI standards for best practices, SAP customers look to both extend native encryption by using additional encryption methods, and to segregate the encryption function (which helps limit *scope*). To pass QSA audits, SAP customers need an encryption method that fits the following criteria:

- There must be a separation of duties between the business application and the encryption function.
- The encryption key and key-generation capability must reside on a separate server.
- A practical key rollover strategy is critical to success. If switching over to new keys requires system downtime, most companies realistically won't tolerate this. Auditors know that companies won't *do* key rollovers without a *reasonable* way to do them.

SAP customers are also faced with additional concerns. First, SAP native encryption is designed for SAP databases only, so SAP customers running other business software applications must maintain two encryption strategies – one within SAP solutions and one for all other applications.

Secondly SAP companies using legacy hardware encryption modules, such as nCipher or Ingrian Networks, will need an alternative encryption solution. Finally, SAP native encryption handles credit card numbers, but enterprises now need encryption for *personally identifiable information* - social security, Bank ACH, and tax ID numbers. Unfortunately, due to SAP field space restrictions, these data cannot be placed back in the original fields once encrypted – they become too long.

The "encryption in SAP" method has been proven to consistently pass PCI audits.

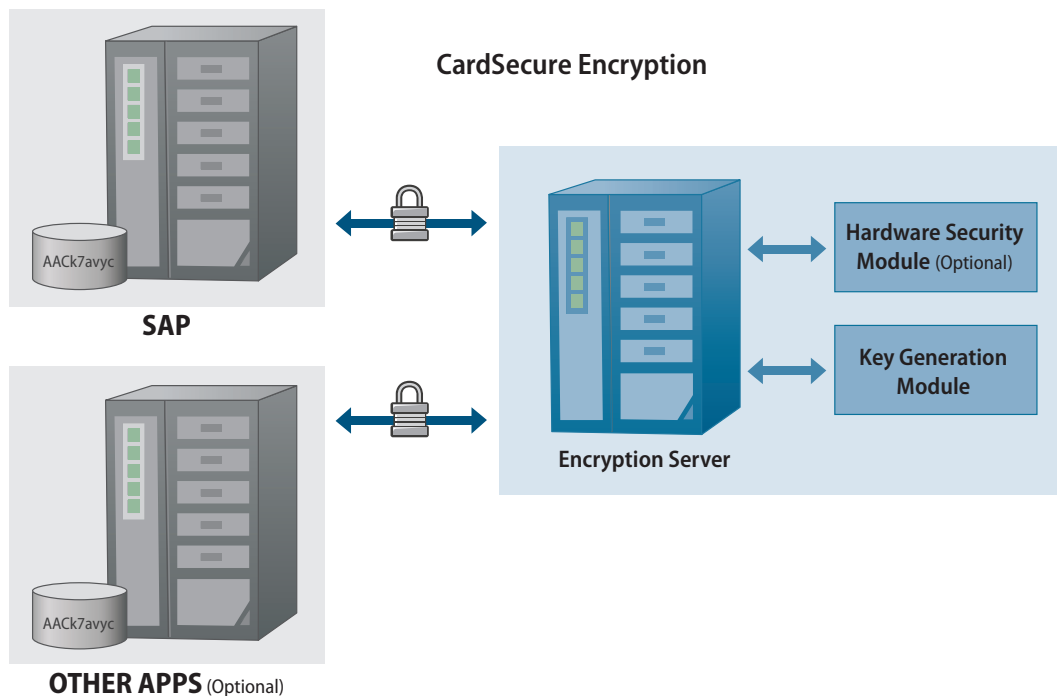
Encryption in SAP

Many customers have found that the encryption method that has proven most successful in passing PCI audits uses an external encryption server, such as a hardware security module, which stores encrypted payment card data directly in the SAP database. The encryption server is invoked by an SAP Remote Function Call (RFC) whenever encryption or decryption is required, as shown in the following diagram.

In this method, the encryption process follows these steps:

1. When the SAP system receives a piece of sensitive data as input, such as a card number, it invokes a Remote Function Call (RFC) that passes the input field to the external encryption server to be encrypted in a manner that passes SAP validity checks.
2. The server returns an encrypted value to the SAP system.
3. The encrypted information is stored in the SAP database like regular data, but now it's secure and unreadable.
4. When an authorized SAP user needs to decrypt the data for use, it passes the encrypted value back to the external encryption server using another RFC and receives the decrypted value in response. The card data is displayed in a masked fashion, i.e. first two digits, last four digits.

The Key Generation Module, which manages the creation and rollover of encryption keys, is separate from the SAP system itself. It is segregated, as mandated by the PCI.



CardSecure has one of the highest numbers of references and passed audits among encryption solutions for SAP environments. And, it is one of the most cost-effective solutions, often by a factor of two or more.

This architecture enforces several key PCI mandates:

- Card data is stored in an encrypted format. No data is stored or displayed “in the clear.”
- The encryption mechanism and the business application are separate, and can be stored or displayed by different administrators.
- Key management is separate from business applications.
- It can accommodate sophisticated key management techniques, so keys can roll over without any SAP system downtime.

The encryption in SAP approach has several other advantages:

- There’s no need to maintain a separate, high-availability database.
- The company can maintain a single security standard. The encryption server easily adapts the SAP system to meet a company’s enterprise-wide standards for security, including specific engines:
 - Supports Hardware Security Modules (HSMs) such as those from Ingrian or nCipher (discussed in detail a little later).
 - Supports external software encryption modules such as Protegrity.
- The encryption can work with other applications to encrypt their data, such as social security, ACH, or tax ID numbers, if desired. However, SAP cannot accept encrypted PII, only tokenized PII.
- Integration does not require changes to the SAP database schema.

Most importantly, this method has been proven to consistently pass PCI audits.

Tokens in SAP

The third and final method for encrypting SAP data involves the use of tokens. Businesses using this method can take the SAP application out of the scope of a PCI audit, thus reducing costs. Tokens may also be used to encrypt hard to manage *personally identifiable information* such as Social Security, Bank ACH and telephone numbers. Tokens can be crafted to meet all SAP validity checks and fit in SAP data fields. Similar to the previous method, an external data server (the token server) handles the encryption process. However, instead of returning encrypted values to the application, the token server stores the encrypted data in a separate database and returns a token that stands in for the encrypted data.

The token method works like this:

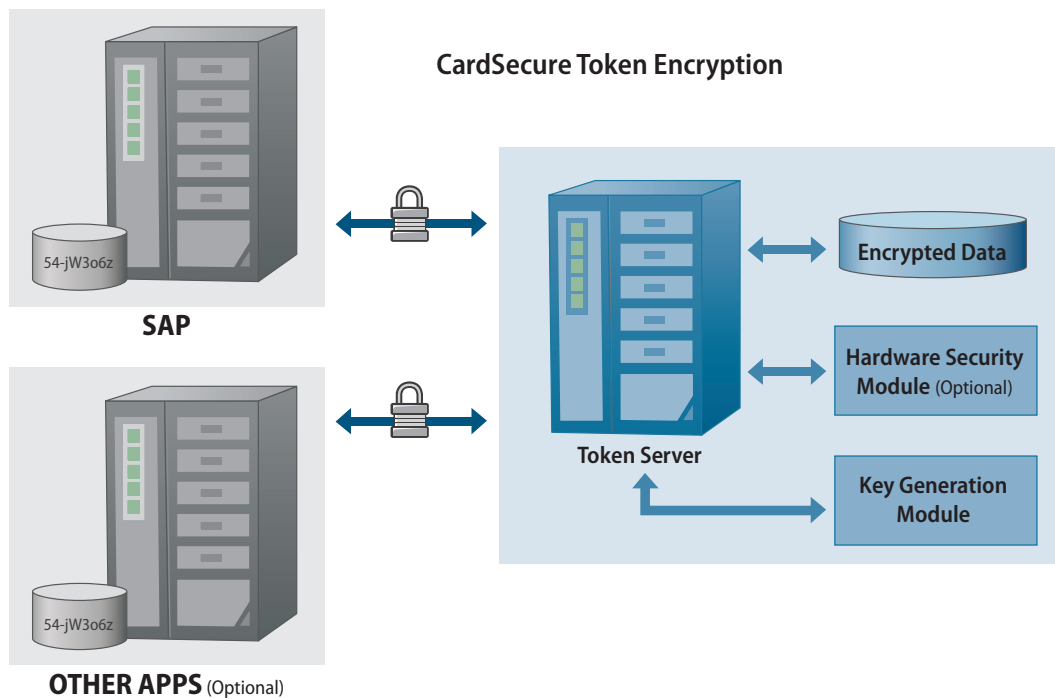
1. When the SAP system receives sensitive data, such as a card number, it sends the data to the token server using an SAP RFC.
2. The token server encrypts the card number and stores it in its own segregated database.
3. The token server returns a unique token to the SAP system that “stands in” for the actual sensitive data; the SAP system stores this token. Sensitive data is completely segregated from the enterprise software.
4. When an SAP function requires an actual card number, it sends the representative token to the token server, which looks up the associated card number, and returns the data to the originating SAP function. Actual card data is always cloaked from non-authorized individuals.

The token approach works with multiple applications and both centralizes and segregates the storage of sensitive information.

Like the *encryption in SAP* method that stores data in SAP, the *tokens in SAP* method satisfies several key PCI requirements:

- The card number is encrypted for storage and the business application does not display data “in the clear.”
- The encryption capability is separate from the application itself, and the token server can be administered by a different group than the SAP administrators.
- Key management is separate from the business application.
- It allows for a practical and efficient key rollover mechanism that doesn’t require application downtime.
- If the enterprise database is running on an insecure platform, tokens thoroughly remove the card number, and even its encrypted representation, from the database to ensure protection against hackers.

The token method is a new, but proven, addition to the PCI encryption arsenal that successfully passes audits. In the SAP environment, it has been in place for over a year.



Hardware Cryptography

Hardware cryptography is well-known as the most secure and efficient encryption method, and many companies already use specialized hardware for their cryptography needs. Hardware Security Modules (HSMs) handle the encryption itself, as well as manage key generation and key rollover. They provide hardware acceleration and tamper-proof protection for keys, so they are faster and more secure than standard encryption engines.

Two types of hardware cryptography are commonly used to speed and secure their encryption processes:

- A hardware server (or “box”), such as made by Ingrian
- A cryptography board that plugs into a server, like nCipher’s

Both the encryption in SAP and the tokens in SAP methods work with existing hardware or software cryptography modules.

CardSecure: An Audit-Friendly “Encryption in SAP” Solution

CardSecure and the optional *CardSecure Token Server* module, from Princeton Payment Solutions, are among the most mature and most widely deployed external encryption solutions that protect card data in SAP environments. These solutions have one of the highest success rates in passing PCI audits for data security, and have earned PCI-SSC Validated Payment Application Status. *CardSecure* provides token encryption and decryption of payment card numbers in SAP solutions and can easily be extended to tokenize other sensitive data such as social security numbers, tax ID numbers and bank ACH numbers.

CardSecure and its Token Server module work within the existing SAP solution structure to encrypt, mask, and protect card data. It requires minimal integration: the SAP system must only be revised to make a remote function call (RFC) to the *CardSecure* external encryption server. Once integrated, *CardSecure* receives all cryptographic requests directly from the SAP system and conducts encryption and decryption transparently to the application.

The *CardSecure* solution addresses all of the PCI’s requirements to protect cardholder data, such as separation of encryption from the application, practical key rollover strategy, and masking displayed card data. Where the use of tokens is desired, *CardSecure* Token Server replaces data within the SAP system with tokens, and card data storage is segregated from the SAP system. These tokens represent the account number and other sensitive data, and will remain the same every time that data is used. For companies who prefer to use the strongest encryption appliances, *CardSecure* works with industrial-strength hardware and software encryption modules from Ingrian and nCipher to provide extra security and efficiency. For companies who prefer a more economical solution, *CardSecure* can provide its own software encryption engine that supports both 3DES and AES encryption.

CardSecure has one of the highest numbers of references and successful audits among encryption solutions for SAP environments. And, it’s one of the most cost-effective solutions, often by a factor of two or more.

Summary and Recommendations

More companies, especially of medium size, are receiving requests for onsite audits from their acquiring banks. With these audits mandatory for companies who need access to the payment card system, it is imperative that companies understand the requirements and properly secure their data. The following chart compares the four main encryption solutions on the market for SAP environments:

	Native Encryption	A Competitors Encryption	CardSecure Encryption	CardSecure Tokens
Secure encryption of data	✓	✓	✓	✓
Card data masked	✓	✓	✓	✓
Enforces separation of encryption capability from SAP system	X	✓	✓	✓
Enforces separation of key generation and management from SAP system	X	✓	✓	✓
Practical key rollover that does not require system downtime	X	✓	✓	✓
Enables different groups to administer SAP system and encryption	X	✓	✓	✓
Encrypts data beyond card numbers, such as SSN & ACH	X	✓	✓	✓
Requires no changes to database schema	✓	✓	✓	✓
Works with additional applications	X	✓	✓	✓
Works with hardware cryptography modules	X	✓	✓	✓
Applications can pass encrypted data between themselves	X	✓	✓	✓
Data not exposed during key rollover process	X	X	✓	✓
Stores data in SAP database	✓	X	✓	X
Replaces data in SAP database with tokens	X	✓	X	✓
Encryption keys safe from hacker assault	X	✓	✓	✓
Does not require additional high-availability server, database, or disaster recovery mechanism	✓	X	✓	X
No downtime for key rollover process	X	✓	✓	✓
Five years of proven success passing PCI audits	X	X	✓	✓
Payment card interface connects directly to token server	X	X	X	✓

Types of Encryption in SAP Environments

Other Useful Resources

PCI Security Standards Council – Data Security Standard

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

PCI Security Standards Council – Home page

<https://www.pcisecuritystandards.org/>

Visa's Cardholder Information Security Program (CISP) Overview

http://usa.visa.com/merchants/risk_management/cisp.html

Visa USA Cardholder Information Security Program (CISP) – Details in PDF

http://usa.visa.com/download/merchants/cisp_overview.pdf

Another good strategy to ensure that companies pass the audit the first time is to hire a PCS-SSC Qualified Security Assessor for a preliminary review. These experts can be counted upon to be helpful advisors – their goal is to help you achieve and then maintain compliance. They can explain the necessary steps for securing data in detail and point out specific flaws in a company's current procedures. Companies then have the opportunity to address any issues before the actual audit.

Companies that are serious about passing PCI audits must look for encryption solutions that have been consistently proven to pass, such as CardSecure from Princeton Payment Solutions. By proactively securing their data according to PCI-DSS standards, companies can avoid the heavy PCI fines that are assessed for failure to comply, and they can better protect their customers.

For more information about how to pass PCI audits and the CardSecure encryption solution for SAP solutions, please contact Princeton Payment Solutions.

Princeton Payment Solutions
116 Village Blvd. Suite 300
Princeton Forrestal Village
Princeton, NJ 08540

Contact: Alex Chapman
Email: achapman@prinpay.com
Phone: +1 (203) 952-5715
www.prinpay.com